PKI Assessment Guidelines

GUIDELINES TO HELP ASSESS AND FACILITATE INTEROPERABLE TRUSTWORTHY PUBLIC KEY INFRASTRUCTURES

PAG v0.30
Public Draft for Comment
June 18, 2001

Information Security Committee
Electronic Commerce Division,
Section of Science & Technology Law, American Bar Association

June 18, 2001

Subject: Release of PAG v0.30 Public Draft for Comment

Dear Colleagues,

It is with great pleasure that the Information Security Committee (ISC) releases the *PKI Assessment Guidelines* – PAG v0.30 Public Draft for Comment (the "PAG") for consultation and comment. The result of a multi-year initiative of intensive research, debate, and drafting, the PAG provides an overview of Public Key Infrastructure (PKI), discusses specific technical, legal, business, and policy issues related to PKI operations, and proposes guidelines for the assessment of PKIs and their components. In the context of the PAG, "assessment" refers to the process of determining whether a PKI satisfies a set of defined criteria, including but not limited to satisfaction of commercial standards, regulatory requirements, and trust mark licensure.

1. Public Comment Solicited

To ensure that the PAG becomes a sustainable, meaningful and unique resource to the broader information security community (including users, providers, and regulators), we offer it for public comment and solicit your considered views. The PAG has already received contributions from over 400 professionals from the fields of law, business and technology. We are thus requesting comments from a wide readership, because an expansive work of this type correspondingly requires a diverse community of reviewers, including professionals in the business and legal community, consumer advocates, and technical experts. As was true with the development of the ISC's *Digital Signature Guidelines* (1996), public comment is both essential and will invariably result in the further refinement and evolution of the PAG. We welcome and encourage your participation in this consultation process.

While all comments are welcome and will be carefully considered, comments on the following topics would be most helpful:

- Suggestions of any topics not covered.
- Qualifications of existing text or suggestions for new text. It would be helpful to also provide the rationale for such suggestions.
- Suggested text or corrections related to considerations of comparative law, business or technology.
- New citations or citation corrections.
- Comments regarding the PAG's organization and "usability."
- Identification of typographical, grammatical and syntax errors would also be appreciated.

2. How to Comment

We appreciate your submission of comments on the comment form that is posted and available for download from the ISC's Home Page located at: <http://www.abanet.org/scitech/ec/isc/home.html>. The comment form requests that you provide the PAG subsection (not merely page number, which is constantly changing) to which each of your comments applies. Because footnotes are constantly being added in our working draft, you should identify a footnote both by number and by a unique phrase in the footnote which can be located with the "Find" command.

Comments should be communicated as follows:

email: < pag-comments@abanet.org >
fax: +1 (312) 988-6797
surface:
PAG Editorial Board
Information Security Committee
Section of Science and Technology Law
American Bar Association
750 North Lake Shore Drive
Chicago, IL 60611-4497

It is most helpful if comments include an e-mail address so that we can obtain any clarification of the comments that might be needed. Although the ISC is pleased to accept comments in any media, comments in electronic form are preferred.

3. Editorial Schedule

Please submit all comments on or before October 18, 2001. The receipt of comments will be acknowledged electronically (provided a return email address is included). Comments will then be reviewed by the PAG Editorial Board and reflected in a proposed final draft for review and comment by the ISC. The disposition of the final draft will then be considered at the next regularly scheduled meeting of the ISC. The ISC meeting schedule is available at the ISC's Home Page.

4. The Fine Print

This PAG Public Draft for Comment is intended exclusively for purposes of obtaining public comment and is not in its current draft form intended to be relied upon in any manner whatsoever. In particular, the PAG does not contain any legal advice; any specific questions that may arise should be referred to qualified counsel. Because this draft is circulated for comment purposes only, any permitted reference to or excerpt from this draft must clearly indicate that the reference is to the "ABA ISC PAG v0.30 Public Draft for Comment Only". For more complete information regarding the copyright notice, please see page 2 of the PAG.

Thank you in advance for your consideration of this draft. We greatly appreciate your time and interest.

Sincerely,

The Information Security Committee

ISBN 1-57073-943-9. Printed in the United States of America.

TABLE OF CONTENTS

A. INTRODUCTION

A.1 Purpose and scope

A.1.1 GENERAL GOALS

The Information Security Committee (the Committee) of the American Bar Association Section of Science and Technology Law developed the *PKI Assessment Guidelines* (PAG)[1] first and foremost as an educational resource. Developed over a period of five years as a sequel to its 1996 *Digital Signature Guidelines* (DSG),[2] the ISC's writing of the PAG coincides with the earliest phase in the commercial and governmental deployment of PKI technology. Given the infancy of the PKI industry, the literature concerning the means and methods for assessing PKIs and concerning PKI in general is relatively sparse. At the same time, the increasing demand for PKI services and products has created a commensurately increasing demand for information about PKIs and how to assess their quality. The shortfall of literature to satisfy this demand has left a gap in knowledge. Accordingly, the Committee has drafted the PAG as an educational resource and guide to address this need.

PKI is an acronym for Public Key Infrastructure, a system utilizing public key cryptography,[3] that when combined with a well-implemented infrastructure, provides a level of security for communicated and stored data sufficient to justify trust in such information by business, consumers, governments, and the courts. "Assessment" refers to the process of determining whether a PKI satisfies a set of defined criteria, including but not limited to satisfaction of commercial standards, regulatory requirements, and trust mark licensure. The PAG provides an overview of PKI, discusses specific technical, legal, business, and policy issues related to PKI operations, and provides guidelines for the assessment of particular PKIs and their components. It is intended for a broad audience ranging from government, business, and legal professionals, to information technology professionals charged with developing, maintaining, and assessing PKIs, regardless of relative familiarity with PKI.

Unlike many assessment standards, the PAG is not limited to technical, legal or compliance concerns, and it is not presented as a prescriptive document. Rather, it addresses technical and business requirements of PKI components within a legal framework, and, based upon the collective experience and expertise of the Committee, it provides guidance on selecting appropriate controls, procedures, and policies to ensure trustworthy PKI operations. Furthermore, because PKIs range from highly-centralized to highly-distributed systems, the PAG contemplates diverse PKI structures and their varying dynamics and requirements for both closed and interoperating PKIs.

A.1.2 SPECIFIC GOALS

The PAG is intended:

[1] References in this document to the "PAG" are in the singular, but the plural is used when referring to its full name, the PKI Assessment Guidelines.

[2] *See* PAG APP 2 (*Digital Signature Guidelines*, ABA Information Security Committee (1996), *available at* <http://www.abanet.org/scitech/ec/isc/digital_signature.html>, hereinafter "DSG"). Information about other publications and membership in the ABA Section of Science and Technology is available from the Manager, Section of Science and Technology, American Bar Association, 750 North Lake Shore Drive, Chicago, IL 60611 USA, Fax: (312) 988-6797, E-mail: sciencetech@abanet.org.

[3] For an introduction, *see* PAG § B.2 2 (The Technology Behind PKI) and PAG APP 3, § 3.1 (Tutorial on Public Key Technology).

- to provide a tool by which people can assess a PKI and its trustworthiness;
- to explain basic PKI assessment models, PKI assessment terminology, and the interface among, and implications of, business, legal, and technical issues in PKI;
- to provide guidance for the selection of policies, standards, and legal agreements, including certificate policies (CPs), certification practice statements (CPSs), relying party agreements, and subscriber agreements;
- to promote smooth interoperation among different PKIs and their components; and
- to provide an intellectual framework and educational resource for understanding PKI services, products, technologies, and emerging legal concepts.

The PAG is *not* intended

- to dictate policies, processes, or legal doctrines; instead, it is intended to foster the development of rational and consistent criteria, profiles, and legal rules;
- to mandate any particular models for assessment; indeed, different needs may be better served by diverse assessment models;
- to remain static; rather, the Committee intends the PAG to be a *living* document, periodically updated and made available to the PKI community on the Internet as needed; or
- to be self-contained, for the PAG attempts to aggregate, focus, and build upon the knowledge and experience of others, by extensively referencing other relevant documents and authorities.

A.1.3 DEVELOPMENT OF THE PAG

The PAG is a logical extension of the *Digital Signature Guidelines* (DSG), which was designed to provide basic technical and legal guidelines regarding the rights and responsibilities of certification authorities, certificate subscribers, and relying parties for digital signature applications of PKI. Reflecting subsequent developments in the PKI industry, the PAG extends and clarifies the DSG. Rather than simply focusing on digital signatures, the PAG addresses additional applications in which PKI plays a central role. In addition, the PAG contemplates the complexity arising from today's demands for PKI interoperability, emphasizing broad assessment issues instead of merely stating the basic issues of PKI installation and use. Like the DSG, the PAG is a product of intense and fruitful collaboration among auditing, business, legal, and technical professionals throughout the world, with the common goal of facilitating secure electronic commerce and communications. The PAG draws upon and seeks to reflect the primary paradigms and practices contained within a broad range of standards, best practices, guidelines, and laws.

Secure e-commerce system interoperation can be facilitated (in terms of certainty, economy, and recognition) when the assessment process and criteria are as uniform as possible. This has occurred somewhat with the adoption of the AICPA/CICA *WebTrust*$^{tm/sm}$ *Program for Certification Authorities*,[4] which provides an assessment checklist. To promote further understanding of PKI systems and the assessment of their underlying policy infrastructure, however, the Committee presents the PAG as an unabridged reference to be used in PKI assessment.

[4] The American Institute of Certified Public Accountants, Inc. and the Canadian Institute of Chartered Accountants released the first version of its WebTrust Program for Certification Authorities on August 25, 2000. *See* PAG APP 2 (*WebTrust Program for Certification Authorities*, v. 1, AICPA/CICA (25 Aug. 2000), *available at* <http://ftp.webtrust.org/webtrust_public/certauth_fin.doc>, hereinafter "AICPA/CICA WebTrust").

Moreover, selecting terms to be used for "PKI assessment" in this document has been difficult because the PAG presents and considers a variety of assessment models and approaches used in a variety of countries[5] by a variety of disciplines. Consequently, some within the PKI community may disagree with the definitions and analytic approaches selected. The Committee out of necessity made choices to improve the usefulness of the PAG, not because it inherently favors one perspective over another. An effort has been made to recognize and discuss different opinions, and the PAG is intended to reconcile and harmonize divergent views within the PKI Community.

A.2 Introduction to PKI Assessment

PKI assessment is the process of determining whether a PKI satisfies a set of defined criteria. Because there are several approaches to PKI assessment,[6] a variety of technical and legal terms are discussed here. PKI assessment can be an essential prerequisite to many PKI licensing regimes,[7] to obtaining and maintaining approval to operate as a PKI service provider for several communities of interest,[8] and to beginning operations[9]

[5] *See* PAG APP 2 (*Community Framework for Electronic Signatures*, Council Directive, 1999/93/EC, 2000 O.J. (L 013) 12-20 (13 Dec. 1999), *available at* <http://www.bmck.com/ecommerce/directivecomp1.htm>, hereinafter "EU Signature Directive"). Opinions vary as to the extent to which assessment criteria should be altered to accommodate regional or local requirements (such as variations in legislation or specific operational requirements of the local environment), or whether the same assessment criteria should be applied everywhere, with variances manifested exclusively in the implementation's CP and CPS. In the European Union, assessment criteria are used to avoid regional or local requirements that can effectively stifle commerce and interfere with the free market of the collective member states. Lacking the equivalent of the Commerce Clause of the U.S. Constitution, which prohibits discriminating against trade originating in sister states, the drafters of the EU Signature Directive chose instead to rely upon a mechanism of voluntary accreditations, not only with respect to "the issuance and management of certificates" but also to "any other product using, or ancillary to, electronic signatures, such as registration services, time-stamping services, directory services, computing services or consultancy services related to electronic signatures." *Id.* at Preamble, ¶ 9.

[6] The concept of a formal audit is encompassed in the term "assessment." An "inspection" is another form of assessment, performed on a regular basis to ensure ongoing compliance with a CP or other applicable requirement or document. A formal inspection is normally referred to as an audit. The Committee has chosen to use as a generic term "audit and other assessments" because the Committee anticipates that the majority of PKI assessments will be referred to as audits, although a minority of Committee members felt that the word "inspection" might better describe the PKI assessment process.

[7] *See, e.g.*, PAG APP 2 (*Washington Authentication Administrative Rules*, WASH. ADMIN. CODE §§ 434-180-200, 240 and 360 (1997), *available at* <http://www.secstate.wa.gov/ea/ealaws.htm>, hereinafter "Washington Admin. Rules"). The initial assessment of a CA for purposes of licensing is based on technical issues only because of its safe harbor based on Guidance for COTS Security Protection Profiles (formerly CS2 Protection Profile Guidance for Near-Term COTS). *See* PAG APP 2 (*Guidance for COTS Security Protection Profiles (CSPP)*, Gary Stoneburner, NISTIR 6462 NIST (Dec. 1999), *available at* <http://csrs.nist.gov/cc/pp/pplist.htm>, hereinafter "Stoneburner"). The subsequent periodic assessment required for continued licensing requires compliance with the much broader Washington Digital Signature Law and Regulations, including legal requirements.

[8] S*ee generally* PAG APP 2 (*Access Certificates for Electronic Services (ACES)*, US Gov't Services Admin. (Mar. 1998), *available at* <http://hydra.gsa.gov/aces>, hereinafter "ACES"), requires "government authorization to operate" prior to issuing certificates. *See also* Advanced Network Exchange (ANX), *available at* <http://www.anxo.com/certified/index.html>. Formerly known as the "Automotive Network Exchange", a CA must become certified as fully compliant with the requirements to issue ANX Certificates. Similarly, Identrus has a solution provider certification program that validates vendor solutions and certifies them as compliant with the brand license and Identrus' standards, *available at* <http://www.identrus.com>.

[9] *See e.g.*, PAG APP 2 (*Guidelines, Methodologies and Standards to set up a CA for Digital Signatures* (GUIDeS), v. 1.1, European Union Project, SPRITE-S2, *available at* <http://www.regione.emilia-romagna.it/guides>, hereinafter "GUIDeS"). GUIDeS is primarily intended for public sector entities and presents a recommended model for evaluating competing PKI vendor technologies and services with the ultimate goal of deciding whether to implement an insource or outsource PKI solution. It emphasizes adherence to industry standards and recommends using the traditional Request for Information (RFI) to vendors followed by a Request for Proposal (RFP)."

pursuant to many PKI interoperability regimes.[10] PKI assessment includes consideration of the technical and architectural details of a PKI, operational practices, and the implementation of technologies, policies, controls, and auditing (including the assessment process itself).

Assessment can take various forms, including self-assessment, formal audits, and rigorous technical evaluations. Therefore, the term "assessors," as used herein, includes inspectors, auditors, accountants, information security professionals, and attorneys and the entities they represent. Discussed below in further detail in PAG § A.6 (PKI Participants). Some assessments are performed prior to a PKI commencing operations. Other assessments are performed periodically to ensure ongoing compliance with the CP or other applicable documents. *See* PAG APP 4 (PKI Audit Methodology and Guidelines).

A.3 Audience

Many individuals and organizations will find the PAG useful, including the following entities:

- *Certification Authorities* (CAs) – the issuers of digital certificates – might use the PAG to assist with the development and review of their practices and to assist in developing and reviewing assessment programs.
- Auditors[11] might use the PAG to develop assessment criteria for judging and reporting upon the performance of CAs and other PKI vendors in a variety of legal contexts.
- Relying parties might use the PAG to gauge the trustworthiness of PKI vendors.
- Licensing and regulatory agencies (including consumer protection bodies) might use the PAG to assess the quality and trustworthiness of a CA for licensing purposes, and to assist in the development of PKI quality requirements.
- Non-Governmental accreditors and local organizations might use the PAG in their role as overseers of a profession or industry (e.g., education and health care[12]) to help them assess the institution as part of a broader accreditation process.
- Repositories might use the PAG to establish or maintain trustworthy operations.
- Purchasers of PKI products and services might use the PAG to assist in selecting a PKI vendor.

A.4 Organization and Use

Major sections. The PAG is divided into sections as follows:

Section A – Introduction – this section provides an introduction to the PAG.

[10] Applicants for interoperability with the Federal Bridge Certification Authority must attach a copy of the latest audit report attesting to the applicant's compliance with the applicant's CP and CPS, *available at* <http://csrc.nist.gov/pki/fbca>.

[11] *See supra* PAG § A.2 (Introduction to PKI Assessment) and discussion of "assessors" in PAG § B.6.1 (PKI Assessment, Participants) *infra*.

[12] For example, the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) might look to the PAG to help in the oversight of implementation of PKI solutions within the delivery and payment for health care to the extent that the infrastructure relies on PKI. (In addition, local boards of registration, which license healthcare professionals, might want use the PAG for issues related to quality of care and modes of delivering the same.)

Section B -- PKI Overview – includes a broad overview of PKI and PKI assessment, some of the most important PKI-related terms, and references highlighting a selection of significant related documents. Section B serves as a prelude to more detailed material found in the **Appendices.**

Section C – Legal Preface – presents important legal principles that interrelate with the implementation of PKI.

Section D -- PAG Provisions -- contains the PAG's substantive assessment provisions that follow a modified version of the outline issue format of RFC[13] 2527 (Formerly PKIX4).[14]

Appendix E.1 -- Glossary of Definitions and Acronyms

Appendix E.2 -- Bibliography with Online URLs

Appendix E.3 -- Tutorial on Public Key Technology

Appendix E.4 -- PKI Audit Methodology and Guidelines

Appendix E.5 -- Proposed Guidance for Development of Compatible End-User Product

Appendix E.6 -- Sample PKI Disclosure Statement

Appendix E.7 – PKI and XML

Appendix E.8 – PKI Assessment Examples

When to consult the PAG. Users may find the PAG helpful at a number of different stages:

- *Before establishing a new PKI.* The PAG can help organizations establishing a PKI to choose appropriate assessment models and criteria. Risk managers and legal advisers will find the PAG a useful checklist when considering the pros and cons of establishing a particular type of PKI. Those crafting legal documents necessary for PKI will also benefit from the PAG, as will those developing and implementing PKI liability insurance coverage and other relevant risk management programs with appropriate premiums and policies.

- *During an assessment.* The PAG is designed to assist those currently assessing a PKI. For example, the PAG may help an assessor determine the equivalence of specified and substitute security controls. Assessors may also use the PAG as a resource for selecting a PKI vendor, making decisions about outsourcing and interoperability, and for training.

- *After an assessment.* Because the PAG explains legal principles related to PKI and its use, it can provide operational guidance on the legal consequences of operating a PKI, as well as insight into dispute resolution issues. Especially in legal disputes destined to become influential cases of first impression, the PAG may be a useful source for legal counsel in preparing pleadings, briefs, and trial strategy, and a secondary source for judges in making judicial decisions and writing opinions.

[13] "RFC" is the acronym for Request for Comments. RFCs form a series of proposed standards, started in 1969, for the Internet. Sometimes an RFC will be adopted within an industry as the de facto standard or guidance on a particular aspect of computer communication, networking protocol, procedure, program or concept, *available at* <http://www.rfc-editor.org/overview.html>.

[14] The Editorial Committee recognizes that an effort has been undertaken to update the CP and CPS framework of RFC 2527. A significant portion of that update has been based on the modified framework of the PAG. Due to the publication schedules of each document, however, the PAG and the updated draft of RFC 2527 will not necessarily track each other provision by provision. It is contemplated that after the public comment period ends, the PAG may be updated to reflect the updated framework.

A.5 Contributors

A.5.1 THE INFORMATION SECURITY COMMITTEE

The Information Security Committee is a group of lawyers and non-lawyers who are practicing attorneys in corporate, private, and government practice, information technologists, auditors, notaries from various legal regimes, trade experts, academics, and others dedicated to exploring and advancing the legal and information security aspects of e-commerce and information technology.

A.5.2 LEADERSHIP AND INDIVIDUAL CONTRIBUTORS

Editorial Board

Joseph H. Alhadeff	Oracle Corporation, Washington, DC
Michael S. Baum *ISC Chair*	Los Altos, CA
Barclay T. Blair *PAG Co-Rapporteur and Incoming Distinguished Committee Rapporteur*	Pure Edge Solutions, Inc., Vancouver, BC
Kimberly Kiefer *Incoming ISC Co-Chair*	Brobeck Phleger & Harrison, LLP, Washington, DC
Charles R. ("Chas") Merrill *PAG Co-Rapporteur and Incoming Distinguished Committee Rapporteur*	McCarter & English, LLP, Newark, NJ
Michael Power	Gowlings Lafleur Henderson, LLP, Ottawa, ON
Randy V. Sabett *PAG Co-Rapporteur and Incoming ISC Co-Vice Chair*	Cooley Godward LLP, Reston, VA
Ruven Schwartz *ISC Vice Chair*	Wells Fargo Cryptography Services, Minneapolis, MN
Gary Stoneburner	NIST, U.S. Dept. of Commerce, Gaithersburg, MD
Benjamin Wilson *PAG Co-Rapporteur and Incoming ISC Co-Vice Chair*	Digital Signature Trust Co., Salt Lake City, UT
Stephen S. Wu *PAG Co-Rapporteur and Incoming ISC Co-Chair*	VeriSign, Inc., Mountain View, CA

Individual Contributors to the PAG

Adamache, Maureen	GOC Dept of Justice	Ottawa, Canada
Adams, Dean	Trustis, Ltd	London, England
Aisenberg, Michael	VeriSign, Inc.	Washington, DC
Akridge, P. Bai	IBM	Mitchellville, MD
Allen, Kenneth	DataCorp	Salt Lake City, UT
Ankney, Richard	CertCo, Inc.	New York, NY (Deceased)
Aragonés, Patricia C.	Attorney/Business Development Advisor	New York, NY
Arceneaux, James C.	Graham & Arceneaux	New Orleans, LA
Arcioni, Paula	State of NJ, E-Govt Services	Trenton, NJ
Aresty, Jeffrey M.	Aresty International Law Offices	Boston, MA
Arthur, Dwight	National Securities Clearing	New York, NY
Asay, Alan	Bolero.net	Salt Lake City, UT
Austin, Tom	IBG Internet Business Group, LLC	Bedford, NH
Aveni, John J.	New York State Office for Technology	Albany, NY
Ball, Robert O., III	Akamai Technologies, Inc.	Cambridge, MA
Barassi, Theodore S.	CertCo, Inc.	New York, NY
Baxter, Mitchell S.	LegalNetWORKS, Inc.	Falls Church, VA
Bejnar, Thaddeus P.	New Mexico Supreme Court Law Library	Santa Fe, NM
Bennett, Daniel	Citizen Contact, Inc.	Washington, DC
Berman, Tony	Thawte Consulting (Pty) Ltd.	Cape Town, South Africa
Bertsch, Andreas	SIZ GMBH	Bonn, Germany
Bezdek, Roger H.	US Dept of Treasury	Washington, DC
Biesheuvel, Andre J.	Dutchgroup.nl	Netherlands
Billeter, David	General Motors Corp.	Detroit, MI
Boeyen, Sharon	Entrust Technologies Limited	Ottawa, ON, Canada
Bogino, Charles	BNA Electronic Commerce & Law Report	Washington, DC
Bohannon, Mark	US Dept of Commerce	Washington, DC
Bond R.	Hobson & Audley	London, England
Boots, Andrew J.	US General Services Administration	Washington, DC
Bos, Janjaap J.	DSEMCO	Waterloweg, Netherlands
Boss, Amelia H.	Temple University School of Law	Philadelphia, PA
Boulay, Liette	Notarius	Montréal, Québec, Canada
Bowler, Richard W., Jr.	US Dept of Jutice	Washington, DC
Bradley, Rebecca G.	Whyte Hirschboeck Dudek	Milwaukee, WI
Brandt, Leopold	Azpurua & Asociados	Caracas, Venezuela
Brandt, Linda	National Security Agency	Ft. George G. Meade, MD
Brecher-Kovacevic, Valerie	US Environmental Protection Agency	Washington, DC
Bréniel, Marie-Josée	Notarius	Montréal, Québec, Canada
Brice, Bill	AlphaTrust Corp.	Dallas, TX
Bro, Ruth Hill	Baker & McKenzie	Chicago, IL
Brown, Laurence W.	Edison Electric Institute	Washington, DC
Brown, Toby	iLumin	Orem, UT
Bryan, Mathew R.	World Intellectual Property Organization	Geneva, Switzerland
Buhle, Gordon L.	Oracle Corporation	Redwood Shores, CA
Burger, Robert J.	McCarter & English, LLP	Newark NJ
Burman, Harold S.	US Dept of State	Washington, DC
Burr, Bill	NIST, US Dept of Commerce	Gaithersburg, MD
Byass, Kenneth	Internatl Comm Law & Society	London, England
Cahill, John F.	Carter Ledyard & Millburn	Washington, DC
Cain, Pat	GENUiTY	Burlington, MA
Caldwell, Kaye	CommerceNet	Capitola, CA
Canavan, Blair	Chrysalis-ITS	Ottawa, ON, Canada
Carlson, Amy L.	Kirkpatrick Stockton LLP	Reston, VA
Champi, David L.	EDS	Herndon, VA
Cheng, Edward K.	Law Clerk, US Court of Appeals, DC Circuit.	Washington, DC
Chew, Denley Y. S.	Federal Reserve Bank of NY	New York, NY
Chokhani, Santosh	Cygnacom Solutions, Inc	McLean, VA
Chong, Debra	Virtual Boardwalk (Lenos.com)	San Francisco, CA
Christiansen, John R.	Stoel Rives LLP	Seattle, WA
Claypoole, Theodore F.	Womble Carlyle Sandridge &Rice	Charlotte, NC
Cleland, Bartlett D.	Senator John Ashcroft Staff (?)	Washington, DC
Cloutier, Michel	Treasury Bd Secretariat, Govt of Québec	Sainte-Foy, Quebec, Canada
Coburn, Kathryn R.	WellPoint Health Networks Inc.	Woodland Hills, CA

Cohen, Andrea	Boston Univ Law School Student	Boston, MA
Coleman, Kevin M.	KPMG LLP	San Francisco, CA
Cooper, David	NIST, US Dept of Commerce	Gaithersburg, MD
Cooper, Michele	SynData Technologies	Teaneck, NJ
Copeland, Guy	Computer Sciences Corporation	Falls Church, VA
Corwin, Philip S.	Federal Legislative Associates	Washington, DC
Cotter, B. Paul Jr.	US Nuclear Regulatory Commission	Washington, DC
Couillard, Bruno	Chrysalis-ITS	Ottawa, ON, Canada
Cox, Wanda	Apple Computer, Inc.	Cupertino, CA
Crabree, Bruce	Conanticut Communication, Inc	Conanticut, CT
Cramm, David	Labcal Technologies, Inc	Hull, Québec, Canada
Crittenden, Leianne	Oracle Corporation	Redwood Shores, CA
Cronin, J. Leo	Lexis-Nexis	Miamisburg, OH
Crystal, Jamie	Frank Crystal & Co., Inc	New York, NY
Cyr, Miriam	Labcal Technologies	Ottawa, ON, Canada
Daguio, Kawika	Financial Information Protection Assn.	Washington, DC
Dalton, Clark W.	Alberta Justice, Civil Law Division	Calgary, AB, Canada
Damaso, Tinna	University of Baltimore	Baltimore, MD
Daniels, Robert W.	EDS	Herndon, VA
Danner, David	State of Washington, Dept of Info Services	Olympia WA
Davidson, Glenn K.	Computer & Communications Industry Assn	Washington, DC
De Maria, Elayne	Certco, Inc.	New York, NY
DeJarnette, Ken	Deloitte & Touche, LLP	San Francisco, CA
Dodson, Donna F.	NIST, US Dept of Commerce	Gaithersburg, MD
Doherty, Alan	Collaw.org.ul	London, England
Doonan, Wes	Surety Technologies, Inc.	Reston, VA
Dorney, Maureen S.	Gray Cary Ware & Freidenrich, LLP	Palo Alto, CA
Driggs, Alex	Cooley Godward LLP	Reston, VA
Dubishar, Wm. Craig	Venable Baetjer and Howard LLP	McLean, VA
Dulin, Charles	CertCo, Inc	Cambridge, MA
Dunford, Anthony G.	The Notaries' Society	Ipswich, Suffolk, England
Durst, Rob	NeoMedia Technologies	Ft. Myers, FL
Duthler, Anne-Wil	Duthler Associates	The Hague, Netherlands
Dziadyk, William G.	Domus	Ottawa, ON, Canada
Eckl, Peter	Anhausser, Unger, Eckl & Bergien	Karlsruhe, Germany
Edfors, Patricia N.	PNE Associates	Reston, VA
Effross, Walter E.	Washington College of Law, American Univ.	Washington, DC
Ellison, Carl M.	CyberCash, Inc.	Baltimore, MD
Ellison, John P.	Univ. of Michigan Medical Center	Ann Arbor, MI
Engelke, Charles	Info Tech Florida	Gainesville, FL
Engler, Katherine A.	Minnesota Office of Secretary of State	St. Paul MN
Enright, Keith P.	Techne Consulting	Boston, MA
Evans, Christine	GOC Security Intelligence Service	Ottawa, ON, Canada
Fares, David A.	U.S. Council for International Business	New York, NY
Farrell, Stephen	Baltimore Technologies	Dublin, Ireland
Ferguson, Bill	Compaq Computer Corporation	Cupertino, CA
Field, Richard L.	Attorney at Law	Cliffside Park, NJ
Field, Steven J.	DSI Technology Escrow Services	Rosell, IL
Fillingham, David	National Security Agency	Ft. George G. Meade, MD
Fisher, Ann	US Dept of Transportation	Washington, DC
Fisher, Richard D.	Cohasset Associates, Inc.	Los Gatos, CA
Fleisher, Steven M.	MEDePass, Inc.	San Francisco, CA
Foley, Parker	First Union National Bank Corporation	Charlotte, NC
Ford, Warwick	VeriSign, Inc.	Wakefield, MA
Fox, Barbara	Microsoft Corporation	Redmond, WA
Francoeur, Jacques Remi	Silanis Technology, Inc	Campbell, CA
Frankel, Yair	TechTegrity	Westfield, NJ
Frazer, Deb	KPMG LLP	Mountain View, CA
Fresen, Gary W.	Baker & McKenzie	Chicago, IL
Frith, Bob	Motorola	Scottsdale, AZ
Frye, Emily	iWitness, Inc.	Boulder, CO
Garden, Jay T.	GOC Communications Security Establishment	Ottawa, ON, Canada
Gauthier, Barry	VeriSign, Inc	Manotick, ON, Canada
Gellatly, Erik W.	Legal Anywhere, Inc.	Tualatin, OR
Gesmer, Lee T.	Lucash, Gesmer & Updegrove	Boston, MA
Ghahremani, Joanne	Concert/GV	Reston, VA
Gilbert, Françoise	Gray Cary Ware & Freidenrich, LLP	Palo Alto, CA
Gillman, Libby F.	Cap Gemini	Toronto, ON, Canada
Glassey, Todd	Glassey-McNeil Technologies	Scotts Valley, CA
Goldberg, Alan S.	Goulston & Storrs, PC	Boston, MA
Goldstone, David Jerald	US Dept of Justice	Washington, DC
Gora, Daniel M.	Thomson Legal & Regulatory Tech Svcs	Eagan, MN

Graff, Jon C.	Deloitte & Touche Security Services LLC	San Jose, CA
Greco, Tom	Digital Signature Trust Co	Washington, DC
Green, Lawrence M.	US Commodity Futures Trading Commission.	Washington, DC
Greenwood, J. Daniel	MIT E-Commerce Architecture Project	Boston, MA
Gregorits, Angela	BNA Electronic Commerce & Law Report	Washington, DC
Gregory, John	Ministry of Attorney General/Management Board Secretariat/Govt of Ontario	Toronto, ON, Canada
Grimm, Eric C.	Sonnenschein Nath & Rosenthal	Washington, DC
Guida, Rich	Johnson & Johnson	New Brunswick, NJ
Gupta, Sush	GOC Dept of Justice	Ottawa, ON, Canada
Haack, Marr T.	St. Paul Fire and Marine Ins. Co.	Stillwater, MN
Hagen, Gregory R.	McCarthy Tetrault	Vancouver, BC, Canada
Hai, Lim Huck	KPMG Peat Marwick / Desa Megat & Co	Kuala Lumpur, Malaysia
Hale, W. Michael, Jr.	Morris, Manning & Martin	Atlanta, GA
Hall, Eamonn G.	Telecom Ireland	Dublin, Ireland
Hallam-Baker, Phillip	VeriSign, Inc.	Wakefield, MA
Hare, Lisa L.	US Dept of Navy	Washington, DC
Harllee, John	Oracle Corporation	Bethesda, MD
Harrold, Todd	Entrust Technologies Limited.	Ottawa, ON, Canada
Harter, Peter F.	Securify, Inc.	Mountain View, CA
Heben, Tiffanie	National Notary Association	Chatsworth, CA
Hedlund, Julie	National Automated Clearing House Association	Herndon, VA
Hein, Werner J.	Mayer Bown & Platt	Washington, DC
Heller, William J.	McCarter & English LLP	Newark, NJ
Hellstrom, Per	The European Commission	Brussels, Belgium
Helm, Troy K.	ID Certify	Sunnyvale, CA
Hicks, G. Mack	Bank of America	San Francisco, CA
Hill, Jane	Barrister-at-Law, Lincoln's Inn	London, England
Hiller, Marc David	New York State Office for Technology	Albany, NY
Hilton, Jeremy	ADDTrust	Europe
Hines, Eugene E	American Society of Notaries	Washington, DC
Hines, Michael S.	Institute of Internal Auditors	West Lafayette, IN
Hirsh, Skip	Certicom Marketing	McLean, VA
Hodkowski, William A.	Gray Cary Ware & Freidenrich, LLP	Palo Alto, CA
Hommer, J. Scott, III	Venable, Baetjer and Howard, LLP	McLean, VA
Hood, Gary A.	Piper Marbury Rudnick & Wolfe LLP	Chicago, IL
Hopcroft, Thomas	Massachusetts Electronic Commerce Assn	Waltham, MA
Hopkins, Dale	Atalla Incorporated	San Jose, CA
Hornbeck, Rick	Hornbeck Consulting	Pasadena, CA
Horning, Richard Allan	Tomlinson Zisko Morosoli & Maser LLP	Palo Alto, CA
Housley, Russell	SPYRUS, Inc	Herndon, VA
Howland, John Jr.	State of Vermont, Deputy Secretary of State	Montpelier, VT
Hurtt, Marva S.	Oracle Corporation	Washington, DC
Hustein, Joseph	Freelance Legal Tech Reporter	Palo Alto, CA
Ihara, Tomohito	Ministry of Internatl Trade & Industry, Japan	Tokyo, Japan
Jensen, Steven	Commonwealth of Massachusetts	Alston, MA
Johnson, L. Arnold	NIST, Natl Info Assurance Prtship (NAIP)	Gaithersburg, MD
Johnson, Robert A.	Syracuse Research Corporation	Chantilly, VA
Jorgensen, Aimee	Insweb Corporation	Redwood City, CA
Jueneman, Robert R.	Novell, Inc	Provo, UT
Juffernbruch, Dale	Household Bank	Prospect Heights, IL
Kaewjumnong, Surangkan	Ministry of Science, Technology & Environment, Govt of Thailand	Bangkok, Thailand
Kahn, Rebecca	US General Services Administration, FPKISC	Washington, DC
Kalsy, Kavita	US Dept of the Treasury Bureau of the Public Debt	Washington, DC
Kaminski, Shawn Taylor	ABA Section of Science & Technology	Chicago, IL
Kaplan, Ray	Secure Computing.com	
Kastner, Richard P.	Ernst & Young, LLP	San Francisco, CA
Kellenbenz, Jerry	Apple Computer, Inc	Cupertino, CA
Kelly, Debra	Digitalcounsel.com	Washington, DC
Kennair, William B.	Society of Scrivener Notaries, City of London	London, England
Kent, Stephen T.	BBN Communications	Cambridge, MA
Kesterson, Hoyt L., II	Chair, X.509 Working Group; Bull (emeritus)	Glendale, AZ
Kikos, Peter	Systems Research	Sunnyvale, CA
Kinard, Lisa M.	Monterey Institute of Internatl Studies	Monterey, CA
King, Michael	GMTsw	Scotts Valley, CA
Kirwan, Mary P.	Baltimore Technologies	Dublin, Ireland
Klein, Sheldon	Superior Consultant Holdings Corporation	Southfield, MI

Koeppen, Susan Kelley	KPMG LLP	Washington, DC
Kong, Stephen	Squire, Sanders & Dempsey L.L.P.	San Francisco, CA
Koorn, Ronald	KPMG LLP	San Francisco, CA
Koso, Johanna D	Harris Trust and Savings Bank	Chicago, IL
Kowalsky, Ann	ABA Section of Science & Technology	Chicago, IL
Kuo, Teresa	VeriSign, Inc	Mountain View, CA
Kurzban, Stanley K.		Chappagua, NY
Kutz, Bruce	US Bureau of Export Administration	Washington, DC
Lam, Shannon	VeriSign, Inc.	Mountain View, CA
Lambert, Frank	Iwitness, Inc.	Denver, CO
Landon, Christopher	Deloitte & Touche LLP	San Francisco, CA
Larimer, Jane	National Automated Clearing House Association	Herndon, VA
Laster, Gerry A.	Law Office of Gerry A. Laster	San Mateo, CA
Lauzon, Yvan	Secretariat du Conseil du trésor Gouvernement du Québec	Montréal, Québec, Canada
Lazarus, Rhonda	GOC Dept of Justice	Ottawa, ON, Canada
Ledig, Robert H.	Fried, Frank, Harris, Schriver & Jacobson	Washington, DC
LeFevre, Kristen R	US Social Security Administration.	Baltimore, MD
LeGrand, Charles H.	The Institute of Internal Auditors	Altamonte Springs, FL
Leopard, Matthew	US Environmental Protection Agency	Washington, DC
Leslie, Brian G.	Georgia State University	Atlanta, GA
Lestage, Richard	Secrétariat du Conseil du Trésor du Canada	Ottawa, ON, Canada
Levine, Diane	Strategic Systems Management, Ltd.	New York, NY
Levine, Judah	NIST, US Dept of Commerce	Boulder, CO
Levy, David	International Law Institute	Washington, DC
Ling, Theodore	Baker & McKenzie	Toronto, ON, Canada
Linnstaedter, Susan	NationsBank	Dallas, TX
Lipp, Peter	Graz University of Technology	Graz, Austria
Lobenstein, Kenneth W.	Claritech Corporation	Pittsburgh, PA
Longtin, Benoit	Chambre des notaries du Québec	Montréal, Québec, Canada
Louden, T. Michael	The Mitre Corporation	McLean, VA
Lovejoy, Jim	National Security Agency	Ft. George G. Meade, MD
Lucas, Jay	U. S. Patent and Trademark Office	Arlington, VA
Lundin, Mark A.	KPMG LLP	San Francisco, CA
Lynch, Kevin	Fidelity Investments	Boston, MA
Lyons, Patrice A	Law offices of Patrice Lyons	Washington, DC
Macauley, Tyson	JAWZ, Inc.	Ottawa, ON, Canada
Mack, Greg D.	National Security Agency	Fort George G. Meade, MD
Mack, Laurie	GOC Communications Security Establishment	Ottawa, ON, Canada
Mackintosh, Linda	ID Certify	Redondo, WA
MacLellan, Elizabeth	Entrust Technologies, Limited	Ottawa, ON, Canada
Madden, Steve C	Bell Global Solutions (Canada)	Toronto, ON, Canada
Maher, David W.	Sonnenschein, Nath & Rosenthal	Chicago, IL
Mann, Michelle	GOC Dept of Justice	Ottawa, ON, Canada
Manning, Jan A.	National Security Agency	Ft George G. Meade, MD
Manoff, Hector Ariel	Vitale, Manoff, Feilbogen & Lavalle	Buenos Aires, Argentina
Marchant, Michael W.	Entegrity Solutions Corporation	San Jose, CA
Marinier, Francois	Labcal Technologies	Hull, Québec, Canada
Marks, Richard	Davis Wright Tremaine LLP	Washington, DC
Marrero, Angel R.	McConnell Valdes	San Juan, PR
Masse, David G.	Chait Amyot, Barristers & Solicitors	Montréal, Québec, Canada
Matthews, Tim	RSA Security, Inc.	San Mateo, CA
Matthias, Rebecca	VeriSign, Inc	Mountain View, CA
Mauzy, Renee	Texas Dept of Information Resources	Austin, TX
Maxwell, Gary	DOMUS Software	Ottawa, ON, Canada
McClure, Susan	Cooley Godward LLP	Reston, VA
McConnell, Bruce	US Office of Management and Budget	Washington, DC
McCullagh, Adrian	SPYRUS, Inc.	San Jose, CA
McCullough, John A.	Doyle & Bachman	Washington, DC
McGee, Kate	Oracle Corporation	Redwood Shores, CA
McJohn, Steven	Suffolk University Law School	Boston, MA
McNeil, Michael E.	Glassey-McNeil Technologies	Scotts Valley, CA
McNulty, Lynn	RSA Security, Inc	Vienna, VA
Mears, Rena	Deloitte & Touche LLP	San Francisco, CA
Meijer, Paul	VeriSign, Inc.	Mountain View CA
Meinhardt, Robyn	Foley & Lardner	Denver, CO
Melling, Thomas G.	Elf Technologies, Inc.	Issaquah, WA
Mendelson, Kenneth A.	Tristrata Security	Bethesda, MD
Merrill, Andrew T.	Synapsis Solutions, Inc.	Berkeley, CA

Merrill, Whit	Synapsis Solutions, Inc	Berkeley, CA
Messing, John	Law-on-Line, Inc.	Tucson, AZ
Miccoli, Mario	U.I.N.L.	Livorno, Italy
Miller, Chuck	ZEFER Corp.	San Francisco, CA
Miller, Greg	Network Tool-&-Die, LLC	Portland, OR
Miller, Larry	Identrus, LLC	New York, NY
Miller, Robert	US Dept of Commerce, Critical Infrastructure Assurance Office	Washington, DC
Mitrakas Andreas	GlobalSign	Brussels, Belgium
Mitty, Todd Jay	NetDox, Inc	Deerfield, IL
Moran, Amy K.	State of Wisconsin, Div of Technology Mgmt	Madison, WI
Morgan, Michael F.	Entrust Technologies Limited	Ottawa, ON, Canada
Mori, Keiko	Washington CORE	Bethesda, MD
Moses, Tim	Entrust Technologies Limited	Ottawa, ON, Canada
Moskowitz, Robert G	International Computer Security Assn	Oak Park, MI
Mueller, Otto	Zurich Chamber of Commerce	Zurich, Switzerland
Muftic, Sead	COST Sweden	Hasselby, Sweden
Muller, John D.	Brobeck, Phleger & Harrison LLP	San Francisco, CA
Myers, Michael	TraceRoute, Inc.	Half Mon Bay, CA
Nadeau, Jason	Pure Edge Solutions, Inc.	Concord, CA
Nagle, Timothy J.	TRW Systems & Information Technology	Fairfax, VA
Nakamura, Yoshito	Mitsubishi Corporation	Tokyo, Japan
Nazario, Noel A.	KPMG LLP	Washington, DC
Nelson, Barry C.	Technology Specialist	Boston, MA
Nelson, Ben	Kansas Department of Transportation	Topeka, KA
Nelson, Larry D.	MCS, Inc	Washington, DC
Newell, James A	Freddie Mac	McLean, VA
Nilsson, Hans	Sonera SmartTrust AB	Stockholm, Sweden
Nobles, Kimberley G.	Blakely Sokoloff Taylor & Zafman	Costa Mesa, CA
Nordén, Anna	International Chamber of Commerce	Paris, France
Nuara, Leonard T.	Thacher Proffitt & Wood	Jersey City, NJ
O'Higgins, Brian	Entrust Technologies Limited	Ottawa, ON, Canada
O'Neill, Kevin	SPYRUS, Inc	San Jose, CA
Olson, Dwight	DSI Technology Escrow Services	San Diego, CA
Ophir, Gol C.	Morgan Stanley & Co., Inc.	New York, NY
Orlowski, Steve	Australia Dept of the Attorney-General	Sydney, NSW, Australia
Oshman, Dave	PriceWaterhouse Coopers LLP	Linthicum, MD
Othman, Noor Azil	Digicert SDN	Kuala Lumpur, Malaysia
Ozgar, Gene A.	KPMG LLP	Charlotte, NC
Pagan, Michelle M.	Tovaris, Inc.	Charlottesville, VA
Pallante, Jody	Attorney at Law	Philadelphia, PA
Parenty, Thomas J.	Sybase, Inc.	Emeryville, CA
Parisien, Serge	Université de Montréal Faculté de droit	Montréal, Québec, Canada
Parker, Ira H.	GTE Internetworking	Boston, MA
Parker, Mary C.	Oracle Corporation	Bloomington, MN
Paul, George	Lewis & Roca, LLP	Phoenix, AZ
Pawliczek, Jamie C.	Gray Cary Ware Freidenrich, LLP	Palo Alto, CA
Pérez, Aram	Wave Systems Corp	Cupertino, CA
Perreault, Claude	VPN Tech, Inc	Longueuil, Québec, Can
Piazza, Ethna M.S.	Sheppard, Mullin, Richter & Hampton, LLP	San Diego, CA
Pickford, Robert W.G.	W.& A. Glossop, Solicitors	Sheffield, England
Piette-Coudol, Thierry	Avocat	Cran Gevrier, France
Piombino, Alfred E.	NotaryPublicLaw	Portland, ME
Pluswick, Leo	International Computer Security Assn	Carlisle, PA
Pope, Nicholas	Security & Standards Consultancy, Ltd	Chelmsford, England
Popyk, Louise	EDS	Troy, MI
Porter, John I.	StarGate Development Group	Somerset, NJ
Pretorius, Bertus	The South African Certification Agency Ltd	Hennoposmeer, So. Africa
Pugnetti, Jerry	State Auditor's Office, State of Washington	Olympia, WA
Purcell, Arthur F.	US Patent and Trademark Office	Arlington, VA
Radcliffe, Mark F.	Gray Cary Ware & Friedenrich, LLP	Palo Alto, CA
Ramsay, John T.	Gowlings Lafleur Henderson. LLP	Calgary, AB, Canada
Randall, James	Trans Union Corporation	Chicago, IL
Randall, Karen T.	SPYRUS, Inc.	Jackson, NJ
Ray, Philip	Siemens Aktiengesellschaft	Erlangen, Germany
Redden, Wynn	GOC Communications Security Establishment	Ottawa, ON, Canada
Redmon, Gant, III	Axent Technologies, Inc.	Rockville, MD
Reed, Elise	Old Republic Natl Title Ins. Co.	Minneapolis, MN
Remsu, Joan E.	GOC Dept of Justice	Ottawa, ON, Canada
Ricchio, Mike	Washington Secretary of State's Office	Olympia WA
Richardson, J. Blair	Aristotle	McLean, VA
Rishikof, Harvey	US Federal Bureau of Investigation	Washington, DC

Ritter, Jeffrey B	Kirkpatrick & Lockhart LLP	Washington, DC
Roback, Edward A.	NIST, US Dept of Commerce	Gaithersburg, MD
Robinson, David C.	Datum, Inc.	San Jose, CA
Robinson, Joe	US Postal Inspection Service	Washington, DC
Robinson, Peter	US Council for International Business	New York, NY
Rodriguez-Torrent, Juan	Aposematic Corp.	Southbury, CT
Roelofs, Dawn	Cooley Godward LLP	Reston, VA
Rosenberg, Tim	White Wolf Consulting	Norristown, PA
Ross, Ronald	NIST, Natl Info Assurance Partnership	Gaithersburg, MD
Rousseau, Francois	Chrysalis-ITS	Ottawa, ON, Canada
Rubin, Julie A. H.	Aresty International Law Offices	Boston, MA
Rubin, Michael	NIST, US Dept of Commerce	Gaithersburg, MD
Rubinstein, Ira S.	Microsoft Corporation	Redmond, WA
Russell, Shauna D.	Office of US Secretary of Defense	Washington, DC
Russell, William	Piper Marbury Rudnick & Wolfe LLP	New York, NY
Ryan, Mike	G5 Technologies, Inc.	Wilmington, DE
Sabo, John T.	IBM Tivoli	Annapolis, MD
Samar, Vipin	Oracle Corporation	Redwood Shores, CA
Sams, Wayne	First Union National Bank Corporation	Charlotte, NC
Sanford, David	Mitretech Systems, Inc	McLean, VA
Santesson, Stefan	Accurata	Stockholm, Sweden
Sauriol, J.F.	Labcal Technologies	Ottawa, ON, Canada
Savage, Russ	Office of the Secretary of State of Arizona	Phoenix, AZ
Schessel, Harry B.	Science Applications International Corp	San Diego, CA
Schmid, Linda	Coalition of Service Industries	Washington, DC
Schmidt, Joshua J.	Washington State Auditor's Office	Olympia, WA
Schnapp, Daniel E.	Merrill Lynch	New York, NY
Schneider, Daniel B.	US Dept of Justice	Washington, DC
Schnizlein, John M.	U.S. House of Representatives, Information Resources	Washington, DC
Schooler, William L.	Universal Hi-Tech Development, Inc.	Rockville, MD
Schwartz, Mark J.	NetDox, Inc.	Deerfield, IL
Schwarz, David	US Environmental Protective Agency	Washington, DC
Scott, Steve	Compaq Computer Corporation	Cupertino, CA
Sebring, Jeff	The Mitre Corporation	McLean, VA
Sharron, Stephanie L.	Wilson Sonsini Goodrich & Rosati	Palo Alto, CA
Shesko, Marianne	Silanis Technology, Inc.	Campbell, CA
Shirey, Robert W	BBN Systems and Technologies	Arlington, VA
Sigel, Schuyler M	Baker & McKenzie	Toronto, ON, Canada
Silvern, Mark	VeriSign, Inc.	Mountain View, CA
Simonetti, David	Securify, Inc.	Owings Mills, MD
Slocum, Patricia	US General Accounting Office	Washington, DC
Smedinghoff, Thomas J.	Baker & McKenzie	Chicago, IL
Smith, Edgar	Litton Industries, Inc	Arlington, VA
Smith, Malcolm	Microsoft Corporation	Redmond, WA
Solo, David	Citicorp	New York, NY
Sorebo, Gib	Office of the Clerk, US House of Representatives	Washington, DC
Spencer, Judith A.	US General Services Administration, Chair FPKISC	Washington, DC
Sriram, Kaushik P. (Ram)	Madan & Morris	Houston, TX
Staggs, Dave	Science Applications International Corp	San Diego, CA
Stapleton, Jeff	KPMG LLP	Boston, MA
Starrett, Paul	RSA Security, Inc.	San Mateo, CA
Steele, Shari	Electronic Frontier Foundation	Bryans Road, MD
Stempora, Jeffrey	State Farm Insurance Cos	Bloomington, IL
Stewart, Jon	Digital Signature Trust Company	Salt Lake City, UT
Stewart, Robert	CertCo, Inc.	Cambridge, MA
Sudia, Frank Wells	Fintegrity Ventures, LLC	New York, NY
Sugiyama, Hitofumi	The Center for Financial Industry	Tokyo, Japan
Sullivan, Alanna	ABA Section of Science & Technology	Chicago, IL
Sweigert, David G.	EuroSignCard S.A	Luxembourg
Talkovsky, Steven H.	AT&T	Washington, DC
Tancredi, Perry	VeriSign, Inc.	Wakefield, MA
Tapling, Peter G.	NetDox, Inc.	Deerfield, IL
Taylor, Paul W.	Washington State Dept of Info Services	Olympia WA
Teck, Lee Hooi	Mimos	Kuala Lumpur, Malaysia
Temple, Robert	BT Laboratories	Ipswich, Suffolk, England
Tepper, Ralph F.	CertCo, Inc.	New York, NY
Teppler, Steven W.	TimeCertain, LLC	Kensgington, MD
Theriez, Dominique	Cap Gemini	Issy-Les-Moulineaux, France
Thibodeau, Suzanne	Deloitte & Touche, LLP	Montréal, Québec, Canada
Thiessen, Kendall	Gibson Dunn & Crutcher	Washington, DC

Thomas, Philip	World Intellectual Property Organization	Geneva, Switzerland
Till, Gregory J.	US Dept of the Treasury, Bureau of the Public Debt	Washington, DC
Tippett, Peter S.	International Computer Security Assn	Carlisle, PA
Tomaszewski, John P.	Attorney at Law	Austin, TX
Trout, Stephen N.	State of California, Secy of State's Office	Sacramento, CA
Turner, Sean	Internatl Electronic Commun Analysts, Inc.	MD
Usher, Ron	The Law Society of British Columbia	Vancouver BC, Canada
Vacura, Richard	Piper Marbury Rudnick & Wolfe LLP	Washington, DC
Van Eecke, Patrick	Interdisciplinary Centre for Law and IT	Leuven, Belgium
Van Hess, Edmond P.	GOC Communications Security Establishment	Ottawa, ON, Canada
Vandagriff, David P.	LEXIS-NEXIS	Miamisburg, OH
Versace, Michael	ZEFER Corp.	San Francisco, CA
Vincent, Todd	Georgia State University	Atlanta, GA
Volk, Michael L.	Trans Union Corporation	Chicago, IL
von Bernhardt, A. Shaen	DeLoitte & Touche Security Services, LLC	Deerfield, IL
Vreeke, Arjan	KPMG EDP Accountants N.V	Rotterdam, Netherlands
Vuylsteke, Bram	Lic. Rechten, Lic Notariaat	Riemst, Belgium
Wakonig, Harald	Oracle Corporation	Redwood Shores, CA
Waldron, Roger	General Services Administration	Washington, DC
Walkama, Dorianne	VeriSign, Inc.	Wakefield, MA
Walsh, John P. (Jack)	Verizon	New York, NY
Walton, Charles	Securify, Inc.	Weymouth, MA
Walz, Jerry A.	US Dept of Commerce	Washington, DC
Ward, John	US Patent and Trademark Office	Arlington, VA
Warren, Pamela M.	Oklahoma Department of Central Services	Oklahoma City, OK
Watkins, Brenda	GOC Chief Information Officer Branch, Treasury Board of Canada Secretariat	Ottawa, ON, Canada
Wattiez-Larose, Veronique	University de Montreal Faculte de droit	Montréal, Québec, Canada
Weiss, Peter	US Office of Management and Budget	Washington, DC
Wetenkamp, Kristin L.	Sun Microsystems	Broomfield, CO
White, Jeff W.	American Financial Group, Ltd	Berwyn, PA
Wiegand, Jamie	The Boeing Company	Seattle, WA
Williams, Al	Security Business Solutions	Rixeyville, VA
Williams, Peter	Valicert, Inc.	Mountain View, CA
Wilson, Deborah M.	Wilson Scientific Computing	Arlington, VA
Wilson, John H.	Intel Corporation	Hillsboro, OR
Wilson, Stephen	PriceWaterhouse Coopers LLP	Sydney, NSW, Australia
Wims, Mike	Utah Attorney General's Office	Salt Lake City, UT
Windley, Lawrence E.	Delaware Secretary of State's Office	Dover, DE
Winn, Jane Kaufman	Southern Methodist Univ School of Law	Dallas, TX
Wittow, Mark H.	Preston Gates & Ellis, LLP	Seattle, WA
Wolff, Rupert	Wolff, Wolff & Wolff	Salzburg, Austria
Wong, Norman	GOC Communications Security Establishment	Ottawa, ON, Canada
Wood, Robert Y., III	Alston & Bird LLP	Atlanta, GA
Wrosch, Tom	Oregon Secretary of State's Office	Salem, OR
Yaich, Virginie	Service Central de la Securité d'Info	Paris, France
Yang, Wendy	VeriSign, Inc	Mountain View, CA
Yeo, Matthew S.	Steptoe & Johnson LLP	Washington, DC
Yukins, Christofer R.	Holland & Knight LLP	Falls Church, VA
Zeichner, Lee M.	LegalNetWORKS, Incorporated	Falls Church, VA
Zisko, William E.	Tomlinson Zisko Morosoli & Maser LLP	Palo Alto, CA
Zubeldia, Kepa	Arcanvs	Kaysville, UT

B. PKI OVERVIEW

B.1 The Need For PKI and PKI Assessment

With the rapid deployment of electronic commerce and communications globally, the security of electronic transactions and records has become a pivotal concern. To exploit fully the inherent advantages of the Internet and other computer networks, and to promote the continued growth of e-commerce, the following needs must be addressed:

- reliable methods for authenticating the identity and authority of individuals and organizations communicating electronically;
- reliable methods for providing assurances of the integrity of electronic communications and records and detecting unauthorized modifications to them;
- reliable methods for the protection of electronic messages and records against interception, unauthorized access, and the disclosure of confidential or sensitive information within them;
- reliable methods for controlling access to sensitive information and ensuring that only properly authorized parties have such access;
- a legally-robust system to prevent parties from successfully repudiating electronic transactions, messages, and records; and
- the adequacy of particular technologies, including PKI, to comply with emerging legal mandates.

PKI demonstrates great promise as a leading method for satisfying these requirements. A PKI-based digital signature provides authentication and integrity, while PKI-based encryption provides confidentiality. A PKI can also support efforts to control access to sensitive information and provide critical evidence tying a transaction, message, or record to its originator. In general, PKI can provide a solid technical and legal foundation for secure e-commerce and communications.

The rapid proliferation of different types of PKI has created a critical need for this document. Those who rely on PKI or are charged with overseeing PKI providers must be able to judge the quality and trustworthiness of a particular PKI. In addition, PKI providers must be able to assess their own operations in order to maximize efficiency and trustworthiness. While the process of PKI assessment may be complex or resource-intensive, there is a mounting consensus that the benefits outweigh the costs. Whatever the motivation for assessing a particular PKI, those involved in an assessment need the right tools to make accurate judgments.

B.2 The Technology Behind PKI

This section summarizes some of the information about PKI technology appearing in PAG APP 3, § 3.1 (Tutorial on Public Key Technology) to allow the reader to have a brief overview of the technology. For more details, *see id*.

The underlying technology that makes PKI applications possible is asymmetric, or "public key" cryptography, which uses two mathematically related "keys" (strings of bits) to encrypt and decrypt electronic data. One key can be made public without compromising the security of the corresponding key, which the key holder keeps private. Symmetric cryptography, by contrast, uses a single key for all cryptographic functions. *See* PAG APP 3 (Tutorial). PKI technology encompasses a broad range of disciplines, including asymmetric cryptography, symmetric cryptography, key management, and other cryptographic protocols.

An *electronic signature* is "an electronic sound, symbol, or process attached to or logically associated with a[n electronic] record and executed or adopted by a person with the intent to sign the record."[15] A *digital signature* is a specific type of electronic signature, created using PKI technology.[16]

A *digital certificate* is an electronic record, generated by a certification authority, containing (among other things) a certificate subscriber's name and public key and other designated information. It is used by the recipients of digitally-signed messages to verify the signatures on the messages for the purpose of authenticating their senders, having assurances of their integrity, and ultimately providing evidence tying the senders to the messages. A digital certificate can also facilitate the encryption of confidential information and help enforce access controls to sensitive information.

A *public key infrastructure*, or PKI, is the sum total of the organizations, systems (hardware and software), personnel, processes, policies, and agreements that allow public key technology to function for a given set of users. Individuals, businesses, governments, and other organizations have adopted many different kinds of PKIs around the world. The term *infrastructure* also refers to a common architecture or foundation on which generic applications (e.g., general e-commerce transactions, file servers, directories, e-mail, calendars, encrypted tunnels setting up virtual private networks) and business applications (e.g., word processing, spread sheets, publishing, contract management, electronic form retrieval, time management) can be securely implemented and operated.

Perceived and actual lack of security in electronic transactions can impede the advancement of global e-commerce. PKI technology provides critical security functions that the Internet was not designed to provide and, indeed, cannot provide. These functions include, but are not limited to, certificate status services, archiving, time stamping, business resumption services, and risk management mechanisms, including legal provisions for the apportionment of risk (such as indemnities, warranties, disclaimers of warranty, and limitations of liability).

B.3 PKI Components

PKI components are the elements that comprise a public key infrastructure, including entities (such as CAs) and individuals (such as subscribers) participating within the system, technologies (such as algorithms and key generation software), processes (such as key management procedures), records (such as digital certificates), and policy instruments (such as CPs and CPSs). In order to help the reader more fully understand the scope and viability of the assessment process, this section describes several important PKI components.

The common entities that participate within a PKI are:

- Certification authorities (entities that issue certificates),
- Subscribers (individuals and/or organizations operating the private key corresponding to the public key within the certificate),
- Relying parties (individuals and/or organizations relying upon the certificate to use the public key within that certificate),
- Registration authorities (individuals and/or organizations assisting a CA to authenticate the identity and/or other attributes of a certificate applicant, initiating the revocation of certificates upon a

[15] *See* PAG APP 2 (*Uniform Electronic Transactions Act (UETA*), § 2(8), U.S. Nat'l Conf. of Comm'rs on Uniform State Laws (NCCUSL) (13 Dec. 1999), *available at* <http://www.law.upenn.edu/bll/ulc/uecicta/eta1299.htm>, hereinafter "UETA"). A PKI digital signature is a "process" meeting this definition, and is therefore a type of electronic signature.

[16] *See* EU Signature Directive, *supra* note 5. Legislation that recognizes other security technologies besides PKI often uses the term electronic signature broadly, rather than digital signature; under such legislation, digital signatures are generally considered to be a particular type of electronic signature.

subscriber's request or otherwise, and approving or rejecting requests to renew or rekey a certificate), and

- Repositories (entities and/or organizations providing publication, storage, and access to certificates and other PKI-related information).

The participants within a PKI use the PKI technologies to establish a secure infrastructure to issue certificates, collect certificate applications, validate those certificate applications, issue certificates, publish or distribute certificates, revoke certificates, renew or rekey certificates, and ultimately decommission the infrastructure. The participants use these processes consistent with security policies and practices.[17]

B.4 PKI Documentation

This section summarizes some of the information about PKI technology appearing in PAG APP 3, § 3.3 (Tutorial on PKI Documentation) to allow the reader to have a brief overview of the types of documents commonly used to support PKIs. For more details, *see* PAG APP 3, § 3.3 (Tutorial on PKI Documentation).

The four main types of documents particular to PKI business arrangements are:

- Certificate policies. A certificate policy or "CP" sets forth general requirements that PKI participants must meet in order to operate within a PKI. Typically, a CP also describes the appropriate uses for certificates and the kinds of individuals and organizations that can participate in the PKI. A CP is particularly appropriate for promoting the interoperation of multiple certification authorities.

- Certification practice statements. A certification practice statement or "CPS" typically is a comprehensive statement of practices and procedures followed by a single CA or single organization's set of CAs. Where the PKI is governed by a CP, which sets forth general requirements, a CPS can be used to explain how a CA meets the requirements appearing in the CP. Where a PKI includes only a single CA, and interoperation is not necessary, the PKI can set forth its practices and procedures in a CPS. A CPS deals with the same kinds of subjects that appear in CPs, but a CPS is typically more detailed than a CP. While a CP's purpose is establishing requirements, a CPS is oriented towards disclosure of practices and procedures.

- Subscriber agreements. A subscriber agreement is an agreement between a subscriber on one hand and a CA or RA on the other. The subscriber agreement focuses on the subscriber's responsibilities and the terms and conditions under which the subscriber may use the subscriber's certificate.

- Relying party agreements. A relying party agreement is typically an agreement between a party that wishes to rely on a certificate and the CA that issued the certificate. A relying party agreement governs the terms and conditions under which the relying party is permitted to rely upon the certificate. Most commonly, the agreement requires the relying party to check the status of the certificates in the chain of certificate upon which he, she, or it wishes to rely.

- Other types of PKI documents are described in PAG APP 3, § 3.3 (Tutorial on PKI Documentation).

[17] For a more extensive discussion of PKI components and what they do, *see* PAG APP 3 (Tutorial on Public Key Technology).

B.5 PKI Interoperation

When different CAs or entire PKIs wish to interoperate, PKI documentation becomes the main tools to facilitating that interoperation. First, the interoperating organizations may wish to establish minimum operating requirements in a certificate policy. The organization coordinating the entire PKI can require that CAs agree to meet the requirements of the CP as a condition of becoming part of the PKI. Alternatively, interoperating organizations having a peer-to-peer relationship can agree among themselves to the terms of a CP by entering into a bilateral or multilateral interoperability agreement. Interoperation may include, but need not necessarily entail, CAs issuing certificates to each other (cross-certification) or one CA issuing a certificate to another CA without receiving a certificate in return (unilateral certification). Other forms of interoperation are possible, though, and may not involve the certification of interoperating organizations. For instance, interoperation may consist only of making certificates and certificate status information available to the different organizations participating within the PKI.

When an organization operating a PKI considers including a new CA within its PKI via cross- or unilateral certification, the organization will likely want to review the new CA's CPS to determine whether the CA's practices and procedures meet the minimum requirements of the PKI typically appearing in the PKI's CP. CAs wishing to interoperate via cross-certification or unilateral certification on a peer-to-peer basis may also want to view each other's CPSs to determine if their practices are compatible and provide equivalent levels of assurances. Judgments of this kind are typically made by looking at the elements within a CA's CPS and comparing them element-by-element with the standard against which the CPS is judged, that is, either the CP governing the entire PKI or the other CA's CPS.

Besides the straight policy-element-by-policy-element mapping process of legal and business requirements or practices, an assessment comparison must be performed of security mechanisms or practices. This assessment comparison is used to assess the adequacy of the mechanisms of one domain's practices to others. For example, the "medium" policy level of the U.S. Federal Bridge CP requires the use of a FIPS 140-1 level 2 cryptographic module and the "Class 3" policy level of the U.S. DOD CP also requires a FIPS 140-1 level 2 cryptographic module. While both policy levels may appear equivalent, the mechanisms and practices required to comply with each policy may differ greatly. Because multiple factors may be involved in determining certificate assurance levels or allowed certificate usages, believing that two policies are equivalent only from their identification is highly dubious, and should be avoided. The application environment that a CP covers is also a critical factor in the comparisons. In some environments the identity mechanism used by the CA may be more important than the rating of the CA or users' cryptographic module. Or, if significantly different, the mechanism used to protect the private key of the user may impede a certificate's use in certain applications. There is currently no universally-accepted way of performing a comparison between two CPs, between two CPSs, or between a CP and a CPS either to assess their security, or more specifically to assess the risk tradeoffs of various options.[18]

Completion of the policy and practice comparison does not necessarily resolve interoperability issues. Indeed, differing technical issues such as cryptographic algorithms key sizes, or complex differences in the underlying legal regimes such as those between the common law and civil law legal systems of the two entities (seeking interoperation) thwart easy comparison.[19] Nonetheless, interoperating organizations will ultimately need to make decisions as to whether one set of practices is roughly equivalent to another in terms of assurance levels based on the exercise of sound judgment. Where one set of practices falls short in comparison with another, it

[18] The Extensible Markup Language (XML) provides many of the functions necessary for comparing CPs. XML is an information technology standard that was developed by the (W3C) World Wide Web Consortium and published in 1998. XML is part of the family of "markup languages," that is, languages designed to facilitate a standardized, non-proprietary method for structuring and exchanging information. *See* PAG APP 7 (PKI and XML).

[19] *See, e.g.*, PAG APP 2 (*CA-CA Interoperability White Paper*, PKI Forum, Technical Work Group (TWG), (2001) *available at* <http://www.pkiforum.org/resources.html>, hereinafter "TWG White Paper").

may nonetheless include compensating controls that make up for the shortfall and permit the two practices to remain equivalent in assurance levels.

B.6 PKI Assessment

PKI assessments fall into two basic categories, those performed prior to a PKI commencing operations and those performed periodically to ensure ongoing compliance[20] with the CP, CPS, or other applicable documents. One example of the former is a Common Criteria (CC) evaluation performed by information security professionals. An example of the latter is an internal audit of an operational system performed by an auditor working for the system owner/operator. *See* PAG APP 4 (PKI Audit Methodology and Guidelines).

Before further addressing the assessment process, note that the development and justification of particular assessment requirements can be quite complex. Also, particular requirements may appear arbitrary and tangential to specific e-commerce business goals because regulatory requirements may not keep pace with the marketplace, and represent a necessary compromise between uniformity and administrative manageability.

B.6.1 PARTICIPANTS

Although assessment processes do vary, their structures and procedures may involve some or all of the following actors:

- PKI Service Providers – CAs, RAs, as well as ancillary service providers (or Managed Security Service Providers (MSSPs)), are typically the targets[21] of a PKI assessment effort.
- Assessors - An assessor is an entity that determines whether a PKI system complies with the criteria contained in the CP, CPS, and/or other applicable documents, such as assessment guidelines. Assessors might be approved to perform only certain types of assessments. Some examples of assessors are:
    - a laboratory performing technical evaluations of security components,
    - a certified public accounting (CPA) firm,
    - a certified information system security professional (CISSP),
    - a computer security professional, such as a certified information system auditor (CISA),
    - a law firm or an individual attorney with PKI legal expertise,
    - a governmental or quasi-governmental agency,
    - a for-profit organization, such as the International Computer Security Association (ICSA),[22]
    - an individual performing a self-assessment while investigating PKI deployment,
    - a non-profit organization such as the Open Group's *X*Open[23] or the Alliance for Electronic Business' tScheme in the UK,[24] and

[20] *See* Washingon Admin. Rules, *supra* note 7.

[21] *See, e.g.*, PAG APP 5 (Proposed Guidance for Development of Compatible End-User Product).

[22] *Available at* <http://www.icsa.com>.

- casualty insurance underwriters.

- Policy authority – Although not a direct participant, a policy authority will be involved at the periphery of PKI assessment as a result of having adopted a CP for a particular class of certificates applicable to a particular community, either by creating the CP or approving an externally created CP.[25]

- Accrediting body - An accrediting body can provide explicit approval for an organization or individual to perform a function but does not necessarily participate directly in the assessment of the PKI. Two different classes of accrediting bodies are envisioned by the PAG, assessor accreditation and PKI accreditation. A given body may perform both functions, or separate bodies may exist for each function. For example, an accrediting body may approve an assessor to perform a certain type of assessment, or approve the operation of a PKI system. Depending on the environment, such a body can either establish an assessment process or seek to conform to an existing assessment regime. Examples of accrediting bodies include:

  - Common Criteria evaluation and validation scheme (CCEVS) of the National Information Assurance Partnership (NIAP), which approves laboratories to perform Common Criteria (CC) technical evaluations and certifies the results of these evaluations;[26]

  - Electronic Health Network Accreditation Commission (EHNAC); and[27]

  - Internet Corporation for Assigned Names and Numbers (ICANN).[28]

- Subscribers and relying parties – A PKI could require that its subscribers and relying parties satisfy designated requirements, such as implementation of specific security capabilities; satisfactory completion of courses in computer security, PKI, and e-applications; or holding professional qualifications. Under some schemes, e.g., those based on "foreign recognition of certificates,"[29]

---

[23] *Available at* <http://www.opengroup.org>.

[24] *Available at* <http://www.tscheme.org.uk>.

[25] For example, Canada's Policy Management Authority (PMA) is a policy adopting body that creates CPs for a particular community (the Canadian government's PKI). Note, however, that a PMA or other policy adopting body is not a necessary element of a PKI.

[26] *See* EU Signature Directive, *supra* note 5, art. 2, § 13, ("'voluntary accreditation' means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body").

[27] EHNAC, is an independent, not-for-profit accrediting body. Its mission is to: "promote standards, quality service, innovation, cooperation and open competition within the healthcare EDI industry." Furthermore, it: 1. establishes minimum criteria for industry self-regulation, 2. encourages firms in the industry to improve performance, 3. facilitates open market access and competition ("open access" referring to acceptance of transactions from any source or routing), 4. fosters consistency in transmitted information, and 5. enhances customer service and satisfaction ("customers" include providers, payers, intermediaries and third parties), *available at* <http://www.ehnac.org>.

[28] *Available at* <http://www.icann.org/policy_statement.html>.

[29] Under one model of foreign recognition, PKIs are cooperating without cross-certification. Instead cooperation is achieved when PKI A acts as relying party to PKI B, and relies on certificates from the PKI B when issuing new certificates. In this scheme a PKI can issue a new certificate for an entity having a certificate in another domain by just studying the existing certificate. The advantage is that the entity can be easily updated with new certificates and that the need for interdomain cross-certification can be eliminated. The problem with this model may be that the number of certificates handled by PKI is increasing. This may however be successfully handled in various ways if client products and protocol usage is well-structured. (Continued next page)

the relying party is responsible for making the complete trust decision. In such cases, the required competency of relying parties may be considerable.

B.6.2 ASSESSMENT PROCESS

Figure B-1 presents a very basic PKI assessment process.

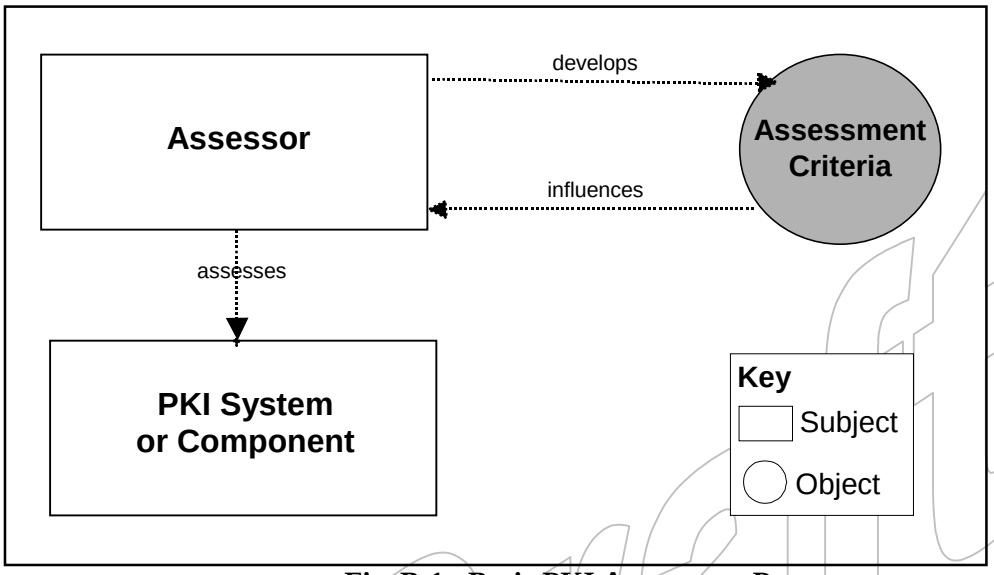


Fig. B-1: Basic PKI Assessment Process

PKI assessment can be undertaken at differing levels of *formality* and *independence*. The formal requirements for an assessment will define the level of competence required of assessors (including requirements for professional certification), the overall rigor of the assessment, the extent of the assessment's documentation, and the scope of the attestations provided by assessors. Similarly, these requirements will determine the extent to which assessors must be independent of the owner/operator of the PKI. This range of formality and independence extends from self-assessment by the PKI owner/operator to technical evaluation by an independent, approved laboratory.

- Self-Assessment – Assessments can be undertaken, in whole or in part, by the owner/operator of the PKI's target of evaluation (TOE). Such assessments are often called "self-assessments." The lack of independence inherent in self-assessments may limit their trustworthiness. Yet, a combination of self-assessment and periodic third-party assessment may provide a particularly efficient and cost-effective regime. Additionally, where the self-assessment is performed by an owner/operator with an established "pedigree," the combination of self-assessment with third-party oversight may result in a high level of assurance. The ability to establish this pedigree is critical to the effective use of self-assessment for other than lower assurance needs.

Footnote 29, continued. *See* EU Signature Directive, *supra* note 5, art. 7 (foreign legal recognition of a non-EU certification-service-provider can be obtained in any EU member state if (a) the certification-service-provider meets the requirements of the Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or (b) another certification-service-provider provider within the Community which fulfills the requirements of the Directive guarantees the certificate; or (c) pursuant to a bilateral or multilateral agreement between the Community and others establishing such recognition).

- Formal Evaluation – A formal evaluation is a technical assessment by an approved laboratory against a rigorous requirement set. Sources for such requirement sets include the Common Criteria and other computing security criteria sets.

Figure B-2, below, presents a more detailed and complete assessment process than that appearing in Figure B-1. This figure illustrates that the primary actors directly involved in PKI assessment are:

- Assessors
- The party responsible for the CA system being assessed

The primary actors interfacing with the PKI assessment are:

- Policy authority. This body has the authority to specify the certificate policy (CP) that is to be implemented by the PKI element or component to be assessed.
- PKI accreditation body. This is the body responsible for making the management decision either to (1) grant approval to operate or (2) provide official indication of compliance with necessary requirements.
- Assessor Accreditation Body. A recognized accrediting body may accredit an assessor. Such a body will typically be concerned with the competence and impartiality of assessors for the purpose of enhancing the correctness and completeness of the assessment process. Furthermore, the PKI accreditation body may require assessor accreditation.

Primary inputs to the assessment process include:

- Certificate policy (CP). Functions for approving a CP are not diagrammed, other than indicating that often a policy authority comes into play. A CA within the PKI, however, might approve its own CP, perhaps with a particular market segment or user group in mind. The processes for CP creation and approval may be outside the PKI, which can be viewed as an implementation of a specified policy. The PKI may also create and approve a CP through its own policy authority and be used to assess the PKI.
- Assessment criteria. The assessment is conducted against specific criteria that can come from various sources as indicated in PAG § C.5.3 (Relevant Legislation).
- PKI standards. Various standards for PKI implementations are expected to be applied in the implementation of the PKI being assessed.

The PKI assessment model comprehensively focuses on:

- PKI information technology, and
- the procedures and operations used to meet the requirements of a CP.

These elements of a PKI are usually documented in the PKI's CPS.

Extent of the PKI being assessed. It is generally a decision of the PKI accrediting body, at its discretion, as to the scope of an assessment, both in breadth and depth. Several examples that are consistent with the PAG are:

- Assessing a certification authority (CA).
- Assessment of a registration authority (RA) by a CA, or other party.

- Assessment of PKI capabilities at the subscriber or relying party level.[30]

The primary output from the assessment process is an assessment report that indicates and substantiates a pass or fail. The prime audience of the report is the PKI accreditation body. Additionally, the report can be used by PKI users in determining whether a specific PKI meets their needs.

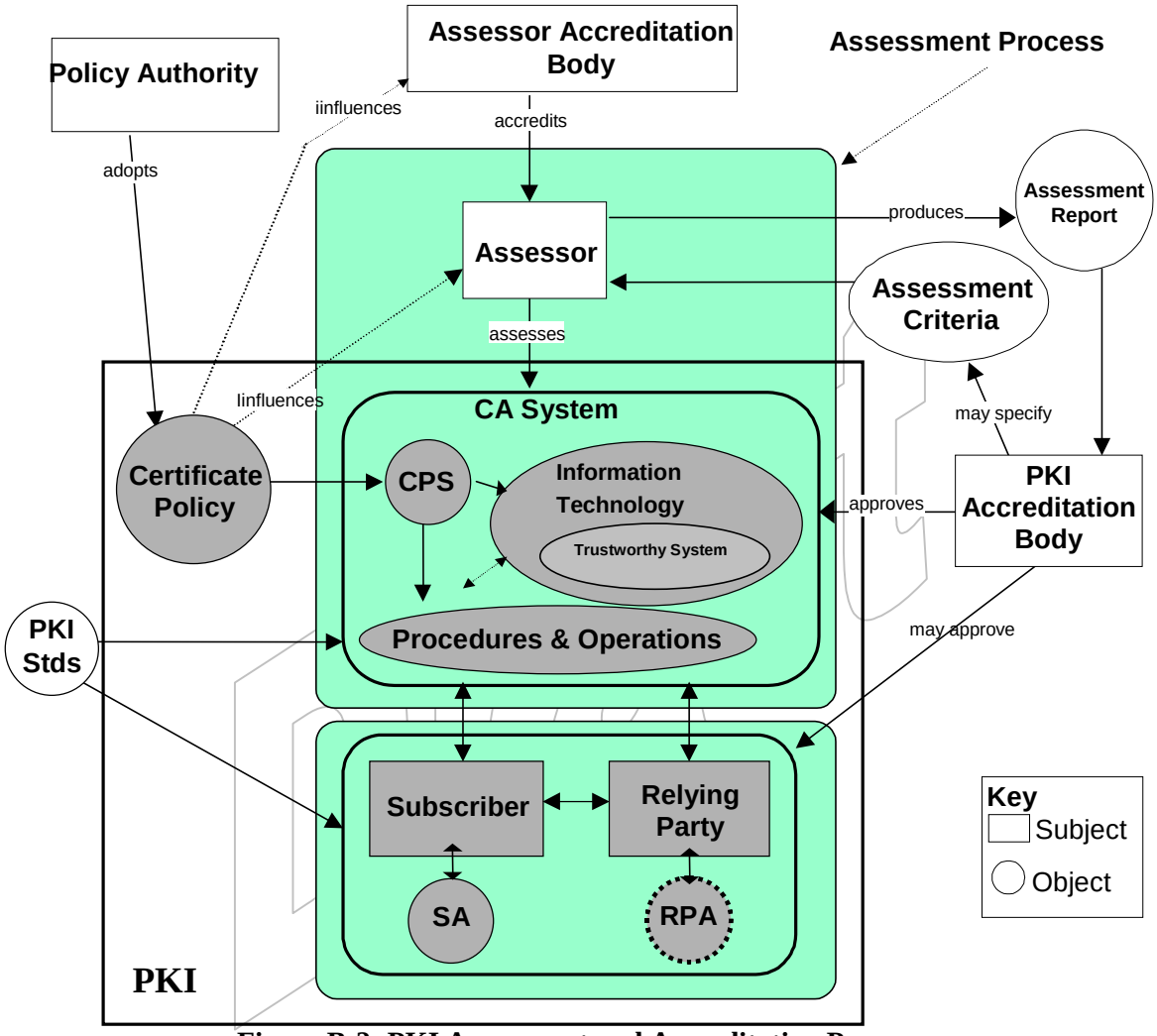


Figure B-2: PKI Assessment and Accreditation Process

B.6.3 ASSESSMENT CRITERIA

B.6.3.1 Methodology for Criteria Selection

Business and regulatory requirements generally determine or greatly influence the criteria[31] used for assessing a particular PKI. Such criteria are typically influenced by various factors, including:

- available technologies and services,

[30] This is expected only when the subscriber or relying party is under the authority of the PKI accrediting body.

[31] *See generally* PAG APP 2 (*Secure Electronic Commerce*, Warwick Ford and Michael Baum, pp. 433-467 (Prentice Hall, 2nd ed. 2001), hereinafter "Ford"), presenting an overview of PKI Assessment and Accreditation.

- the results of risk analyses,
- legal responsibilities,[32]
- the applications intended to be secured,
- mandatory standards and voluntary guidelines, and
- provider and user policies.

Factors unique to specific PKI models will also impact the nature of the assessment. These factors include:

- the PKI model itself (i.e., centralized, distributed, supporting single vs. multiple applications and jurisdictions),
- the PKI security/trust services (e.g., digital signatures, encryption, secure access, support for nonrepudiation),
- the level(s) of assurance required, and
- the extent to which a "critical infrastructure" is present (*see* "Critical Infrastructure Protection" below).

B.6.3.2 Sources of Assessment Criteria

Assessment criteria should be based principally on answering the question, "does the PKI faithfully implement the Certificate Policy that it is asserting?" Assessment criteria must also address the business and security demands of the organizations serving, and served by, a particular PKI. Criteria can derive from both private and governmental domains and can be manifested from different sources, including but not limited to the following:

- CP – The CP is typically the highest-level operative requirements document within a PKI.
- CPS – The CPS typically provides the second level for assessment purposes, since the assessor bases its control objectives on, or otherwise ascertains the implementation requirements and purported assurances provided by the PKI through, this document.
- Relevant agreements – Agreements may establish requirements for PKIs. Such agreements include subscriber, relying party, interoperation, and reciprocity agreements.
- Security policy – A security policy and other security and control documents, including security procedures and control objectives, may also be a source of ascertaining requirements.[33]

[32] *See infra* PAG § D.2.1 (Apportioning Legal Responsibilities and Liability Among the Parties to a PKI Transaction).

[33] *See* PAG APP 2 (*Criteria for Accreditation of Certification Authorities*, v. 9, Australian National Office for the Information Economy (Feb. 2001) p. 8, *available at* <http://www.govonline.gov.au/publications/CA_AccreditationCriteria_v9.pdf>, hereinafter "Gatekeeper Criteria"). The Security Policy states "what protection is needed for the system and information it is to process." An evaluator will base its security policy evaluation on three criteria: confidentiality, integrity, and availability. *See* PAG APP 2 (*Security Guidelines for Australian Government IT Systems*, § 2, Annex B, Australian Communications Security Instruction No. 33 (ACSI 33), *available at* <http://www.dsd.gov.au/infosec/acsi33/acsi_index.html>, hereinafter "ACSI 33"). The Gatekeeper program also requires a Protective Security Plan, which is a description of "the practice of ensuring the security and integrity of the overall operation of the CA service, including the establishment of standards for the access and operation of CA service elements." *Id*.

- Certificate management control objectives – Such objectives should be criteria applied to a PKI in connection with an audit or other assessment.

- Legislation and regulations – Legislation including PKI-specific laws and regulations, general "electronic signature" rules, as well as application- and market-specific rules, which may specify and incorporate standards and guidelines by reference.

- Standards – Standards for the assessment of information security systems have become critical to the assessment process. It is expected that the most influential and important will be the Common Criteria. Also of great importance to PKI (because of their extraterritorial influence) are U.S. Federal Information Processing Standards such as FIPS 140-1.[34]

B.6.3.3 Common Criteria

Background

As global reliance on PKI grows, there is a corresponding need to provide independently-verifiable assurances of a PKI's trustworthiness. The use of recognized standards is an important means of objectively specifying the criteria governing such an assessment.[35]

With respect to assessment of Information Technology (IT) security functionality and the technical trustworthiness of IT, two standards are widely accepted and anticipated to play a significant role in the future. These standards are the European Union's Information Technology Security Evaluation Criteria (ITSEC)[36] and the Common Criteria Project's Common Criteria for Information Technology Security Evaluation (CC). Of these two, the CC is the most likely candidate for long-term future use. In fact, a CC evaluation of CA products may be a requirement asserted in a Certificate Policy.

The Common Criteria has been adopted by security establishment organizations in a growing number of countries, including Canada, France, Germany, the Netherlands, the United Kingdom, Australia, New Zealand, and the United States. Additionally, the CC has been adopted by ISO as standard 15408, further increasing the likelihood that a certification awarded by one country or industry sector will utilize the CC as the underpinnings of foreign recognition.

Overview

The CC is essentially a catalogue of security requirements with identified dependencies. Requirements are given for security features (or functionality) and for security assurance (defined as grounds for confidence).

Functional requirements are provided for the following areas:

- Audit

- Nonrepudiation

[34] *See supra* PAG § B.5 (PKI Interoperation). Because of the growing importance of the CC to PKI assessment (as demonstrated by its inclusion in the German Digital Signature Regulation and the Australian Gatekeeper Methodology), an introduction to the CC is presented below.

[35] *See* Gatekeeper Criteria, *supra* note 33 at 12. One criterion for accreditation under the Gatekeeper program is "[c]ertified CA and RA Technology, ITSEC E3 (or Common Criteria)." Accreditation requires a Functionality Specification in conformance with ACSI 37 and Section 11 of the Supplement to ASCI 37 – SSM-1 System Security Mechanisms.

[36] *See* PAG APP 2 (*Information Technology Security Evaluation Criteria (ITSEC)*, Council Recommendation 95/144/EC (7 April 1995), a*vailable at* <http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/SecurityIssues.html#ITSEC>, hereinafter "EU Recommendation").

- General cryptographic features
- Protection of user data
- Identification and authentication
- Management of security functionality
- Privacy
- Protection of security functions and their data
- Resource usage
- Controlling access to the target of evaluation (TOE)
- Trusted communications between user and TOE and between TOE and other IT

In addition to functionality, the CC provides requirements for the following assurances:

- Configuration management
- Delivery and operation
- Development requirements
- Guidance documents (for user and administrator)
- Life cycle support
- Testing
- Vulnerability assessment
- Maintaining assurance level
- Evaluating protection profiles and security targets, i.e. Common Criteria requirement sets

The Protection Profile

The CC also provides common constructs for defining security requirement sets. The protection profile (PP) is the basic vehicle for specifying these requirements.[37] The PP captures a security design through several levels of refinement, as follows:

- The starting point for a PP is a description of the security capability desired by a mission or business process owner.
- This security capability is refined into a description of the TOE, clearly identifying the nature of the TOE and the boundary between the TOE and its environment.

[37] *See* PAG APP 2 (*Certificate Issuing and Management Components (CIMCs) Protection Profile*, v. 2.1, ISO/IEC 15408 (26 Jan. 2001), *available at* <http://csrc.nist.gov/pki/documents>, hereinafter "CIMCs Profile"). NIST has developed a Certificate Issuance and Management Component (CIMC) Protection Profile specifically for PKI components.

- The problem is further refined into a description of the security environment surrounding the TOE. The security environment includes a definition of the policies to be met and the threats to be addressed, as well as a list of the significant assumptions made in the production of this PP.

- The environment description is now refined into a set of top-level security objectives for the TOE and its environment. These objectives serve to facilitate the development of requirements by identifying the strategy to be used in meeting the policies and addressing the threats in light of assumptions made.

- Specific security requirements for TOE function and TOE assurance are now given, being driven by the security objectives.

The Security Target

As a statement of user need, the PP is a natural starting point for requirement definition with the CC. The next step is the development of a security target (ST) that, like the PP, is a document outlining security requirements and accompanying rationale. The ST extends the PP by adding the specific details of an implementation meeting the requirements of a PP. This is accomplished by tailoring the sections of the PP as needed to apply it to a specific implementation and by adding a new section capturing another level of refinement, namely a TOE summary specification that is in essence a functional specification for a specific TOE meeting the PP security requirements.

While the ST is a logical follow-on to a PP, the ST can also be the starting point by capturing an existing design in the CC construct. This provides a common structure for expressing security capabilities, greatly improving the ability of the user community to interpret vendor claims. The ST also provides the vehicle for vendor claims to be readily evaluated by third-party assessment.

Evaluation Assurance Levels

The CC provides one additional feature, a set of seven pre-defined assurance packages termed Evaluation Assurance Levels (EALs). The approximate relationship between these EALs and assurance levels from other criteria is shown in Table 1. The other criteria described are: ITSEC (European Information Technology Security Evaluation Criteria)[38], TCSEC (US Trusted Computer System Evaluation Criteria)[39] and the CTCPEC (Canadian Trusted Computer Product Evaluation Criteria).[40] Note that for TCSEC, this relationship is to the assurance elements in the TCSEC class without regard to the functions called out. The ITSEC is only an assurance specification and the CTCPEC, like the CC, separates functions from assurance.

CC	ITSEC	TCSEC	CTCPEC
EAL1	-------	-------	-------
EAL2	E1	-------	-------
EAL3	E2	C2	T-1
EAL4	E3	B1	T-2
EAL5	E4	B2	T-4
EAL6	E5	B3	T-5
EAL7	E6	A1	T-6

Table 1 – Approximate Assurance Correspondence

[38] *See* EU Recommendation, *supra* note 36.

[39] *Available at* <http://www.radium.ncsc.mil/tpep/library/tcsec>.

[40] Information on the Canadian Security Establishment and the Canadian approach to the Common Criteria is *available at* <http://www.cse-cst.gc.ca>.

IT evaluation under the Common Criteria

The formal, technical evaluation of PKI IT will only be one part of an overall PKI assessment since a CC technical evaluation does not assess procedural, personnel, and other non-technical issues.

A CC evaluation has three primary actors:

- Scheme. The scheme provides oversight of the evaluation, issues the approval for the assessor to perform that evaluation, and confirms the results of an evaluation.
- Sponsor. The sponsor is the individual or organization that contracts with the evaluation laboratory for the conduct of the evaluation. Generally this is the author of the requirement set (PP) or the developer of the IT being evaluated, although others can be the sponsors.
- Laboratory. The laboratory is the assessor who will perform the evaluation as a business contract with the sponsor. The laboratory is approved specifically by the national scheme to perform such evaluations.

Upon successful evaluation under a national scheme, the information technology evaluated is certified as meeting an identified requirement set and is placed on the national evaluated products list (EPL). This in turn would, presumably, be one requirement that the PKI system must meet in order for the accrediting body to approve the system.

A likely scenario for the PKI evaluation under a national CC scheme is:

- the PKI system approval authority specifies a specific Common Criteria protection profile (PP) as the requirement set to which the PKI IT must conform,
- this PP is evaluated to insure that it is a correct and complete requirement set. The PKI system approval authority is a likely sponsor for the PP evaluation,
- a PKI IT developer/owner/operator produces an ST claiming conformance to the PP,
- PKI IT developer/owner/operator contracts with an approved laboratory to have the ST and the PKI IT (the TOE) evaluated,
- the laboratory coordinates with the scheme to ensure that the planned evaluation meets all scheme requirements,
- the laboratory performs the evaluation and provides a report to the scheme, and
- the scheme reviews the evaluation report and determines whether to place the IT on the scheme's EPL.

B.6.4 GRANULARITY AND MODULARITY

Assessment of a PKI typically includes a range of topics. For example, the categories provided for in RFC 2527 represent a categorization of topics that can be divided into component assessments where the aggregation of those components could actually form the comprehensive assessment. Separate assessments may be required by other certified organizations or individuals to ensure correct management, change control, and backup of mission-critical systems. The sum of these individual assessments may provide a level of assurance sufficient for final accreditation of the entire PKI. However, assessment of any subsystem or component of that PKI should not necessarily be influenced by a failure to gain approval in any other subsystem or component. Rather,

inter-component/subsystem impact, including dependencies and acceptable compensatory controls, should be assessed within the context of the overall PKI. In other words, discrete component assessment or multiple component assessment alone is ineffective without assessing each component's effect on the system's trustworthiness.

Before undertaking an assessment, a great deal of information must be available and well understood, including but not limited to the following:

- provider and community-of-interest requirements and usages of trade (as expressed in agreements and other documents),
- applicable electronic and digital signature rules, adjudication, and local requirements,
- the methods of the applicable accreditors or standards measurement group,
- preparatory requirements for events to be instigated by the assessor and corresponding accreditor, and the anticipated timeline and flow chart for such events, and
- the PAG and related guidelines.

A complete assessment can incorporate the results of individual technology and product assessments to ensure that the applicable products are installed, configured, and operated securely. Also, the assessment must ensure that valid, assessed version of the products are deployed. *See* PAG APP 8 (PKI Assessment Examples).

B.6.5 LARGER ISSUES OF ASSESSMENT

B.6.5.1 The Role of Risk Management

Risk management underlies the development of assessment criteria and can also be used in the assessment process. Risk management within a PKI combines technical controls with policy, procedures, and physical controls to enable the PKI to function with the level of trustworthiness required to adequately manage and mitigate risk. Establishing the working definition of "adequately" is an essential part of the risk management process. The process should concentrate on the operations environment and should document the risk management approach used, including a description of relevant policies procedures, controls, assessments, recovery plans, audits, and all material risks faced by the PKI.

In some respects, the methodology may parallel that of risk analyses in the insurance industry, where categories of risk are created and certain events are identified and linked to them. Combining human, logical, and technological factors, the probability that certain events may occur is evaluated to determine potential risks, which are then compiled to form a PKI risk profile. The risks identified are then managed cross-functionally. For optimal results, this process should be periodically (if not continually) reevaluated.

As PKI business and technical requirements evolve, the inherent risks are likely to change. Consequently, a comprehensive risk management program must contemplate evolving issues to ensure that potential gaps in coverage are effectively identified and managed.

B.6.5.2 Critical Infrastructure Protection

The rapid and ubiquitous spread of modern information technologies has brought about considerable changes in the nature of economic transactions. The Internet has created significant personal, organizational, and infrastructure dependencies that are not confined by national borders. The Internet is, in essence, a "backbone

of backbones." It is a system of networks that are not centrally administered for quality control, that are complex, and whose functions are devoid of clear parameters. The growing codependence of public and private organizations on common systems, networks, and commercial hardware and software is increasing the risk related to ownership of these infrastructures. Our common dependence on a decentralized network makes it exceptionally difficult to determine where accountability and responsibility should reside for strategic vulnerabilities.

Resolving internet infrastructure challenges must include legal steps – both domestic and international – that will assist national security forces and the private sector in improving both defenses against cyber attacks and preventive measures to counter cyber threats as they become apparent, but before they cause harm. There is a pressing need for uniform, dependable approaches to the recovery of communications and information systems that have been harmed during a cyber-incident. In order to create a forum in which such approaches can be formulated, a collaborative dialogue between the public and private sectors needs to build an information-sharing system that protects private-sector participants from antitrust and tort liability, as well as from private-sector trade secret leakage. It is also important to note that numerous legal constraints exist in the realm of international collaboration in addressing and countering cyber threats and prosecuting cyber attacks. Additional information about the current limitations on, and status of, national and international legal development can be obtained from the Critical Infrastructure Assurance Office (CIAO).[41]

At the same time, globalization and the advent of the Information Age have empowered individuals, national subgroups, and non-state actors to begin to assess the Internet's vulnerabilities for the purposes of protecting their interaction with the infrastructure and at times, unfortunately, for the purposes of exploiting these vulnerabilities. When determining the approach to assessment that is most appropriate in a given case, it is important to consider global developments in the area of critical infrastructure protection. When a PKI is adopted for use within a highly sensitive environment, or an environment that is critical to an organization's success, additional assessment criteria may apply. While a PKI itself can be the infrastructure that requires protection, it can also be a tool in the protection of other infrastructures. CAs active within industries that rely on critical infrastructure need to attend to developments within these industries. Such developments may occur through the activities of self-regulating organizations or information-sharing committees (ISACs) within these industries that establish procedures for audit, standards for insurance underwriters, methodologies for operating in a cross-border environment, and certification practices for members of these industries. At the time of writing, the newly-formed Information-Technology ISAC is one example of a body whose activity should be monitored for its relevance to assessment in a given environment. Over time, it is also possible that trusted service providers such as CAs may establish their own procedures for monitoring appropriate criteria for particular environments.

When assessing the proper controls of a PKI, it is important to consider global developments in the area of critical infrastructure protection. When a PKI is adopted for use within a highly sensitive environment, or an environment that involves national security, an additional set of assessment criteria may apply. It is important to recognize that while a PKI itself can be the infrastructure that requires protection, it can also be a tool in the protection of other infrastructures. PKI service providers active within industries that rely on critical infrastructure need to attend to developments within these industries and within critical infrastructure initiatives that impact their operation. Such developments may come about through the activities of self-regulating organizations or information-sharing committees within these industries that establish security standards, procedures for audit, standards for insurance underwriters, methodology for operating in a cross-border environment, and certification practices for members of these industries. Over time, it is also possible that these trusted-service providers may establish procedures for monitoring the controls for these environments. This section covers factors that should be considered when establishing specific compliance criteria for systems under evaluation.

[41] The United States' National Plan for Critical Infrastructure Protection, *available at* <http://www.ciao.gov>.

C. LEGAL ISSUES PREFACE

The reliability of any PKI application (whether based on digital signature, encryption, or user authentication) depends on: *technical issues relating to security controls that* implicate software, hardware, and processes; particularly the *legal responsibilities* of the participants; the *legal liability* of the participants resulting from a breach of those responsibilities; and *legal remedies* available to redress wrongs and reimburse damage caused by such breach. Many of the *technical* aspects of PKI have been studied, discussed, and documented for decades and are relatively familiar.[42] On the other hand, the real-world *legal* implications of PKIs did not surface and advance until messaging, EDI, and the World Wide Web became deployed to an extent sufficient to enable widespread e-commerce.

The PAG § C (Legal Issues Preface) provides an overview of legal concepts as they interrelate to PKI. More legal commentary is set forth in PAG § D.2 (General, Legal and Business Provisions), substantially consistent with RFC 2527 § 4.2, General Provisions. This section C is intended as a "backgrounder" to facilitate a fuller understanding of the legal principles applied to PKI issues in section C.2. This legal preface identifies and surveys six legal subjects that are fundamental to a properly functioning PKI. These are as follows:

- PAG § C.1 – Sources of Law
- PAG § C.2 – Agency Principles
- PAG § C.3 – Evidence and Expert Witnesses
- PAG § C.4 – Foundations and Presumptions
- PAG § C.5 – Consumer and Privacy Issues
- PAG § C.6 – Risk Management and Insurance

C.1 Sources of Law

The legal rights and responsibilities of the parties to a PKI transaction derive from many sources, including:

- *PKI documentation*, including certificates, CPs, CPSs, subscriber agreements, relying party agreements, system and other rules that are incorporated by reference, and interoperability or cross-certification agreements, not all of which may be present in every PKI;
- If the transaction is entirely governed by the laws of a *single jurisdiction* within a common law or civil law regime, the *governing body of law* of that jurisdiction, expressed variously by constitutions, codes, legislation, regulations, evidentiary and procedural rules, and judicial decisions considered to be substantive precedent for future cases;
- If the transaction involves *more than one jurisdiction*, and the laws of those jurisdiction are in conflict, the *choice of law* principles provided by legislation, regulations, and judicial decisions that determine which jurisdiction's body of laws is applicable;

[42] The History of Non-Secret Encryption, *available at* <http://www.cesg.gov.uk/about/nsecret/home.htm>.

- *Bodies of law governing multiple jurisdictions*, including international law and treaties between nations, uniform and model acts adopted in multiple jurisdictions,[43] overarching federal laws governing in tandem with laws of the constituent or member states, provinces, or nations, and bilateral, multilateral, and regional cooperation agreements and agencies among certain states, provinces or nations related by geography and common interests;

- *Interpretations of laws* by various dispute resolution authorities such as courts, arbitrators and mediators;

- The participants' *prior course of dealing* with each other;

- *Custom or usage of trade* generally or in particular industries, as well as sectoral codes and other self-regulatory practices; and

- *Secondary sources* providing pertinent commentary, analysis, opinions, and suggested guidelines as to legal issues as yet undecided, such as the PAG and the DSG.

Concepts from the various sources of law become easier to understand and apply when organized under substantive areas or subjects of law grouped around unifying principles. Some substantive areas of law pertinent to PKI transactions are:

- **Contract -** A *contract* is "a promise or a set or promises for the breach of which the law gives a remedy, or the performance of which the law in some way recognizes as a duty."[44] A contract may or may not be based on a written *agreement*,[45] and it may be *express* or *implied*.[46] In PKI agreements, clauses that express *contractual responsibilities* of a party include representations, warranties, and covenants.[47] *Contractual liability* is the consequence of breached contractual responsibilities, and is subject to *liability limitation* provisions in the contract. In some PKI transactions, it may be legally significant which of the parties to the transaction are parties to the same contract, sometimes referred to as being in *privity* with each other. For example, a subscriber and a CA are typically in privity with each other, but under some business models, a relying party may not be.[48] Where the CA and relying party are not in privity, the contract would directly bind the CA and subscriber (and the RA if there is one) but would affect the relying party only indirectly, as a *third-party beneficiary* of the contract.[49] Thus, contract provisions limiting the

[43] Particularly applicable to PKI and digital signatures is the recently published UNCITRAL Draft Model Law on Electronic Signatures. *See* PAG APP 2 (*Report of the Working Group on Electronic Commerce*, UNCITRAL, 37th Sess., U.N. Doc. A/CN.9/483 (6 Oct. 2000), *available at* <http://www.uncitral.org/english/sessions/unc/unc-34/483e.pdf>, hereinafter "UN 2001 Model Law"). An updated version of both the 2001 Model Law and the Draft Guide to Enactment was produced in late January, 2001. *See* PAG APP 2 (*Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures*, UNCITRAL, 38th Sess., U.N. Doc. A/CN.9/WG.IV/WP.88 (30 Jan. 2001), *available at* <http://www.uncitral.org/english/workinggroups/wg_ec/wp-88e.pdf>, hereinafter "UN Draft Guide").

[44] Restatement (Second) of Contracts, § 1 (1979).

[45] "An agreement is a manifestation of mutual assent on the part of two or more persons…." *Id.*, § 3.

[46] "Express and implied contracts. Contracts are often spoken of as express or implied. The distinction involves, however, no difference in legal effect, but lies merely in the mode of manifesting assent. Just as assent may be manifested by words or other conduct, including silence, so will intention to make a promise may be manifested in language or by implication from other circumstances, including course of dealing or usage of trade or course of performance. " *Id.*, § 4, comment a.

[47] *See supra* PAG § D.2.1 (Apportioning Legal Responsibilities and Liability Among the Parties to a PKI Transaction).

[48] In a credit card business model, one party (the credit card issuer) who is in privity with all of the other parties serves to create privity among all the parties.

[49] "The doctrine of privity means that a person cannot acquire rights or be subject to liabilities *arising under* a contract to which he is not a party. It does not mean that a contract between A and B cannot affect the legal rights of C indirectly." *See* PAG APP 2 (*The Law of Contract*, G.H. Treitel (8th ed. 1991) p. 538, hereinafter "Treitel").

liability of the CA and subscriber towards a relying party that is not in privity with them would need to be couched in terms of conditions or limitations upon the rights granted to the relying party as a third party beneficiary, and not as liability limitations to which the relying party has agreed. Responsibilities can also be imposed upon parties in situations where an enforceable contract does not exist, but misrepresentations by one party have induced detrimental reliance by another party, with the effect that the first party is *estopped from denying* the accuracy of the misrepresentations.[50]

- **Tort** – Tort law is another potential source of *responsibilities* of PKI participants. The common law principle of *tort* is defined as a "civil wrong for which a remedy may be obtained, usually in the form of damages . . . ."[51] There are a number of different causes of action under which behavior of the defendant alleged to be wrongful or tortuous may; result in *tort liability* to compensate the plaintiff for damages suffered. These are: *negligence* (failure to act with reasonable care under the circumstances where a duty of care exists), *recklessness* (acting without regard for the consequences), *strict liability* (situations where there is liability for plaintiff's damages without the need to demonstrate that defendant was at fault), and *intentional tort* (the defendant intended to commit acts that damaged the plaintiff). Unlike contractual responsibilities, *tort responsibilities* can be breached without there being any express or implied agreement. In a transaction where a relying party is not in contractual privity with a CA, and therefore has not agreed to provisions in the contract limiting the CA's liability, a damaged relying party might prefer to seek recovery under a tort theory such as negligent misrepresentation, rather than under a contractual theory such as a third party beneficiary theory.

Common Law and Civil Law Regimes. In analyzing the legal responsibilities of the parties to a PKI transaction, it is important to know which jurisdiction's laws govern the transaction, and further, whether the laws of that jurisdiction are based upon a common law regime or a civil law regime. Most Anglo-American jurisdictions fall within the common law regime -- the collection of legal principles developed by English, US, Canadian, Australian, and other common law courts in response to actual cases presented before them, and used as precedent to decide future cases. Superimposed on the common law are statutes enacted by legislatures, both at the state and national level. In civil law jurisdictions, however, statutory codes such as the Code Napoléon, rather than to court-made rules, serve as the set of fundamental rules and background law.

Many nations, states, and provinces of the world are governed or influenced by a civil law regime.[52] There are a number of differences in substantive law between common law jurisdictions and civil law jurisdictions. For example, civil law regimes grant less recognition (or none whatsoever) to the doctrines of constructive notice, incorporation by reference, and the rights of third party beneficiaries than is typical in common law regimes. The concept of self-authenticating documents tends to be more robust in civil law countries than in common law countries. In civil law countries, a notation in a notaire's journal, even if not readily accessible to the public, is considered a public record and given effect as such. Civil law principles of agency tend to give relatively more

[50] A possible PKI example of estoppel is a case presenting this factual situation: (i) the subscriber's private key is stolen and used by an imposter, (ii) the subscriber fails to instruct the CA to revoke her certificate within a reasonable time after discovery of the theft and (iii) the relying party relies, to his detriment, upon the subscriber's unrevoked certificate. Even in the absence of an enforceable contract between the relying party and the subscriber, the relying party might argue that the subscriber's failure to timely revoke the certificate constitutes a continuing misrepresentation that the private key is uncompromised – a misrepresentation that the subscriber is estopped to deny. If the subscriber is a consumer, such arguments on behalf of subscriber liability to the relying party would appear stronger if the subscriber's conduct is reckless or intentional. Presumably such arguments in favor of subscriber liability would be weaker if the PKI roles were reversed, so that the relying party is a consumer and the subscriber is not. For example, in the case of a digitally-signed insurance policy, the insurance company would typically be the subscriber, and the consumer beneficiary or insured seeking to enforce the policy would be the relying party.

[51] Black's law Dictionary 1496 (7th ed. 1999).

[52] Examples of civil law regimes include most of the nations of the European Union, all Latin American nations, Mexico, the Canadian Province of Montreal and the U.S. State of Louisiana. Some predominately common law jurisdictions adhere to certain civil law institutions or traditions, such as use of Latin Notaries in the UK and elsewhere for international transactions.

weight to the existence of the agent's actual authority to bind the principal, and relatively less emphasis to the agent's apparent authority, than do common law regimes.

C.2 Agency Principles

Many PKI participants carry out functions as *agents* for other participants. Accordingly, the basic principles of *agency* law are an essential foundation for the assessment of the PKI's scheme of legal responsibilities and liability of its participants.

C.2.1 THE CONCEPT OF AGENCY

Agency is a legal relationship between two parties, *principal* and *agent* that can arise under both contract and tort law. Under the agency relationship, one party (the agent) has the authority to act on behalf of another (the principal), and any acts by an agent on behalf of the principal legally bind the principal. An agent's authority may be limited in scope -- for example, limited to certain types of transactions or to a monetary limit. The principal-agent relationship may be created orally or in writing, although certain types of agency relationships must be in writing to be enforceable. Examples of agency include (i) a corporate officer with authority to sign contracts on behalf of a corporation, and (ii) a partner of a partnership signing a contract on behalf of a partnership.

Agency involves the *delegation of duties* and the agent's power to create and alter legal relationships between the principal and third parties.[53] The principal authorizes the agent to perform duties on behalf of the principal that are within the scope of the agent's *authority*. The agent's authority is either *actual authority* expressly given to him by the principal, *implied authority* derived from the position or office held by the agent,[54] or *apparent authority* arising from circumstances that cause third parties to reasonably believe the agent has actual authority to serve as agent of the principal. When acting within his authority (whether actual, implied, or apparent), the agent has the power to legally obligate his principal to a third party.[55] Alternatively, a principal might be liable for *agency by estoppel* by carelessly allowing third parties to believe that a party is actually acting as the principal's agent, or by failing to take steps to correct third parties' impressions of such agency, once the principal becomes aware that a party is falsely claiming to be his or her agent.

Agency principles are common-sense rules that have evolved over time in common law jurisdictions, to the point where the rules operate predictably even if they are not expressed in written contracts.[56] Moreover, agency principles tend to be quite protective of the rights of third parties who are strangers to the agency

[53] Restatement (Second) of Agency, § 12.

[54] For example, a person having the office of president in a corporation has implied authority to bind the corporation in transactions made in the ordinary course of business. The role of president includes general managerial authority, and therefore entitles the person holding the office to enter into such transactions, even though the directors have not specifically authorized each and every one of these transactions.

[55] This doctrine, holding an employer or principal liable for the employee's or agent's acts committed within the scope of the employment or agency is known as respondeat superior, or "let the superior make answer." BLACK'S LAW DICTIONARY 1313 (7th ed. 1999).

[56] It should be noted that western and asian views of agency tend to differ, based on cultural differences. In the west, agency is often evidenced by a document such as power of attorney, with the agent attaching a signature on the authority of the principal. In Asia, agency is quite often practiced by the transfer of the signing device, chop or hanku, from the principal to the agent who then uses the signing device as agent. *See* PAG APP 2 (*Malaysia's Digital Signature Act* §§ 39, 48, *available at* <http://www.geocities.com/Tokyo/9239/digisign.html>, hereinafter "Malaysia's Signature Act"), which seems to permit agents to obtain, hold or use the principal's private key. Also, certain Asian cultures do not have the concept of individual property and any transactions are communal rather than individual. In such cultures, the sharing of private keys within a community or extended family might be common. *See* PAG APP 2 (*Issues Relating to the Use of Electronic Authencation: Executive Summary*, ¶¶ 111-114, APEC Telecomm. Working Group, *available at* <http://www.apii.or.kr/apecdata/telwg/eaTG/eaTG-2.htm>, hereinafter "APEC").

relationship, particularly if they have reasonably relied on apparent authority. For these reasons, agency principles are fundamental to many business relationships, such as employer and employee, contractor and subcontractor, partner and partnership, and corporation and officer. It is no surprise, therefore, that principles of agency law are relevant to the allocation of responsibilities and liability among participants in a PKI, the central focus of PAG § D.2, *infra*.

C.2.2 AGENCY AND PKI

The delegation of duties by a principal to its agent does not normally relieve the principal of its continuing responsibility to third parties for the performance of those duties. Thus, if a CA obtains an agent to act as an RA to perform certain "front-end" CA duties (such as the confirmation of a certificate applicant's identity prior to certificate issuance), such delegation does not normally relieve the CA from liability for damages suffered by a third party (such as a relying party), that are caused by the RA's errors. Subject to any contrary provisions set forth in an applicable CPS or agreement, the CA is liable for faulty identification of a subscriber whether the CA performed the work itself, or delegated it to an RA acting as the CA's agent. At the same time, if the error was the fault of the RA, the CA may seek reimbursement for any damages the CA is required to pay the third party, via the RA's *indemnification*[57] of the CA. The continuing liability of the principal notwithstanding delegation of CA duties to an agent causes the possibility of an RA's insolvency to be less important to end users (subscribers and relying parties) in a situation where the CA is a solvent and creditworthy "deep pocket." Granted, the competency of the RAs appointed by a CA always remains important for the smooth functioning of the PKI, but at the end of the day, the RA's future solvency is critical to the end users only to the extent that the CPS or agreement relieves the CA of liability for an error by an RA, or if the financial resources of the CA are limited.[58]

The relationship between a CA and RA, however, may not always be one of principal and agent. An agency relationship exists if the RA acts on behalf of the CA in dealing with third parties, such as certificate applicants. An RA, however, may be authorized to approve certificate applications based on searches of its internal databases of identity information and not deal at all with third parties. In that case, the RA is perhaps best viewed as a service provider or simply a party undertaking the performance of a covenant with another contracting party, rather than an agent. In fact, the CA-RA agreement in this example may even disclaim the existence of an agency relationship. In short, a CA's delegation of duties to an RA does not automatically create an agency relationship.

C.3 Evidence and Expert Witnesses

When a PKI is intended to support digital signatures for the purpose of authenticating a transaction or a communication that needs to be attributed to a particular subscriber, the digital signature does not by itself result in legal "nonrepudiation."[59] When a subscriber attempts to repudiate a transaction or communication, there may be factual and legal questions and disputes that, if not settled, will need to be resolved in litigation, arbitration, or other alternative dispute resolution mechanism, in order to determine whether the attempted repudiation is ultimately successful. The unique value of PKI is its *technological* ability to provide robust factual inferences

[57] Indemnification is the act of compensating for loss or damage sustained. BLACK'S LAW DICTIONARY 772 (7th ed. 1999).

[58] *See infra* PAG § D.2.3 (Financial Responsibility).

[59] The DSG describes nonrepudiation as, "Strong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents." *See* DSG, *supra* note 2, § 1.20.

[59] "The ISO Nonrepudiation Framework treats nonrepudiation as a technical definition of a security service. The Guidelines define nonrepudiation not as an automatic result of technical mechanisms, but as a property that can only be determined after recourse to available dispute mechanisms such as a court or arbitrator. The definition of nonrepudiation in this Guideline §1.20 is intended to express a legal conclusion or result which flows from the use of digital signatures verified by certificates in the manner provided in these Guidelines . . . . " *Id.*, § 1.20.1.

of nonrepudiation, through cryptography, that will serve to provide credible evidence sufficiently strong to persuade a disinterested third party (the ultimate dispute resolution authority), that a subscriber originated a particular transaction or communication. Once the legal proceedings produced a final judgment to that effect, then *legal* nonrepudiation has occurred. This section discusses how the proponent of evidence produced by a digitally signed transaction or communication could seek its admission at trial or another proceeding under established rules of evidence. More specifically, this section discusses additional threshold evidentiary questions: when expert testimony is necessary; how a witness might be qualified as an expert witness; and the types of testimony such an expert might present in the proceeding if admission of a PKI-related document is contested on authenticity or integrity grounds. This section also covers the admission of evidence in proceedings adjudicating disputes relating to applications of PKI other than digital signatures.

C.3.1 ADMISSIBILITY OF EVIDENCE RELATED TO PKI

The initial question is: through whose testimony can evidence of a digitally signed transaction be introduced? More specifically, is it sufficient to introduce such evidence through the testimony of a fact witness, such as a representative of the CA, technology vendor, relying party, or a third party, or is expert testimony required to supplement the testimony of such fact witnesses?

The advisory committee for the U.S. Federal Rules of Evidence addresses the issue of when expert testimony is appropriate in its comments associated with Rule 702:

> *Whether the situation is a proper one for the use of expert testimony is to be determined on the basis of assisting the trier. "There is no more certain test for determining when experts may be used than the common sense inquiry whether the untrained layman would be qualified to determine intelligently and to the best possible degree the particular issue without enlightenment from those having a specialized understanding of the subject involved in the dispute." Ladd, Expert Testimony, 5 VAND. L. REV. 414, 418 (1952). When opinions [of lay witnesses] are excluded, it is because they are unhelpful and therefore superfluous and a waste of time. 7 Wigmore on Evidence § 1918.*[60]

Due to concerns surrounding the reliability of opinion testimony, lay testimony that conveys opinions is generally prohibited under the common law.[61] Under the Federal Rules of Evidence, opinion testimony other than expert testimony is limited to those "opinions or inferences which are (a) rationally based on the perception of the witness and (b) helpful to a clear understanding of the witness' testimony or the determination of a fact in issue."[62] The limitation, fair or not, is in practice permitted or restricted as a matter of discretion by the trial judge.[63]

The Federal Rules of Evidence admit both expert and lay opinion. The chief difference is that the expert is freer to opine, particularly from facts of which he does not have personal knowledge. The increased latitude for expert testimony is justified by an ostensibly enhanced credibility based upon unique knowledge, training, and education. Rule 702 states, "If scientific, technical, or other specialized knowledge will assist the trier of fact to

[60] Fed. R. Evid. 702 advisory committee's note.

[61] *See* PAG APP 2 (*Evidentiary Foundations*, Edward J. Imwinkelried (4th ed. 2000) § 9-A, hereinafter "Imwinkelried").

[62] Fed. R. Evid. 701.

[63] *See United States v. Skeet*, 665 F.2d 983, 985-986 (9th Cir. 1982) (whether or not to allow lay opinion testimony is discretionary); *Hansard v. Pepsi-Cola Metro. Bottling Co.*, 865 F.2d 1461, 1467 (5th Cir. 1989).

understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise."[64]

Currently, PKI technology is an arcane and esoteric subject, as far as the general public (including most jurors, judges and attorneys) is concerned. Accordingly, the early cases involving PKI will most likely require considerable use of expert testimony to elucidate the technologic inferences it provides. This will likely change over time, just as automobiles and computers eventually emerged from the exclusive purview of hobbyists and engineers when first invented, to become familiar and ubiquitous tools within the public's common knowledge and experience. Until PKI use becomes commonplace, however, opinion testimony related to PKI technology or its application is likely to remain the exclusive province of expert witnesses.[65]

C.3.2 THE U.S. FEDERAL COURT APPROACH TO EXPERT EVIDENCE: DAUBERT AND KUMHO TIRE.

The framework for handling expert evidence in the U.S. Federal courts is set out in Article VII of the Federal Rules of Evidence, as interpreted by the Supreme Court in *Daubert v. Merrell-Dow Pharm. Inc*.[66] and in *Kumho Tire Co. v. Carmichael*.[67] Many state courts follow *Daubert* explicitly or in substance, but others[68] continue to apply the framework established in a 1923 decision of the United States Court of Appeals for the D.C. Circuit in *Frye v. United States*.[69]

Under *Daubert*, the proponent of scientific evidence must show that the evidence is both reliable and supported by "good grounds."[70] The *Daubert* benchmarks of reliability are: (i) adequate empirical verification of the validity of the theory or technique in question, and (ii) a sensible application of that theory or technique to the issue in controversy. Under the earlier *Frye* standard, the proponent was required to show that the theory or technique was generally accepted within the relevant scientific community.

The *Kumho Tire* decision expands the *Daubert* "gatekeeping" function from the "scientific" to the "technical," thus encompassing "the testimony of engineers and other experts who are not scientists" – perhaps to all witnesses purporting to testify about the specialized knowledge governed by Fed. R. Evid. 702.[71] *Kumho Tire* requires the court "to make certain that an expert, whether basing testimony upon professional studies or personal experience, employs in the courtroom the same level of intellectual rigor that characterizes the practice of an expert in the relevant field."[72] PKI technology involves both "scientific" issues such as the mathematics of public key cryptography (*see infra* PAG APP 3 (Tutorial), and "technical" issues such as security controls (*see, e.g., infra* PAG § D.6 (Technical Security Controls) and § D.5 (Management, Operational and Physical Security Controls). Accordingly, in the United States, expert testimony regarding PKI issues will undoubtedly implicate *Daubert* and *Kumho Tire* in U.S. District Courts and jurisdictions that have adopted the federal version of Rule 702, and in all likelihood, the *Frye* standard in other jurisdictions.

---

[64] Fed. R. Evid. 702.

[65] The foundation for an expert's qualifications may include related degrees; specialized training; licensure; practice in the field for a substantial period of time; teaching experience; authorship of publications on the subject; membership in recognized professional organizations; and previous testimony as an expert on the subject matter in question. *See* Imwinkelried, *supra* note 61, § 9-C; *see infra* PAG § C.3.4 (Qualifications of Expert Witnesses).

[66] 509 U.S. 579 (1993).

[67] 526 U.S. 137 (1999).

[68] *E.g., Donaldson v. Cent. Ill. Pub. Serv*., 730 N.E.2d 68 (Ill. Ct. App. 2000); *Logerquist v. McVey*, 1 P.3d 113 (Ariz. 2000).

[69] 293 F. 1013 (D.C. Cir. 1923).

[70] *Daubert*, 509 U.S. at 590.

[71] *See* Fed. R. Evid. 702 and accompanying text.

[72] *Kumho Tire*, 526 U.S. at 152.

C.3.3 APPLYING DAUBERT AND KUMHO TIRE TO PKI TECHNOLOGY AND END-USER APPLICATIONS.

There appears to be little serious doubt about the reliability, scientific integrity, and acceptance of digital signature and other PKI technology as fundamentally valid propositions of scientific and technological fact. A debate is more likely to arise when it is alleged that techniques or protocols were not applied reliably in a specific instance. *Daubert* requires not only "good grounds" to make a general scientific assertion, but also that testimony be reliable as applied to the facts of the particular case. Applied to PKI technology used in a typical digital signature situation, *Daubert* would require a witness proffering a digital signature to provide a reasonable basis for the trial court to admit that testimony into evidence. A reasonable basis would be a showing that PKI technology *as implemented by the end-user applications involved*, has probative value to authenticate the identity of the signer and to confirm that the integrity of the message remained intact. Conversely, a party opposing a digital signature would present expert testimony casting doubt upon either the ability of the PKI technology to authenticate identity or ensure integrity, or that the technology *as implemented by the end-user applications involved*, support authentication and/or the integrity of the message. For example, in a case where there is no dispute about the reliability of the underlying PKI cryptography, there might still be a dispute as to whether a compromise of the subscriber's private key could have or did in fact result in its use by an imposter.

Importantly, once evidence passes muster under *Daubert*, the court is considered to have made only a preliminary gatekeeping determination -- that the evidence is admissible and that the trier of fact should be allowed to hear it. The trier of fact, usually but not always a jury in the United States, retains the responsibility of making the ultimate determination of the facts in issue, whether as to identity of signer, integrity of document, or other contested fact.

As an example of encryption for confidentiality rather than a digital signature, a typical controversy might arise from the compromise of a consumer's personally identifiable private health information, or access to source code by an alleged infringer of software copyright. Such disputes might involve the issue of whether a message, admittedly encrypted *by an end-user application* using the recipient's public key contained in the recipient's certificate, was or was not capable of being decrypted by an eavesdropper lacking access to the recipient's private decryption key. As an additional example, a controversy arising from the end user application might be an allegation that there were acts by external hackers or bugs in the application program that caused the message to be sent "in the clear," despite an instruction to encrypt the message.

Once the Court is satisfied that expert witness testimony is sufficiently reliable under *Daubert* and its progeny, the trier of fact will decide the issue not only by considering the expert testimony, but also by considering the associated facts material to the dispute. Evidence considered could include lay witnesses' testimony about what happened, any paper documents involved, the electronic records, and all other facts necessary and relevant in order to determine whether confidentiality was or was not preserved. One possibility is that disputes involving PKI will not be based primarily on testimony as to the validity of the underlying technical principles of PKI, but rather on testimony demonstrating the trustworthiness of the technology as *actually implemented by the specific end-user applications involved* in the case. Evidence about the pure technology or theory, although novel at the outset, is likely to become a more tractable than the thornier mixed legal/factual question regarding the trustworthiness of the end-to-end implementations. Eventually, accumulated precedent and increased familiarity could lead to attorney and judicial acceptance of PKI technology, in the same manner as once novel radar technology for proof of motor vehicle speed eventually came to be accepted as a technological fact whose basic principles were no longer worth disputing.

C.3.4 QUALIFICATIONS OF EXPERT WITNESSES

Fed. R. Evid. 702 requires all experts to be "qualified." Witnesses in this area may need to demonstrate a number of different areas of expertise. In order to qualify as an expert to testify about the underlying mathematics of cryptography, a witness would need to exhibit a level of education, training, and experience related to mathematics and cryptography sufficient to pass the trial court's gatekeeping function relating to

unqualified expert witnesses. On the other hand, a witness qualifying more broadly as an expert in PKI design, implementation, operation, or assessment could, depending on the facts involved, be required to demonstrate their education and experience related to computer programming, computer and information security, hardware and software systems and applications, statistics, risk management, auditing or equivalent disciplines, mathematics, and cryptography. The nature and extent of the qualifications required under the rules will vary from case to case, given the discretionary nature of the court's preliminary "qualification" gatekeeping function.

C.4 Presumptions

This section discusses evidentiary presumptions under U.S. state law in favor of the authenticity of digital signatures and digitally-signed records, as well as the effect of the U.S. Federal E-SIGN Act[73]on such presumptions. Under such presumptions, a digital signature on a message that can be verified using a certificate is generally presumed to be the digital signature of the subscriber listed in that certificate. This section also discusses evidentiary presumptions outside of the United States.

C.4.1 THE BURDEN OF PROOF: "GOING FORWARD" AND THE "RISK OF NON-PERSUASION"

As a general rule of evidence, the proponent of a fact in a dispute has the *burden of proof* as to that issue.[74] Accordingly, in the paper-based world of commerce, a party relying upon a signature on a document generally is said to have the burden of proving the genuineness of the other party's signature, and the authenticity of the document on which the signature is found.

This loose concept of "burden of proof" actually has two separate components. First, there is the "burden of going forward" with competent evidence in support of a specific fact (sometimes called the *production burden*). Next, there is the burden of persuasion (also called the *risk of non-persuasion*), which is the concept colloquially known as the "burden of proof."[75] In the absence of any presumptions, if the proponent of a fact fails to introduce admissible evidence sufficient to meet the production burden, the trier of fact (a jury, or the judge in a non-jury trial) will not be allowed to consider that fact in making its decision, so that the burden of persuasion question is never reached. Once the production burden is met, the party opposing that fact has the opportunity to introduce evidence tending to disprove the fact, thereby creating a factual dispute. The trier of fact will then decide the truth of the fact, after considering all the evidence, guided by legal rule or instruction to the jury as to which party bears the risk of non-persuasion as to that fact. There are a number of different standards used to describe the quantum of proof required. "A preponderance of the evidence," "clear and convincing evidence," and "truth beyond a reasonable doubt" are three of them.

The proponent of a fact is almost always the party with both the initial production burden and the burden of persuasion.[76] This is true in the case of a party seeking to prove the authenticity of a disputed[77] signature on a

[73] *See* PAG APP 2 (*The Electronic Signatures in Global and National (E-SIGN) Commerce Act*, 15 U.S.C. § 7001 *et. seq.,* (enacted 30 June 2000, effective 1 Oct. 2000), hereinafter "E-SIGN Act").

[74] *See, e.g., Martinelli v. Bridgeport Roman Catholic Diocesan*, 196 F.3d 409, 428 (2nd Cir. 1999); *In Re St. Lawrence Corp*., 248 B.R. 734, 740 (D.N.J. 2000)("burden of proof rests on the party who has the affirmative of an issue").

[75] "[A] presumption imposes burden of going forward with evidence to rebut or meet the presumption, but does not shift to such party the burden of proof in the sense of the risk of nonpersuasion, which remains throughout the trial upon the party on whom it was originally cast." Fed. R. Evid. 301.

[76] The production burden may, under some circumstances, shift between proponent and opponent. The proponent of a fact might satisfy his proof of burden with evidence strong enough to shift the proof of burden to the opponent; the failure by the opponent to produce any controverting evidence might result in a jury instruction to find or assume the truth of the fact in reaching its decision.

signed document so that party can enforce the document according to its terms. If a plaintiff is suing a defendant to enforce a promissory note and the defendant disputes the signature, the plaintiff must first produce competent evidence that supports the authenticity of the signature on the document, in order to have the opportunity to persuade the trier of fact by a preponderance of evidence that the signature on the document was in fact made by the defendant.

C.4.2 ATTRIBUTION PRESUMPTIONS IN DIGITAL SIGNATURE STATUTES

On May 1, 1995, the Utah Digital Signature Law[78] was enacted, reflecting a similiarity with early drafts of the DSG[79], which was subsequently published in its final version by the American Bar Association on August 1, 1996. Both the Utah Law and the DSG set forth a presumption to the effect that a digital signature verified by reference to the public key listed in a valid certificate issued by a CA[80], is presumed to be the digital signature of the subscriber listed in that certificate.[81] This legal presumption is based upon a factual chain of inference: (i) a particular public key can verify its corresponding digital signature, (ii) a particular subscriber is linked to a particular public key because the the subscriber has been issued a certificate binding the distinguished name of the subscriber to the public key contained in the certificate, (iii) the particular public key used for verification is uniquely linked by cryptography with a particular private key used to create the digital signature verifiable by the public key and (iv) that particular private key is linked with a particular subscriber because the subscriber is the person having the sole possession and control of that private key. *See* PAG APP 3 (Tutorial).

With some variations, this evidentiary presumption under the DSG and the Utah Law in favor of the identity of the signer (i.e., that a digital signature verified by reference to the public key listed in a valid certificate issued by a CA is presumed to be the digital signature of the subscriber listed in that certificate) was followed by digital signature legislation in Washington,[82] Illinois,[83] Minnesota,[84] Singapore,[85] Malaysia,[86] and in the U.N. Commission on International Trade Law (UNCITRAL) Model Law on Electronic Signatures.[87]

---

[77] Under the Uniform Commercial Code, a signature is presumed genuine unless the genuineness is raised as a matter of defense. *See* U.C.C. § 3-308 (1990); *see also* PAG APP 2 (*Biometrics and Digital Signatures,* R. R. Jueneman and R. J. Robertson, Jr., 38 JURIMETRICS 427 (1998), *available at* <http://www.mcg.org.br/mirrors/digsig.pdf>, hereinafter "Jueneman"); *see* DSG, *supra* note 2, § 5.6.5; *see also* Reporter's Memorandum of D. Benjamin Beard (15 Aug. 1997), *available at* <http://www.law.upenn.edu/bll/ulc/uecicta/ect997.htm>, hereinafter "Reporter's Memo"), wherein it is mentioned that if the purpose of UETA is to establish legal equivalence between written records/signatures and electronic records/signatures, then UETA should not accord additional legal effect, through the use of presumptions, to the implementation of an electronic signature accompanied by a security procedure.

[78] *See* PAG APP 2 (*Uniform Electronic Transactions Act,* UTAH CODE ANN. § 46-3-406 (2001), *available at* <http://www.le.state.ut.us/~code/TITLE46/htm/46_02025.htm>, hereinafter "Utah Signature Act").

[79] *See* DSG, *supra* note 2.

[80] Under the Utah Law, the CA is required to be licensed by the State. *See* Utah Signature Act, *supra* note 78.

[81] *See also* U.N. 2001 Model Law, *supra* note 43, art. 6(3); U.N. Draft Guide, *supra* note 43, ¶¶ 117 – 118; DSG, *supra* note 2 § 5.6(2); and Utah Signature Act, *supra* note 80.

[82] *See* PAG APP 2 (*Washington Electronic Authentication Act,* WASH. REV. CODE § 19.34.010, 19.34.350(3)(a) (enacted 29 Mar. 1996, effective 1 Jan. 1998), *available at* <http://www.secstate.wa.gov/ea/ealaws.htm>, hereinafter "Washington Authentication Act").

[83] *See* PAG APP 2 (*Illinois Secure Electronic Signature Act,* 5 ILL. COMP. STAT. 175/10-120(b) (enacted 1997, effective 1 July 1999), hereinafter "Illinois Signature Act").

[84] *See* PAG APP 2 (*Minnesota Electronic Authentication Act,* MINN. STAT. § 325K.24, Subd. 1(c)(1), (enacted 19 May 1997), hereinafter "Minnesota Authentication Act").

[85] *See* PAG APP 2 (*Singapore Electronic Transactions Act,* § 18(2)(a) (1998), *available at* <http://www.cca.gov.sg/eta/part5.html>, hereinafter "Singapore Signature Act").

Under state digital signature statute presumptions, once certain minimal foundational facts are proved (i.e., use of the identified technology, proper protocol, etc.), then such a presumption in favor of the authenticity of a digital signature enables a relying party (the proponent of the signature) to efficiently satisfy the burden of going forward regarding authenticity. Thus, the presumption offers economy as to valuable court time. The production burden of evidence challenging authenticity then shifts to the subscriber (the opponent of the signature).

C.4.3 PRESUMPTIONS UNDER FEDERAL RULES OF EVIDENCE 301 AND 302

As introduced above, under Fed. R. Evid. 301, a "presumption" is "directed only to the burden of going forward with evidence," and "does not shift . . . the burden of proof in the sense of the risk of non-persuasion, which remains throughout the trial upon the party on whom it was originally cast." Conversely, Fed. R. Evid. 302 states the federal rule of evidence for presumptions where the substantive rule of decision is provided by state law. It states that "the effect of a presumption respecting a fact which is an element of a claim or defense as to which State law supplies the rule of decision is determined in accordance with State law."[88] This federal rule thus recognizes that presumptions about facts regarding state claims merely govern procedural efficiencies regarding proof, that are implemented in the federal courts by shifting the burden of going forward.

C.4.4 DIGITAL SIGNATURE PRESUMPTIONS ARE REBUTTABLE

Under the DSG, the Illinois Act, [89] and the Washington Act[90] the presumption in favor of the signature is expressly made rebuttable. The omission of the word "rebuttable" in the Utah Act should not be construed as causing the presumption to be conclusive. Similar to Fed. R. Evid. 301, under Utah Law, a "presumption" shifts the production burden rather than the persuasion burden, and an initial shift in production burden is nullified by the introduction of controverting proof.[91] Similarly, the EU Signature Directive[92] provides that "advanced electronic signatures" verifiable by reference to a "qualified certificate," if created by a "secure-signature-creation-device," are guaranteed to be admitted into evidence, but proponents of such signatures do not enjoy a presumption as to the identity of the signer.[93] Although the terminology is different, this EU rule resembles the treatment of a presumption under the Federal Rules of Evidence, in that the production burden is shifted but the risk of persuasion is not. During 2000 in Canada, Part 3 of the Federal Personal Protection and Electronic

[86] *See* PAG APP 2 (*Malaysia Digital Signature Bill*, § 67(b) 1997, *available at* <http://www.geocities.com/Tokyo/9239/digi5.html>, hereinafter "Malaysia Signature Bill").

[87] *See* Utah Signature Act, *supra* note 78; U.N. 2001 Model Law, *supra* note 43, U.N. Draft Guide, *supra* note 43, s*ee also* PAG § C.5 (Relevant Legislation).

[88] For Rule 302 rather than Rule 301 to apply, the presumption regarding the burden of proof must deal with a substantive element of the claim or defense versus application of state law for "tactical" presumptions. Therefore, an analysis would have to be performed as to whether a state's digital signature presumption provides a substantive element of the claim or defense. *See Erie Railroad Co. v. Tompkins*, 304 U.S. 64 (1938) and its progeny.

[89] *See* Illinois Signature Act, *supra* note 83, § 175/10-120(c).

[90] *See* Washington Authentication Act, *supra* note 82.

[91] *See, e.g, Buckley v. Francis*, 6 P.2d 188 (Utah 1931)(presumptions are evidentiary in nature creating a prima facie case and when the opposing party comes forward with controverting evidence the presumption is nullified). This type of presumption is sometimes referred to as a "bursting bubble" presumption.

[92] *See* EU Signature Directive, *supra* note 5; PAG § C.5.3 (Relevant Legislation).

[93] *See* PAG APP 2 (*European Electronic Signature Standardization Initiative (EESSI) Final Report to the European Commission*, EESSI Expert Team (20 July 1999), *available at* <http://www.ict.etsi.fr/eessi/Final-Report.doc>, hereinafter "EESSI Final Report").

Documents Act[94] enacted a variation of the Uniform Electronic Commerce Act[95] that addresses the evidentiary issues of secure electronic signatures in relation to the reliability of electronic documents and affiliated systems, but does not adopt any specific presumptions with respect to PKI or digital signatures. Some jurisdictions have also adopted other or additional presumptions, such as a presumption in favor of the message integrity of the signed document because "hash" technology protects against corruption and alteration of the data contained in the message.[96]

Examples of controverting evidence in the private key compromise situation that could be used to counter a rebuttable presumption in favor of a digital signature include evidence that: (1) the person named in the certificate has never had a key pair or a certificate, and therefore could have not been the signer; (2) the private key of the subscriber named in the certificate was used, but the subscriber introduces evidence in support of the fact that the signing was done without authority from the subscriber, either (3) under duress, or (4) without the subscriber's knowledge, following subscriber's compromise of her private key.

Once an opposing party introduces evidence of unauthorized use of her private key, the original "bursting-bubble presumption" in favor of the signature disappears because the production burden of both parties has been satisfied -- the burden of the proponent (the relying party) by the presumption, and the burden of the opponent (the subscriber), by coming forward with conflicting evidence. In the resulting "level playing field,"[97] the risk of non-persuasion would remain throughout the trial upon the relying party – the party on whom it was originally cast, unaffected by the initial presumption and its subsequent nullification, consistent with Fed. R. Evid. 301. The trier of fact would then apply the burden of persuasion as instructed by jury instruction or legal rule.

In the PKI context, it remains to be seen what legal rule will develop as to whether certain other PKI issues are legal issues to be decided by the court, or factual issues to be weighed by the trier of fact in accordance with legal rules or jury instructions. Such other issues frequently considered in the PKI world might include: (1) whether the subscriber violated her duty of care to avoid compromises of her private key; (2) whether the relying party's reliance on the certificate was reasonable under all the circumstances; (3) whether the subscriber promptly revoked her certificate upon discovery of a private key compromise; (4) whether the relying party freshly validated the certificate up the chain to the root certificate before relying; (5) whether a more prompt revocation or a more freshly-validated certificate would have made any difference by providing earlier notice of revocation in time to avoid reliance upon the certificate; and (6) equitable considerations, such as which of the two innocent parties (subscriber and relying party) was in a better position to protect both of them from damage at the hands of an imposter.

[94] *See* PAG APP 2 (*Personal Information Protection and Electronic Documents Act*, Bill C-6, 2nd Sess., 36th Parliament, 48-49 Elizabeth II, 1999-2000, House of Commons of Canada (Royal Assent 13 April 2000), *available at* <http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html>, hereinafter "Canadian Bill C6").

[95] *See* PAG APP 2 (*Uniform Electronic Commerce Act*, UNCITRAL Draft Uniform Rules on Electronic Signatures in Canada, Adopted by the Uniform Law Conference of Canada (30 Sept. 1999), *available at* <http://www.law.ualberta.ca/alri/ulc/current/euecafa.htm>, hereinafter "Canadian E-Commerce Act").

[96] *See, e.g.*, Illinois Signature Act, *supra* note 83 at 175/10-120(a); Singapore Signature Act, *supra* note 85, § 18(1); Washington Authentication Act, *supra* note 82, § 19.34.350(3)(c). Other presumptions in Utah and Washington are that: (i) the message was signed with the intent of signing the message (*see* Utah Signature Act, *supra* note 78, § 46-3-406(3)(b), Washington Authentication Act, *supra* 82, § 19.34.350(3)(b)); (ii) the certificate has been signed by the issuing CA (*id.*, § 46-3-406(1), § 19.34.350(1)); (iii) the certificate is accepted by the subscriber (*id.*, § 46-3-406(1), § 19.34.350(1)); and, (iv) the information in the certificate is accurate unless the certificate expressly states that it contains unverified information (*id.*, § 46-3-406(2), § 19.34.350(2)).

[97] After the rebuttal of the presumption has occurred, the procedural level playing field resembles the situation in the EU. *See supra* PAG § C.4.4 (Digital Signature Presumptions are Rebuttable), where a PKI digital signature presumption merely ensures admissibility of evidence of the signature, but has no effect upon the risk of non-persuasion.

C.4.5 THE EFFECT OF E-SIGN ON DIGITAL SIGNATURE PRESUMPTIONS

On June 30, 2000, the United States Congress enacted the Electronic Signatures in Global and National Commerce Act[98] ("E-SIGN"), effective October 1, 2000, governing transactions in or affecting interstate commerce. Section 101 of E-SIGN provides a general rule of validity to all electronic signatures used in interstate commerce. At the current time, in the absence of judicial precedent, the precise nature and extent of E-SIGN's effect on state digital signature laws is the subject of considerable scholarly inquiry.[99] Section 102 of E-SIGN prohibits the adoption of conflicting state laws to the extent they "accord greater status or legal effect to, the implementation or application of a specific technology" relating to electronic signatures or records.[100] Some have read section 102 as broadly preempting state digital signature laws (and nullifying presumptions about how digital signature evidence is treated in the courts of those states). Others read section 102 as limited strictly to state laws purporting to modify the rule of general validity stated in section 101, which does not mention presumptions.

In light of the discussions of presumptions above, is E-SIGN a broad technology-neutral mandate (i.e. the "broad preemption" view) intended to nullify such evidentiary presumptions because they "accord greater status or legal effect to, the implementation of a particular technology"? Or is this issue not even reached if a state law does not "modify, limit, or supersede the provisions of section 101" (i.e. the "narrow preemption" view)?

C.4.5.1 Broad Preemption or Narrow Preemption

Most proponents of both the broad and narrow preemption views agree that a state law recognizing only PKI digital signatures as valid "electronic signatures" would be preempted by E-SIGN because the state law is not technology neutral. However, whether a state digital signature law that grants presumptions to implementation of a PKI technology is preempted (assuming that all other provisions of section 101 are met and the state has enacted a standard version of UETA) remains a topic of discussion because of the somewhat ambiguous technology-neutral language of section 102(a)(2) of the E-SIGN Act.

Proponents of broad preemption additionally cite technology-neutral language in the legislative history of E-SIGN. They argue that digital signature laws like the Utah law, which provides presumptions in favor of digital signatures, "accord greater status or legal effect to, the implementation of a particular technology," and hence they are expressly preempted by E-SIGN.

[98] *See* E-SIGN, *supra* note 73.

[99] *See* PAG APP 2 (*Electronic Signatures in Global and National Commerce Act of 2000: Effect on State Laws*, Raymond T. Nimmer, *available at* <http://www.bmck.com/ecommerce/ueta-esign-2.doc>, hereinafter "Nimmer"); (*What Governors Need to Know About E-SIGN: The Federal Law Authorizing Electronic Signatures and Records*, National Governors Association, *available at* <http://www.nga.org/cda/files/000922ESIGN.pdf>, hereinafter "Nat'l Governor's Assoc."); (*Guidance on Implementing the Electronic Signatures in Global and National Commerce Act*, OMB, *available at* <http://www.whitehouse.gov/OMB/memoranda/m00-15.html>, hereinafter "White House"); (*E-Sign of the Times*, Robert A. Wittie and Jane K. Winn, *available at* <http://www.cybersecuritieslaw.com/KL/wittie.htm>, hereinafter "Wittie"); and (*A Preliminary Analysis of Federal and State Electronic Commerce Laws*, Patricia Brumfield Fry, *available at* <http://www.uetaonline.com/docs/pfry700.html>, hereinafter "Fry").

[100] *See supra* note 94 at § 102(a)(2)(A)(ii), 15 U.S.C. § 7002(a)(2)(A)(ii) (2000). The pertinent statutory language is:

"Exemption to Preemption. (a) In General. A state statute, regulation, or other rule of law may modify, limit, or supersede the provisions of section 101 with respect to state law only if such statute, regulation, or rule of law . . . (2)(A) specifies the alternative procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures to establish the legal effect, validity, or enforceability of contracts or other records, if . . . (ii) such alternative procedures or requirements do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures. . . . "

Proponents of narrow preemption argue that as long as the presumptions afforded digital signatures do not modify the basic rule in section 101 of recognizing all electronic signatures, E-SIGN does not apply. In other words, E-SIGN contains no specific intent language to preempt laws that establish presumptions about the authenticity or attribution of a signature or message, and as long as such presumptions do not modify section 101, section 102 does not apply. They also argue that states may provide presumptions about authenticity and integrity that allow digital signatures to be admitted in evidence upon minimal factual foundation.[101]

Regardless of which view, the broad or narrow preemption view, is adopted by the courts, as a practical matter it appears as of this writing that preemption may have little ultimate effect upon the use of PKI and the manner in which courts and fact triers will receive PKI evidence. First, as discussed above, PKI technology offers inherently strong factual inferences in support of attribution, which can take the place of a purely legal presumption to help the relying party satisfy its production burden and avoid adverse summary judgment. Second, once the relying party has met its production burden by introducing factually persuasive PKI digital signature and supporting expert testimony, a high percentage of cases may turn out not to involve any of the thorniest disputed factual issues (such as misidentified subscribers or compromise of private key) and thus, can be resolved relatively quickly. Third, those few cases that raise the thorny issues will require the fact trier to sift through so many issues and counter-issues, that the presence or absence of a legal presumption to satisfy the relying party's initial production burden will be unlikely to have a material impact on the burden of persuasion (the colloquial "burden of proof") one way or the other. Fourth, the impact of E-SIGN's preemption will be as limited as the scope of E-SIGN itself.

C.4.6 LIMITS UPON THE SCOPE OF E-SIGN'S COVERAGE[102]

The following are some exceptions to coverage of E-SIGN in the U.S. that are particularly pertinent to the PKI context. E-SIGN § 101(b)(1) excludes laws that relate to the rights and obligations of persons, other than requirements that contracts or other records be written, signed or in nonelectronic form. Another is section 102(b)'s exception to technological neutrality for laws or rules governing state procurement.[103] Moreover, E-SIGN does not preempt state laws that are within the scope of UETA (as approved and recommended for enactment by NCCUSL), nor does it prevent the parties to a transaction from expressly adopting digital signature presumptions and/or PKI as a "security procedure"[104] for attribution under section 9 of UETA. State laws containing provisions not related to the legal efficacy of electronic signatures, such as CA licensing schemes, remain unaffected by the enactment of E-SIGN. There are, however, potential consumer protection

[101] *See generally* Nimmer, *supra* note 99. It is argued that States, through legislative findings, may determine the amount of evidence needed to establish authenticity under newer technologies. This type of question is traditionally a matter left to state prerogative, not unlike the freedom of a state to apply its choice of standard for determining admissibility of expert testimony under the *Daubert*/*Kumho Tire* standard, or the earlier *Frye* standard. *See supra* PAG § C.3 (Evidence and Expert Witnesses). Moreover, it can be argued that digital signature presumptions are matters related to the "rule of decision" properly controlled by state law under Fed. R. Evid. 302, *see supra* PAG § C.4.3 (Presumptions Under Fed. R. Evid. 301 & 302), and thus were not intended by Congress to be preempted by federal law.

[102] It should be noted that E-SIGN is a law not applicable outside the U.S., and as of this writing, no jurisdiction outside the U.S. has enacted a law following the preemption and exception-to-preemption provisions of E-SIGN.

[103] Also, under section 104, a state or federal regulatory agency may interpret E-SIGN and specify standards to carry out the agency's statutory directives. While an agency may not require the use of a particular type of hardware or software, it can specify a performance standard or technical specification to address issues such as security, record integrity, signer authentication, and interoperability. Section 104(b)(3)(A) of the E-SIGN Act allows state and federal agencies to require, or accord greater legal status or effect to, a particular technology if it first finds that 1) the requirement serves an important government objective and 2) the implementation of that technology is substantially related to achieving that objective.

[104] "'Security Procedure' means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures." *See* UETA *supra* note 15, § 2(14).

issues that dictate adherence to careful disclosure and consent procedures when seeking to validate electronic records and signatures under E-SIGN, as discussed in section C.5, *infra*.

C.5 Consumer Issues and Privacy

Increasing concerns about Internet privacy and security have motivated people and businesses to seek stronger confidentiality and authentication over the Internet through the use of PKI technology. Nonetheless, PKI presents its own implications for the privacy of its users, and may raise issues concerning use by persons who may be considered "consumers" under applicable consumer protection laws. Given that PKI technology is largely designed to be as transparent as possible, it is probably safe to assume that many consumer end users and some, especially smaller-business users of CA products and services, will not be knowledgeable about the underlying PKI technology. Moreover, one cannot reasonably presume that all or even most certificate owners and users will routinely read and understand the complex and lengthy legal documents that usually govern the contractual relationships among the various parties in a PKI. Consequently, organizations that issue certificates must determine how best to inform and bind users, particularly those thought of as "consumers," as to their respective roles, responsibilities, and rights as functional "users" of certificates. Assessors of CAs or RAs should note how a CA or RA incorporates the use of information practices, especially regarding the information it receives from users of its services, and how the CA or RA may treat consumers from other entities.

Consumers ***are*** treated differently than business entities,[105] to some extent in most jurisdictions globally, most often statutorily by national, regional, or local consumer protection laws, and also by the courts in common law jurisdictions. Consumer protections internationally and in various sectors domestically range from compulsory disclosure requirements, to mandated privacy practices, to outright prohibitions on certain types of contract provisions that would be entirely legal (if not appropriate) in a business-to-business transaction. Moreover, local, national, and regional approaches to consumers and appropriate consumer protection differ between civil and common law jurisdictions, and among the various EU, North American, and Asian legal traditions.[106]

From a privacy and consumer law standpoint, PKIs are concerned with how information is used after it has been gathered for authentication purposes, as well as how information is published or otherwise made publicly available during the course of the certificate life cycle.[107] A PKI must also be concerned with how statutory or other legal consumer protections may affect its own business models and practices (such as its liability scheme) in a variety of jurisdictions, wherever its certificates have been sent or used. PKI service providers will thus need to be cognizant of being reviewed by assessors according to the requirements of appropriate national law.

This section is divided into three parts. The first part identifies the consumer framework in which PKI service providers may operate and a number of relevant issues that assessors might review. While the section focuses on consumer issues, references will be made to certain standards in a business-to-business context as well. Among the most important concerns that arise when a CA is operating in a consumer environment are consumer protection laws and guidelines, jurisdiction, forum selection and governing law, online contracting, language, oversight/consumer satisfaction/redress, and fair business practices. The second part outlines what is often referred to as the most important consumer issue: privacy. Although privacy is often considered solely a consumer issue, its effect on business-to-business *and* business-to-consumer operations places it more appropriately under a separate heading. This section ends with several short summaries on relevant legislation

[105] Business-to-business disputes are for the most part decided upon the basis of explicit contracts and/or trade usage. Courts provide greater latitude for businesses to decide for themselves, whereas they often attempt to protect consumers from adverse consequences of their actions.

[106] Some types of consumer information are considered more inviolable than others in certain legal jurisdictions. Europe and the United States do not have identical views as to what personal information is considered "sensitive." By way of example, in the United States, children's information is considered "sensitive" and subject to special protection, whereas, in Europe, certain types of employment data are particularly regulated.

[107] E.g., by publication of personal information in the certificate itself.

affecting consumer protection and privacy, including E-SIGN, the European Union E-Signatures Directive, the Canadian Privacy Act, the Gramm-Leach-Bliley Act, HIPAA, COPPA, and the Privacy Act of 1974.

C.5.1 THE CONSUMER FRAMEWORK

C.5.1.1 Consumer Protection Laws and Guidelines

The history of consumer protection in North America and Europe has seen, to varying degrees, the imposition of disclosure requirements and "deemed" contractual provisions. As mentioned earlier, attempts to protect consumers have run the gamut from requiring so-called "clear and conspicuous" disclaiming language, to a total prohibition on the use of particular products or services. Where legislative requirements permit some degree of choice in contracting, the perceived equality or inequality[108] of the parties to an on-line contract has also become important. Contracting for services related to digital certificates is often accomplished via on-line contracts. A number of variables exist as to what body of law governs and where redress can be obtained, *see infra* PAG § C.5.1.2 (Jurisdiction, Forum Selection and Governing Law).

Other consumer-specific issues arise in a digital certificate context. In some jurisdictions, legally-effective notice to a consumer of contract terms must be via actual notice.[109] Some regulations specify a minimum type size and other paper-based vestigial form requirements, while other jurisdictions require notice to be given in a particular language(s). Disputes may result from potential inconsistencies when combined with the extensive use of "click-wrap" agreements to bind parties electronically to a contract.[110]

A "reasonable expectations" doctrine has been widely used to interpret adhesion contracts (*i.e.*, those agreements in which one party can exert disproportionate amount of influence), such as insurance forms. This doctrine states that when contractual terms are onerous or were not reasonably expected, then contracts can be

[108] The equality or inequality of the parties may be due to many factors including, for example, technical capacity, knowledge, and negotiating power.

[109] Actual, rather than constructive notice is required in most civil law jurisdictions. This creates substantial issues related to incorporation by reference when one considers the limited amount of space available on a certificate. Also, on March 29, 2001 (effective March 30, 2001, compliance required by October 10, 2001), the U.S. Federal Reserve Board adopted an actual notice of approach in promulgating its "interim final rule" implementing E-SIGN to allow use of electronic notices to satisfy mandatory GLB privacy notification provisions under the five consumer protection regulations. *See* PAG APP 2 (*Uniform Standards for E-SIGN Act*, Federal Reserve System, 66 Fed. Reg. 17,329 (30 Mar. 2001), hereinafter "Fed. Reserve Standards"). In addition to the affirmative consent by the consumer to electronic disclosures as required by section 101(c) of E-SIGN, the interim final rule provides that disclosures made by GLB financial institutions to a consumer in any manner other then e-mail to the address supplied by the consumer (such as through a website), the institution must alert the consumer of the website disclosure by sending a notice via email or postal mail, and must make the website disclosure available for at least 90 days. *See* PAG APP 2 (Reg. B – *Implementations for the Equal Credit Opportunity Act*, 12 CFR pt. 202.17(d)(2), (hereinafter "Reg. B"); Reg. E – *Implementations for the Electronic Fund Transfers Act*), 12 CFR pt. 205.17(c), (hereinafter "Reg. E"); Reg. M - *Implementations for the Consumer Leasing Act*, 12 CFR pt. 213.6(d), (hereinafter "Reg. M"); Reg. Z - *Implementations for the Truth in Lending Act*, 12 CFR pt. 226.36(d), (hereinafter "Reg. Z"); and Reg. DD – *Implementations for the Truth in Savings Act*, 12 CFR pt. 230.10(a), (hereinafter "Reg. DD"), *available at* <http://www.federalreserve.gov/BoardDocs/Press/boardacts/2001/20010329>). The interim final rule for each of these consumer protection regulations also mandates that the format of disclosures must be "clear and conspicuous" and in a form that the consumer may keep. The institution must make a good faith effort to redeliver an e-mail disclosure that fails to reach the consumer's e-mail address, using address information in the institution's file.

[110] *See* PAG APP 2 (*Uniform Computer Information Transactions Act*, (formerly UCC art. 2B) U.S. Nat'l Conf. of Comm'rs on Uniform State Laws (23 Jul. 1999), *available at* <http://www.law.upenn.edu/bll/ulc/ulc.htm#ucita>, hereinafter "UCITA"). *See supra* PAG § C.5.1.3 (Online Contracting) and § A.4 (Organization and Use). In its E-SIGN interim final rule for electronic disclosures, the Federal Reserve Board allows institutions to provide disclosures in languages other than English, so long as English is also available. A consumer applicant must be required to access the E-SIGN disclosure prior to electronically signing the application. *See* Fed. Reserve Standards, *supra* note 109.

interpreted by courts to in such a way that they are deemed to be amended to make their provisions objectively reasonable.[111] Assessors of certification authorities may wish to take note of the possibility of CA adherence to this doctrine.

In terms of electronic commerce and on-line contracting, a recent and significant development for consumers has been the OECD's adoption of *Guidelines for Consumer Protection in the Electronic Marketplace*.[112] The OECD Guidelines suggest roles for businesses, consumers, and governments, as well as requirements related to the accuracy of information, electronic contract formation, consumer redress, online fraud, privacy protection, and consumer education.

Private sector use of technology (*e.g.*, through digital certificates) for authentication and encryption purposes will help build trust in the electronic marketplace and provide some measure of privacy protections for consumers.[113] At the time of this writing, there are few PKI-specific legislative or regulatory requirements for consumer disclosure,[114] but it would be best practice for CAs, particularly those that interact regularly with consumers, to take all reasonable steps to ensure full consumer awareness of obligations incurred with respect to the other participants within a PKI (*e.g.*, the certification authority; registration authorities and the repository).

C.5.1.2 Jurisdiction, Forum Selection, and Governing Law

As mentioned in PAG § C.5.1.1 (Consumer Protection Laws and Regulation), *supra*, one of the key legal issues is "jurisdiction." A number of variables exist as to what body of law governs, and where redress of disputes can be obtained, and the concept of "jurisdiction" is sometimes loosely used to refer to all such variables. Jurisdiction depends on whether the nature and extent of contacts between an entity and a particular jurisdiction (e.g., a nation, state, province, or other geographic subdivision) are sufficient under constitutional law or other notions of due process to subject the entity to legal process such as a summons from that jurisdiction to appear and respond to a lawsuit in that jurisdiction. A high profile legal issue today in both the business-to-business

[111] The concept of reasonableness, is a common law concept that does not have an exact counterpart in civil law. Concepts of fairness, appropriateness and proportionality form an approximation. *See* BLACK'S LAW DICTIONARY 1272 (7th ed. 1999)("reasonable, adj. 1. Fair, proper or moderate under the circumstances <reasonable pay>.")

[112] *See* PAG APP 2 (*Guidelines for Consumer Protection in the Electronic Marketplace*, DSTI/CP(98)13/FINAL, OECD, *available at* <http://www.oecd.org/dsti/sti/it/consumer/index.htm>, hereinafter "OECD Consumer Guidelines"). While these Guidelines are voluntary, they have been negotiated by representatives from the 29 most industrialized countries and industry and consumer advocacy groups. The OECD is preparing an inventory of consumer protection laws and regulatory practices across member nations. The inventory remains in draft form but may be finalized by the end of 2001.

[113] *See, e.g.*, PAG § D.3.1.2 (Pseudonyms and Anonymity). Note that an underlying tension exists between the needs of consumers and merchants to increase comfort and trust levels by identifying and authenticating transacting or communicating parties and the desire of some parties to maintain anonymity.

[114] On December 28, 2000, the Dept. of Health and Human Services (DHHS) promulgated a final rule under HIPAA, *see* PAG APP 2 (*Standards for Privacy of Individually Identifiable Health Information (HIPAA)*, Dept. of Health and Human Services, 45 C.F.R. pt. 160, 164 (2000), hereinafter "DHHS Privacy Rule") which requires full industry compliance by April 14, 2003. On August 12, 1998, DHHS promulgated a proposed rule on standards for the security of electronic information systems, which contains a ringing endorsement of PKI technology. "Currently there are no technically mature techniques that provide the security service of nonrepudiation in an open network environment, in the absence of trusted third parties, other than digital signature- based techniques. Therefore, if electronic signatures are employed, we would require that digital signature technology be used." *Id*. *See* PAG APP 2 (*Security and Electronic Signature Standards, Proposed Rule*, Dept. of Health and Human Services, 45 C.F.R. pt 142 (1998), hereinafter "DHHS Security Rule"). The proposed rule on the security of electronic information systems was not made final by the December 28, 2000 final rule on privacy standards, which specifically identified the security standard as still merely a proposed standard. The U.S. Federal Trade Comm'n recommends that a website disclose information about security precautions in its privacy statement. *See* PAG APP 2 (*Privacy Online: Fair Information Practices in the Electronic Marketplace*, FTC Report to Congress (May 2000) <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>, hereinafter "2000 FTC Report"). Websites using SSL (secure socket layers) are increasingly using their privacy statements to disclose that they are providing website authentication plus a secure link that prevents unauthorized access for the duration of the SSL session.

(B2B) and business-to-consumer (B2C) context is the extent to which websites may be amenable to service of process as defendants in the plaintiff's location (the destination). Early precedent appears to be coalescing around the common-sense legal principle that websites tend to be subject to jurisdiction in the destination location if they are "interactive" websites and are focused upon solicitation of sales or other activity in the destination location.[115] An issue directly relevant to the consumer context is the extent to which contractual agreements as to "forum selection" (identification of the jurisdiction(s) where dispute resolution is permitted or required) and "governing law" (identification of the jurisdiction whose substantive body of law will be applied to resolve a dispute) will be enforced against a consumer.[116]

In the PKI context, a pivotal issue is the extent to which a CA issuing certificates or RA approving certificate applications may enforce a contractual provision specifying its own jurisdiction (origin) rather than the residence of the subscriber or relying party (who may or may not be a consumer) as the jurisdiction whose law governs the dispute and/or is a proper (or the only) forum for any dispute resolution. Conversely, is the subscriber or relying party (either or both of which may be consumers) able to avoid a forum selection and/or governing law clause to which the subscriber or relying party agreed in a subscriber agreement or relying agreement? In a B2B context, trade usage or explicit contractual language will most likely determine which law is applied to the dispute and where the dispute will be resolved. In the B2C context, however, there is no corresponding level of certainty, because many consumer protection laws tend to preserve the consumer's right to bring an action in the jurisdiction where the consumer resides despite the consumer's contractual acceptance of an inconsistent forum selection provision.

The uncertainty of jurisdiction and choice of law in B2C disputes has been further exacerbated by the accelerating growth of transactions conducted over the Internet. This occurrence is due, in part, to the elimination of geographical limitations for parties entering into contractual relationships. At both the domestic and international level, courts, governments, and international organizations are working to establish cross-border standards that will bring certainty to companies operating online.[117] For example, in criminal law cases in private international law courts are more inclined to accept jurisdiction. The basis for this stance is the protection of the citizens of the jurisdiction. Whereas in civil matters the court are inclined to adopt the *Zippo* sliding scale position for jurisdiction. Further, it is a basic rule of Private International Law that it is not possible to contract out of criminal liability or Inland Revenue laws of a jurisdiction. This is particularly important from a consumer protection position. For example a provision in a contract that provides for an indemnity for taxes liable by a CA would be unenforceable and could be illegal.

While the OECD has issued *Guidelines on Consumer Protection in the Electronic Marketplace* and industry groups have developed best practices in this area, companies engaging in cross-border consumer commerce must be aware that they may be subject to the consumer protection laws of a foreign country. Adherence to these laws will likely be one of the evaluation criteria for local assessors of PKIs. In Europe, for example, a new EU regulation, to be implemented in March 2001, will allow a EU consumer that purchases goods or services online to sue the seller in the consumer's home country, even if the seller has no business operations or employees in that country.[118] In addition, there is no uniformity across country laws; even within the EU, and in

[115] *See Zippo Manufacturing Co. v. Zippo Dot Com*, 952 F. Supp. 1119 (W.D. Pa. 1997) (leading U.S. case for a "sliding scale" of jurisdiction based upon the interaction of the website). *See generally* PAG APP 2 (*Jurisdiction in the Internet Age*, E. Horwitz & S. Fraser, The Metropolitan Corporate Counsel (Feb. 2001), n. 8, *available at* <http://www.darbylaw.com/jurisdiction.html>, (hereinafter "Horwitz").

[116] *See, e.g., Rudder v. Microsoft Corp.*, 2 C.P.R. 4th 474, Ontario Superior Court of Justice (1999), (validation of a forum selection clause adopted by clicking "I Agree" to the terms of an agreement online at the defendant's website).

[117] Although a sliding scale under *Zippo* is increasingly being followed in civil litigation, it should be noted that courts hearing private international law cases are more inclined to accept jurisdiction in criminal cases, on the basis of protecting the citizens of the forum state, and attempts to contract out of criminal liability and taxation by the forum state, are not likely to be respected.

[118] *See* PAG APP 2 (*Brussels Regulation on jurisdiction and the enforcement of judgments in civil and commercial matters*, European Commission, 18 Int'l Legal Mat'ls 8 (1979), Brussels 1968 (Full Faith and Credit Convention), *available at* <http://europa.eu.int/eur-lex/en/lif/dat/1968/en_468A0927_01.html>, hereinafter "Brussels Regulation"). The EU is currently

some other jurisdictions, consumers cannot waive their rights under certain consumer protection statutes. A CA or RA should be aware that, pursuant to this EU regulation, it might be subject to the substantive laws of all 15 EU member countries in which it provides goods or services online even without a physical presence in Europe. If a losing defendant does not have attachable assets in the country of the forum, the ability to actually enforce judgments of foreign courts may depend to some extent on the company's "presence" in the country in question.

C.5.1.3 Online Contracting

The legal rights and obligations of the parties to a PKI transaction may be formed from online "clickwrap" agreements rather than traditional written contracts. A "clickwrap" agreement may be used, for example, to bind a consumer to the subscriber agreement. These contracts are known as "clickwrap agreements" because the customer typically assents with a click on a button labeled "I accept" or similar language, before an order will be accepted, information provided, or service rendered. Clickwrap agreements derive their origin from "shrinkwrap" agreements, by which most software is sold today. Shrinkwrap agreements are unsigned agreements setting forth terms and conditions on the use of a software application, that are found within the plastic shrinkwrap of the software packaging that is opened for the first time after the purchase or licensing transaction is concluded. The purchaser or licensee of the software agrees by his or her conduct to be bound by such terms. Such conduct typically takes the form of installing or using the software after being provided an opportunity to review the contract's terms and to return the software for a full refund if the terms are unacceptable.

U.S. courts have enforced shrinkwrap agreements that provide notice of the user's ability to accept or reject the terms of the enclosed license/agreement.[119] Although U.S. common law regarding the enforceability of clickwrap agreements continues to evolve and is not as developed as case law regarding the enforceability of shrinkwraps, several U.S. courts have shown a willingness to uphold the validity of clickwrap agreements.[120] In further support of the validity of clickwrap agreements, at least one court has indicated that merely posting the terms and conditions as a link, without the requirement of any affirmative step to assent, such as a clickwrap agreement, does not create an enforceable online contract.[121] In addition, in the consumer context, the validity

negotiating for similar consumer protections under the Hague Conference on Private International Law supporting a draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters. This Convention provides unlimited jurisdiction among member countries to enforce virtually all member country judgments and orders, with no effort to harmonize diverse substantive laws of the member countries. The main result of these initiatives is to (i) prefer the plaintiff's domicile as the forum that has jurisdiction over the contract, and (ii) ensure that choice of law clauses cannot deny a consumer the right to mandatory consumer protection law. Moreover, a new initiative entitled "Green Paper on the Applicable Law of Non-Contractual Obligations", also known as "Rome II", broadens the scope of potential consumer causes of action by applying these principles to areas of law such as tort, product liability, unfair competition and defamation, potentially exposing companies to liability in any EU jurisdiction where the site can be viewed. See discussion of *Rome II* Proposal *available at* <http://www.epceurope.org/news/jan00.htm>(full text of Rome II Proposal not located as of this writing.)

[119] *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1449 (7th Cir. 1996) ("Shrinkwrap licenses are enforceable unless their terms are objectionable on grounds applicable to contracts in general, for example, if they violate a rule of positive law, or if they are unconscionable."). *See also Hill v. Gateway 2000, Inc.*, 105 F.3d 1147 (7th Cir. 1997); *M.A. Mortenson Co., Inc. v. Timberline Software Corp.*, 998 P.2d 305 (Wash. 2000) (finding assent where users were instructed to read the terms and conditions on the shrinkwrap and informed that use of the product indicates agreement to be bound regardless of whether user actually read terms).

[120] *See Hotmail Corp. v. Van Money Pie, Inc.*, No. 98-20064, 1998 U.S. Dist. Lexis 10729 (N.D. Cal. Apr. 16, 1998) (finding evidence of a breach of contract claim where a user violated terms of a clickwrap Terms of Service agreement). *Caspi v. The Microsoft Network, L.L.C.*, 732 A.2d 528 (N.J. 1999). (When properly set out with an opportunity to review terms and to make clear that an act such as clicking on-screen is an assent, and a single indication of assent suffices.) *See also CompuServe Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996) (acknowledging that typing "AGREE" at various points in an online agreement manifests assent to be bound by the terms and conditions thereof). *See generally* UCITA, *supra* note 110, § 112 (Manifesting Assent; Opportunity to Review) and comments thereunder.

[121] *See, e.g., Ticketmaster Corp., et al. v. Tickets.Com, Inc.*, No. 99-7654, 2000 U.S. Dist. Lexis 4553 (C.D. Cal. Mar. 27, 2000); *see also* Fed. Reserve Standards, *supra* note 109.

of clickwrap agreements may depend upon the length and complexity of the agreement. For example, validity may depend on whether the consumer is required to scroll through many Web pages of legalese before clicking an accept button, or whether by contrast the agreement is concise, simple, and viewable within one screen. Some vendors are now requiring consumers to read through or at least scroll through the agreement before being able to click through. CAs should inquire as to the appropriateness of clickwrap agreements in the jurisdiction in which they operate.

C.5.1.4 Language

In recent years, at both the national and international levels, there has been a push to simplify complex and lengthy legal documents and disclosure requirements as a measure of additional consumer protection.[122] A requirement that a particular document or disclosure be in "plain language" means that all information required to be disclosed should be clear, accurate, and easily understandable and accessible. Plain language drafting in the case of consumers should be applied to both legal and technical provisions.

To support and build the consumer need for certificates for trust in the electronic marketplace and to provide some measure of privacy protection, CAs should consider the use of PKI Disclosure Statements[123] to ensure greater consumer understanding of the respective roles and responsibilities of the CA and the consumer/subscriber. Similarly, the use and disclosure of comprehensive, yet easily comprehended, security policies and privacy statements are an additional example of best CA practices that would help educate and protect consumers. One way for such statements to be more easily comprehended by end users it to agree on the ordering of clauses, and the use, to the extent possible, of standardized language.[124]

C.5.1.5 Oversight/Consumer Satisfaction/Redress

A PKI may find itself subject, either expectedly or unexpectedly, to the scrutiny of a variety of government bodies/agencies acting under legal authority, consumer advocacy organizations and/or private sector accreditation services. Potential theories include lack of adequate notice, personal information misuse, false and deceptive advertising, or outright fraud.

In the United States, the federal governmental organization primarily devoted to consumer protection is the Federal Trade Commission (FTC). A PKI owned by a corporation or business entity in a federally regulated industry, may have additional consumer-related oversight, for example, the Federal Communications Commission (FCC) for telephone and cable television industry, or the Federal Reserve for regulating financial institutions.[125] At the local level, every state has some governmental entity or unit devoted to consumer protection (often centered in the state's Office of the Attorney General), and many cities have similar units.

[122] The requirement of "plain language" does not arise in the B2B context because the presumption in such transactions is that both parties are on a level playing field in which special protection from misunderstanding or overreaching is not necessary.

[123] *See* PAG APP 6 (PKI Disclosure Statement).

[124] This presumes a broad inventory of clauses that would allow coverage for varying security and business needs, and would introduce a level of interoperability across statements. *See, e.g.*, International Chamber of Commerce, "Incoterms 2000," (13 three-character phrases that are shorthand for precise definitions of commercial terms for carriage of goods, risk transfer and costs) *available at* <http://www.iccwbo.org/incoterms/wallchart.asp>.

[125] Regulations promulgated to date under GLB provide a panoramic view of virtually every U.S. agency involved in consumer protection in the financial services sector. *See, e.g.*, PAG APP 2 (*Joint Final Rule – Privacy of Consumer Financial Information*, 65 Fed. Reg. 35,161, 12 C.F.R. pt. 40, Office of the Comptroller of Currency; 12 C.F.R. pt. 216, Federal Reserve System; 12 C.F.R. pt. 332, Federal Deposit Insurance Corp.; 12 C.F.R. pt. 573, Office of Thrift Supervision (2000), hereinafter "Joint Privacy Rule"); (*Final Rule – Privacy of Consumer Financial Information*, 65 Fed. Reg. 31,721, 12 C.F.R. pt. 716, National Credit Union Admin. (2000), hereinafter "NCUA Privacy Rule"); and (*Final Rule – Privacy of Consumer Financial Information*, 65 Fed. Reg. 3645, 16 C.F.R. pt. 313, Federal Trade Comm'n (2000), hereinafter "FTC Privacy Rule"). Additional agencies include the SEC and state insurance regulatory agencies

Within the private sector, the Better Business Bureaus of local cities perform a valuable consumer watchdog function by maintaining public records on the number and type of consumer complaints received in many industries. Online self-regulatory groups BBBOnline[126] and TRUSTe[127] provide seals or "trustmarks" to companies that comply with certain privacy and/or fair business requirements. Both groups offer mediation and dispute resolution services to aggrieved consumers who cannot obtain satisfaction from a company's internal complaint handling procedures. Both groups also reserve the ability to publicly withdraw the seal for non-compliance. With respect to consumer privacy, several consumer advocacy organizations, including the Electronic Privacy Information Center (EPIC) and Consumers Union (CU), have undertaken a similar watchdog function on behalf of consumers that claim malfeasance by a business entity.

Similarly, in Europe, consumer protection entities and mechanisms include national consumer protection agencies and private sector groups involved in government-sponsored codes of conduct. For example, in the Netherlands, consumer protection issues are usually addressed through a tripartite coalition of government, industry, and non-commercial private sector entities.

C.5.1.6 Information Practices – Corporate Data

The phrase "information practices" generally refers to a business' policies and procedures with respect to information collected and used as a part of that business. Information practices are a subset of a company's overall business practices. Information collected and used as a part of a company's business practices generally originates from its customers, which may be business entities or consumers. A company's information collection practices with respect to corporate customers and clients are covered in this section. A company's information collection practices with respect to consumer data are covered in PAG §§ C 5.2 (Privacy and Personally Identifiable Information) and D.2.8.3 (Privacy) *infra*. The most important issue that arises with a company's collection and use of corporate data is the appropriate protection and maintenance of any confidential and proprietary nature of that information[128].

Unlike the use of personal information from consumers, the use of corporate customer information in a relatively new industry such as the PKI industry, is governed almost exclusively by contractual limitations. There has been little opportunity to establish an industry norm through customary or longstanding trade usage. Thus, CAs and their corporate customers must negotiate and mutually determine how corporate information may be used. Such negotiations should take into account how corporate information will be shared within the CA's business organization and across its organizational partners, and how corporate information may be shared and sold outside of the company and its affiliates. It is important to be aware that among corporate customers and entities, *contractual silence can imply consent* under certain usage of trade. The EU Data Protection Directive,[129] however, does not exclude personally identifiable information used at the business level from the scope of privacy protection, and the laws of certain EU nations specifically cover such information.

C.5.1.7 Fair Business Practices

Fair business practices are the subset of overall business practices that deal with B2C interactions. In both the national and international arenas, governmental entities and private organizations alike are proposing sets of "fair business practices" to govern the business practices of companies operating in the online market.

[126] BBBOnline is the online arm of the Council of Better Business Bureaus, *available at* <http://www.bbbonline.com>.

[127] TRUSTe is a private nonprofit certification organization promoted by a consortium of Internet companies, *available at* <http://www.truste.com>.

[128] Significant issues related to employee or human resources data may also exist, but are beyond the scope of this analysis.

[129] *See* PAG APP 2 (*Protection of individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Council Directive 95/46/EC, 1995 O.J. (L 281) 31 (24 Oct. 1995), *available at* <http://europa.eu.int/eurlex/en/lif/dat/1995/en_395L0046.html>, hereinafter "EU Data Protection Directive").

Australia, for example, has a set of *Consumer Protection Principles in Electronic Commerce*, which addresses fair business practices, fair advertising and marketing practices, online business identification, and information disclosure requirements.[130] The American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants have also introduced a *Business Practices/ Transaction Integrity Principle and Criteria* in connection with the AICPA/CICA WebTrust Program.[131] The Principle, which applies in both the B2C and B2B contexts, sets out "an overall objective in respect to the completeness and accuracy of the processing of electronic transactions sent over the Internet." During the course of an audit, the criteria are then used to assess whether the Principle has been achieved. The following is version 3.0 of the Principle:

> "The entity discloses its business practices for electronic commerce, executes transactions in conformity with such practices, and maintains effective controls to provide reasonable assurance that electronic commerce transactions are processed completely, accurately, and in conformity with its disclosed business practices."

In the United States, the Electronic Commerce and Consumer Protection Group, formed by a consortium of leading Internet companies,[132] released the *Guidelines for Merchant-to-Consumer Transactions*, which are designed to create a set of best practices for consumer protection in global electronic commerce and transactions.[133]

BBBOnline, has released a set of standards designed to provide guidance for merchants transacting business online, in an effort to promote consumer trust and confidence in electronic commerce. CA's and assessors of CA's seeking guidance as to electronic commerce best practices should take note of the BBB Code of Online Business Practices,[134] which include five basic principles:

- *Truthful and Accurate Communications*. Online advertisers should not engage in deceptive or misleading practices with regard to any aspect of electronic commerce, including advertising, marketing, or in their use of technology.

- *Disclosure*. Online merchants should disclose to their customers and prospective customers information about the business, the goods or services available for purchase online, and the transaction itself.

- *Information Practices and Security*. Online advertisers should adopt information practices that treat customers' personal information with care. They should post and adhere to a privacy policy

[130] *See* PAG APP 2 (*Consumer Protection Principles in Electronic Commerce*, C(98)177, Australian Competition and Consumer Commission (ACCC), 8 Oct. 1998, annex 2, a*vailable at* <http://www.accc.gov.au/ecomm/principles.htm>, hereinafter "Australian Privacy Principles").

[131] *See* AICPA/CICA Webtrust, *supra* note 4.

[132] Members include America Online, AT&T, Dell Computer Corp., IBM, Microsoft, Network Solutions, Time Warner Inc., and Visa Intl., *available at* <http://www.ecommercegroup.org>.

[133] The guidelines address the following topics: (1) disclosure of merchant contact information, (2) accurate representations in marketing practices, (3) clear disclosure of the basic features of the good or service, (4) disclosure of terms and conditions about the transaction and the opportunity to review the transaction, (5) disclosure of cancellation/return/refund policies, (6) appropriate packaging of tangible goods, (7) implementation of appropriate security measures, (8) disclosure of basic information regarding customer service and/or support for goods or services purchased online, (9) disclosure of applicable warranties or limited warranties, (10) adoption of privacy policies that are consistent with existing industry standards and existing legal requirements, (11) disclosure of any self-regulatory programs in which the merchant participates and applicable dispute resolution processes, 12) provision of fair, timely, and affordable means to settle disputes and obtain redress, and (13) participation in effective self-regulatory enforcement programs to provide validation that Merchants adhere to these or equivalent guidelines, a*vailable at* <http://www.ecommercegroup.org/guidelines.html>.

[134] *Available at* <http://www.bbbonline.com/code/index.asp>.

based on fair information principles, take appropriate measures to provide adequate security, and respect consumers' preferences regarding unsolicited email.

- *Customer Satisfaction*. Online merchants should seek to ensure their customers are satisfied by honoring their representations, answering questions, and resolving customer complaints and disputes in a timely and responsive manner.

- *Protecting Children*. If online advertisers target children under the age of 13,[135] they should take special care to protect them by recognizing children's developing cognitive abilities. Specifically, they should adhere to the CARU Self-Regulatory Guidelines for Children's Advertising.

Given the business model of many PKIs today, information usage and practices, including information practices regarding corporate customer information, are likely to be standardized within the PKI itself, thus limiting the amount of options that the PKI will be able to offer any individual customer. Thus, PKIs may want to stress open and ongoing disclosure to its customers as the PKI's information practices evolve. The use of cookies, for example, should be disclosed by a PKI when conferring with its customers,[136] as well as the types of information that will be publicly viewable (and thus considered non-confidential) on a certificate issued by the CA. *See infra* § C.5.2 (Privacy and Personally Identifiable Information).

The most important information practices relate to the collection, use, and disclosure of personally identifiable information ("PII") discussed in the next section.

C.5.2 PRIVACY AND PERSONALLY IDENTIFIABLE INFORMATION

"Privacy," within the realm of information security, refers to a reasonable expectation that personally identifiable information ("PII") and sensitive information will be collected and used only for the purposes for which it was collected and not disclosed without the opportunity to exercise some choice regarding further use of the information. PII generally refers to information that can be traced back to an individual, such as name, mailing address, and email address. Sensitive information refers to certain types of personal information that warrant special protection, such as financial, medical, children's, and employment information. Privacy differs and should be distinguished from "confidential" and "security." "Confidential" refers to the reasonable expectation that information will not be accessed or viewed by unauthorized parties; whereas "security" refers to technological measures taken to prevent theft, disclosure, improper use, and/or unauthorized access to information. Technological measures, such as SSL and message encryption, can be used to create a reasonable expectation of privacy.[137]

C.5.2.1 Background

Privacy with respect to electronic commerce conducted over the Internet and other electronic networks has become one of the most important concerns of both consumers and governments.[138] These concerns have

[135] The jurisdictional requirement for coverage by COPPA, *see infra* PAG § C.5.3.6 (COPPA).

[136] While cookies are used by many to clickstream track for marketing purposes, CAs may be using them for only security and navigation purposes.

[137] SSL means "secure sockets layer," and is a type of PKI-enabled secure communication commonly used to enable a browser to authenticate a website, and to construct a secure link with a browser that prevents eavesdropping and spoofing during the duration of the session. SSL often avoids the need for key distribution by using self-signed certificates that are placed in the browser software as trusted certificates prior to distribution of the software, or added later by the browser user. *See* PAG APP 3 (Tutorial).

[138] *But see* "Survey: Americans Willing to Give Up Privacy Rights" *available at* <http://www.ecommercetimes.com/perl/story/8656.html>. Interestingly, the survey has been interpreted as indicating that Americans would be willing to forego some amount of privacy online in order to help prevent criminal activity.

arisen, in part, because of the relative ease in which large amounts of personal data can be collected over the Internet. Governments in recent years have addressed online privacy generally either by promoting a market-driven, self-regulatory approach coupled with targeted legislation, such as the United States, or enacting comprehensive data protection legislation, such as member states of the EU.

Significantly, many countries have endorsed the OECD *Privacy Guidelines* of 1980 and have data protection laws based on these Guidelines.[139] The basic principles of the Guidelines include: (i) Collection Limitation (i.e., personal data should be obtained by lawful and fair means); (ii) Data Quality (i.e., personal data should be relevant to the purposes for which they are used, accurate, complete, and kept up-to-date); (iii) Purpose Specification (i.e., purposes for which data are to be used should be specified and subsequent use should not be incompatible with those purposes); (iv) Use Limitation (i.e., personal data should not be disclosed or used for purposes not specified unless consent given by data subject or under the authority of law); (v) *Security Safeguards* (i.e., personal data should be protected by reasonable security safeguards against loss, destruction, or disclosure); (vi) Openness (i.e., general policy of openness about developments with respect to personal data); (vii) Individual Participation (i.e., individuals have certain rights with respect to personal data held by data controllers); and (viii) Accountability (i.e., data controller is responsible for complying with the principles).

C.5.2.2 Self-Regulation

The United States has consistently promoted industry self-regulation as a means of protecting personal information collected over the Internet.[140] By way of guidance to self-regulation, the U.S. Dept. of Commerce issued a discussion paper on the "*Elements of Effective Self-Regulation for Protection of Privacy*" ("Elements Paper") in January 1998. The Elements Paper is divided into two sections: (i) principles of fair information practices; and (ii) enforcement. The section on principles of fair information practices tracks much of the OECD Guidelines. Specifically, such practices include consumer awareness, the choice of how data is used, appropriate levels of security, and consumer access to personally identifiable data. The section on enforcement incorporates the OECD's principles of accountability, sanction, and remedy by addressing consumer recourse, verification of a company's privacy policies, and consequences for failure to comply with the fair information practices.

The FTC, by way of its authority under the Federal Trade Commission Act, has been the U.S. regulatory body most active in addressing the issue of online privacy. In June 1998, the FTC issued a comprehensive report to Congress on Internet privacy ("1998 FTC Report"), which was expanded and updated in May 2000. The two FTC reports describe fair information practice principles governing notice, choice, access, security, and enforcement for companies collecting personal information online.[141] Specifically, these principles include providing the consumer with: (i) *notice* of the company's information practices; (ii) a *choice* with respect to the collection, use, and sharing or transfer of PII collected from or about him or her; and (iii) *access* to PII about him or her that is collected and stored by the company. Furthermore, according to the fourth principle, the data collector must take appropriate steps to ensure the *security and integrity* of any PII collected. Lastly, such principles must be *enforced* through industry self-regulation, legislation that would create private remedies for consumers, and/or regulatory schemes enforceable through civil and criminal sanctions.

In response to recent data protection developments, including implementation of the EU Signature Directive and statements from the FTC, and the U.S. commitment to protection of privacy through self-regulation, various

[139] *See* PAG APP 2 (*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, C(80)58/FINAL, OECD (23 Sept. 1980), hereinafter "OECD Privacy Guidelines"). Countries that have adopted the Guidelines include, for example, Denmark, the Czech Republic, Germany, Greece, India, Italy and South Korea.

[140] Recent developments, however, indicate that the US may be moving toward a more regulatory approach to privacy protection. *See* Joint Privacy Rule, *supra* note 125.

[141] *See* 2000 FTC Report, *supra* note 114; *see also* PAG APP 2 (*Privacy Online: A Report to Congress*, FTC (1998) *available at* <http://www.ftc.gov/reports/privacy3/index.htm>, hereinafter "1998 FTC Report").

independent organizations, such as TRUSTe,[142] have developed third-party privacy programs. TRUSTe, discussed above, permits a company that complies with its online privacy policy guidelines, which resemble the safe harbor principles, to display a "seal" of approval. Companies bearing the TRUSTe seal: (i) are subject to oversight and monitoring; and (ii) agree to provide consumers with simple, effective means to submit their privacy concerns directly to the Web site. In the case of unresolved disputes, TRUSTe will act as the liaison between the consumer and the Web site operator, conduct investigations and on-site reviews, and advise and guide the licensee on steps to remedy the problem. In extreme cases, TRUSTe will revoke the trustmark or refer the company to the appropriate government agency.

Although these standards of self-regulation are rarely binding on individual businesses, it is the U.S. government's position that the FTC can enforce individual firm compliance with such guidelines under its Act of 1998. *See infra* PAG § C.5.2.3 (Regulation).

C.5.2.3 Regulation

In the United States, there is no generally applicable body of privacy law[143] that applies to the activities of all CAs.[144] However, there are a variety of unrelated Federal laws that impose varying privacy obligations with respect to particular industries, activities, or types of information. Three areas that may deserve special attention, because of proposed widespread PKI and digital certificate involvement, include medical information, financial information, and children's information. Each of these areas is covered in the section "Relevant Legislation" below. At the state level, there is a patchwork of state law and regulation addressing particular types of information or information users, as well as state common law addressing various aspects of the "right of privacy," which federal privacy legislation and regulation typically do not pre-empt if the state provides greater privacy protection than under federal law. Finally, there are non-legal, but potentially significant, societal expectations concerning the collection, maintenance, and distribution of personal information.

In addition, there is at least one federal statute that has been interpreted to impose privacy obligations, even though its specific focus is not privacy. This statute is the Federal Trade Commission Act ("FTC Act"), section 5 of which addresses "deceptive trade practices" and has been applied by the FTC to privacy issues. Under Section 5 authority, the FTC can enforce any material statements made or terms entered into against a company. Previous enforcement has included wrongful use of information as well as claims relating to online information collection practices. Specifically, in several recent FTC actions, the FTC has held that a company's failure to act consistently with the company's stated information collection practices (*i.e.*, online privacy statement) constituted an unfair or deceptive trade practice in violation of section 5 of the FTC Act.[145] Thus, even if there is no applicable law or regulation requiring a company or a website to provide a privacy statement, the failure to follow a voluntarily-posted or provided privacy statement may be a violation of section 5 of the FTC Act.[146]

---

[142] *See supra* note 127.

[143] In other words, there is no generally applicable body of privacy law that applies to both the public and private sector. The Privacy Act of 1974, discussed infra, deals with privacy of information under the control of federal governmental entities.

[144] Possibly in response to the explosive growth of electronic and online commerce, there is a growing possibility of some form of comprehensive privacy legislation in 2001 at the federal level. Recently, many privacy bills providing varying degrees of data protection have been introduced in Congress. One such example is a bill sponsored by Senators Kerry (D-MA) and McCain (R-AZ), which is a Senate bill requiring web sites to provide users clear and conspicuous notice about their information collection practices and the choice to limit the disclosure of information. The bill also authorizes the FTC to enforce these notice and disclosure requirements through civil penalties and preempts state laws regulating on-line privacy. *See* FTC Privacy Rule, *supra* note 125.

[145] *See, e.g., In re GeoCities, Inc.*, File No. 98-23015, (13 Aug. 1998), *available at* <http://www.ftc.gov/opa/1998/9808/geocitie.htm>.

[146] As of this writing it appears that bankruptcy is not considered grounds for evasion of privacy assurances given in connection with collection of identifiable personal information. *See* PAG APP 2 (*Toysmart Bankruptcy Settlement Ensures Consumer*

C.5.3 RELEVANT LEGISLATION

C.5.3.1 E-Sign

In the general field of e-commerce, a significant development has been the U.S. Federal government enactment of the Electronic Signatures in Global and National Commerce Act, otherwise known as "E-SIGN,"[147] which is widely expected (given its preemption authority) to have a considerable impact upon electronic commerce in the United States in general, and with consumers in particular. For transactions in or affecting interstate commerce[148], section 101(a) of E-SIGN effectively removes e-commerce inhibitors, such as lingering legal rules that require a transaction to have a hardcopy writing, or a pen-and-ink signature. E-SIGN provides that a signature, contract or record relating to such a transaction may not be denied legal effect, validity, or enforceability solely because they are in electronic form or because an electronic signature or electronic record was used in its formation. It appears clear from section 106(5) of E-SIGN that a PKI-related digital signature is an "electronic signature" for most purposes of section 101(a).[149]

In the case where a "statute, regulation, or other rule of law requires that information relating to [such] . . . transactions be provided or made available to a consumer in writing," the use of an electronic record to provide such information is validated under section 101(a), but only if the mandated consumer disclosures and consents are first provided. These consumer disclosures are intended to inform the consumer of what information will be provided electronically, the manner in which information is provided (*i.e.*, by current website "pull" or future e-mail "push"[150]), hardware and software in use, instructions for obtaining paper copies, withdrawing consent to use electronic records, changing addresses for future e-mails, and how it will be demonstrated that a particular consumer has the capability to access the types of electronic records in question. Following (and not before) these disclosures,[151] opt-in consent is explicitly requested from the consumer (which can be given by click-through agreement); the consumer can immediately enter into a binding electronic contract, such as an enrollment agreement, with an electronic signature (including a digital signature). The consumer provisions of section 101(c) of E-SIGN will undoubtedly have an impact that extends beyond B2C commerce, as many of the disclosure and consent provisions are also prudent measures to bolster the evidentiary effectiveness of a click-through agreement in B2B situations. Furthermore, given that it is not always possible to determine whether the user at the other end of a CA transaction is a "consumer" or a business, it may become best practice in the CA industry to use the E-SIGN stipulated consumer procedures for all users, at least until such time as the status of users can be adequately authenticated.

Privacy Protection, Office of NY State Attorney General Eliot Spitzer, Press Release (11 Jan. 2001), *available at* <http://www.oag.state.ny.us/press/2001/jan/jan11a_01.html>, hereinafter "Spitzer press release").

[147] *See* E-SIGN Act, *supra* note 73.

[148] It is hard to conceive of a web-based transaction that does not meet this interstate commerce test.

[149] "Electronic Signature. – The term `electronic signature' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." *See* E-SIGN Act, *supra* note 73, § 106(5).

[150] Website "push" notification by itself is not enough for GLB Act mandatory privacy notifications. The interim final rule of the Federal Reserve Board allows website notification only if "push" notification of the website content is provided by e-mail or postal mail and the website notification remains available for 90 days. *See* Fed. Reserve Standards, *supra* note 109.

[151] In its interim final rule implementing E-SIGN for purposes of making mandated disclosures of privacy policy under GLB with respect to the five consumer protection Regulations B, E, M, Z, and DD, the Federal Reserve states that the clickwrap consent must be set up to require prior actual access of the disclosures by the consumer. It is not sufficient to merely make access available to the consumer. The rule appears to stop short of expressly requiring the consumer to access all screens of disclosure from the beginning to the end of the disclosure. *See, e.g.*, Reg. B, *supra* note 109.

C.5.3.2 EU E-Signatures Directive and EU Privacy Directive

The EU Signature Directive[152] (article 13 of the Directive specifies implementation by all EU Member States before July 19, 2001) provides differing treatment for electronic signatures and "advanced electronic signatures."[153] Electronic signatures are not denied legal effect merely because they are in electronic form, or lack certain enhancements, such as being based upon a qualified certificate. Advanced electronic signatures with certain enhancements (*i.e.*, they are based on a qualified certificate and are created by a secure-signature creation device, both as defined in the Directive) are admissible into evidence in legal proceedings and satisfy the requirements of a written signature.[154]

The EU Data Privacy Directive[155] on creates obligations to adhere to privacy principles, e.g., that personal data must be processed fairly and lawfully for only the purposes specified and only to the extent necessary and for the duration appropriate for those purposes. Most importantly, the Data Privacy Directive prohibits the transfer of personal information to persons (even within the same multinational company) in other countries that do not have "privacy regimes" providing protection of privacy considered "adequate" when compared to the principles enunciated in the Directive. These requirements have been specifically carried forward and made applicable to CAs (known in the Directive as "CSPs") by article 8 of the EU Signature Directive.[156]

C.5.3.3 Canadian Privacy Law

Canada has enacted a comprehensive privacy law, the Personal Information Protection and Electronic Documents Act ("Canadian Privacy Act" or "Act"), effective in stages from April 1, 2000 to January 1, 2004.[157] The Act codifies clear guidelines for the protection of consumer privacy in Canada, and brings all of Canada[158] in line with international privacy laws such as that of the European Union. The Canadian Privacy Act sets forth ten principles of Fair Information Practices, which address the protection of personal information and must be followed by private sector organizations covered by the Canadian Privacy Act *and* entities to which such private sector organizations transfer personal information. The principles require, for example, that entities covered by

[152] *See* EU Signature Directive, *supra* note 5.

[153] "'[A]dvanced electronic signature' means an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable." *Id*., art. 2(2).

[154] *Id*., art. 5(1).

[155] *See* EU Data Protection Directive, *supra* note 129.

[156] "Article 8: 1. Member States shall ensure that certification-service-providers and national bodies responsible for accreditation or supervision comply with the requirements laid down in the EU Data Protection Directive on tile protection of individuals with regard to the processing of personal data and on the free movement of such data. 2. Member States shall ensure that a certification-service-provider which issues certificates to the public may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject. 3. Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent certification-service-providers from indicating in the certificate a pseudonym instead of the signatory's name." *See* EU Signature Directive, *supra* note 5.

[157] *See* PAG APP 2 (*Personal Information Protection and Electronic Documents Act*, (2000), *available at* <http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html>, hereinafter "Canadian Privacy Act"). The Canadian Privacy Act is written to be effective in three stages. As of January 1, 2001, two types of data are covered, including: (i) personal data that is processed by federally-regulated industries, such as financial services, telecommunications, broadcast media, and air transportation; and (ii) data that is transferred under certain conditions outside of Canada. As of January 1, 2002, health information is also covered by the Act. Finally, as of January 1, 2004, all commercial transactions in Canada involving personal data will be subject to the requirements and restrictions of the Act.

[158] The Canadian province of Montreal enacted a comprehensive privacy law in 1994.

the Canadian Privacy Act obtain an individual's consent when collecting, using, or disclosing an individual's personal information. In addition, an individual has a right of access to his or her personal information that is held by an organization and a right to correct any inaccuracies. Also, personal information can only be used for the purposes for which it was collected. If an organization intends on using it for a different purpose, the organization must obtain the individual's consent a second time. An organization is required to protect personal information against loss or theft, unauthorized access, disclosure, copying, use, or modification through a company security policy. Finally, organizations covered by the Act must appoint privacy officer responsible for complying with the Canadian Privacy Act.

C.5.3.4 Gramm-Leach-Bliley

In the financial services industry, the Gramm-Leach-Bliley Act (the "GLB Act")[159] protects the privacy of nonpublic and identifiable financial information of individual consumers. The FTC and the Federal banking and supervisory agencies have promulgated regulations to implement the GLB Act.[160] In general, the GLB Act requires a "financial institution" (engaged in banking, securities or insurance) to (i) provide its "customers" with notice of its privacy policy;[161] and (ii) not disclose non-public personal information about a consumer to nonaffiliated third parties unless the institution satisfies various disclosure requirements and the consumer has not elected to opt out of the disclosure. It is quite possible that a CA or RA affiliated with a financial holding company, in the course of collecting information about individuals applying for issuance of a certificate, would itself be considered a "financial institution" under the GLB Act, and therefore subject to the privacy requirements of the GLB Act and associated regulations.[162] The GLB Act and the accompanying privacy regulations apply only to information about individuals who obtain a financial product or service from a financial institution to be used for personal, family, or household purposes. This might lead to a distinction between a CA's or RA's collection of information for issuance of a certificate to an individual to be used for personal purposes, and a CA's or RA's collection of information for issuance of a certificate to a business organization to authenticate, for example, that organization's web server.

[159] *See* PAG APP 2 (*Gramm-Leach-Bliley Act,* 15 U.S.C. § 6801 *et seq*. (1999), *available at* <http://www.senate.gov/~banking/conf/confrpt.htm>, hereinafter "GLB Act").

[160] See PAG APP 2 (Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, Joint Final Rule, 66 Fed. Reg. 8,616 (1 Feb. 2001), hereinafter "Joint Standards Rule").

[161] The initial privacy notification to "customers" is required to be completed by July 1, 2001. "Customer" is an individual consumer that meets certain requirements as to an existing relationship with the financial institution.

[162] The FTC defines "financial institution" as "any institution the business of which is engaging in activities that are financial in nature as described in section 4(k) of the Bank Holding Company Act of 1956." *See* FTC Privacy Rule, *supra* note 125, § 313.3(j)(1). Section 4(k)(4) of the Bank Holding Company Act of 1956, defines activities that are considered to be "financial in nature" as any activity that the Federal Reserve Board has determined to be "so closely related to banking or managing or controlling banks as to be a proper incident thereto." *See* GLB Act, *supra* note 159, § 103(a); *see also* PAG APP 2 (*Bank Holding Company Act of 1956*, § 4(k)(4)(F), 12 U.S.C. § 1843(k) (1956), hereinafter "Bank Act of 1956"). In one case where a CA specializes in issuing certificates for banking transactions, the Federal Reserve Board has determined by order that the issuance of digital certificates, and acting as a certification authority, are activities "so closely related to banking as to be a proper incident thereto." *See* PAG APP 2 (Federal Reserve Order to Identrus, LLC (10 Nov. 1999), *summarized in* GAO, Letter to the Chairman of the Board of Governors of the Federal Reserve System and to the Comptroller of the Currency, "Bank Regulators' Evaluation of Electronic Signature Systems" (8 Nov. 2000), *available at* <www.steptoe.com/webdoc.nsf/Files/GAObankpki/$file/GAObankpki.pdf>, hereinafter "Fed. Reserve Order").

C.5.3.5 HIPAA

PKI infrastructures for use by healthcare organizations and professionals will need to be administered consistently with the obligations of such parties to ensure the security and privacy of patient- and health plan enrollee-identifiable information. These obligations arise from a complex set of federal and state laws. The application of these laws may vary substantially depending upon the functions performed by or professional status of a given party, and the party's relationship to governmental authorities.[163] Healthcare PKI assessment is therefore likely to be a complex task requiring familiarity with a number of different laws and their application given the legal status of PKI participants.

Healthcare professionals have traditional ethical obligations to protect patient confidentiality, and most organizations and individuals providing healthcare services are licensed by the states in which they operate under terms requiring them to protect patient confidentiality. Most if not all states have enacted legislation or promulgated regulations applicable to the protection of healthcare-related information, and in many jurisdictions there is case law which may be material to this issue.

Federal law is likewise complex in this area. As of the date of publication of this document the primary applicable federal law is the Privacy Act of 1974.[164] The Health Care Financing Administration ("HCFA"), a division of the U.S. Dept. of Health and Human Services, has interpreted the Privacy Act to require governmental agencies and private parties under HCFA contract to protect individually-identifiable information sent over the Internet using encryption protection equivalent to Triple 56 bit DES.[165] Authentication by use of digital certificates in a PKI is acceptable, so long as it is based upon out-of-band authentication.[166]

The most significant federal law in this field is the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[167] HIPAA authorized and directed the U.S. Dept. of Health and Human Services ("DHHS") to promulgate a series of regulations mandating the use of electronic data interchange ("EDI") for healthcare claims processing by healthcare organizations. [168] This mandate include the issuance of regulations controlling the privacy and security of "individually-identifiable health information" created, received or otherwise in the possession of health plans, healthcare clearinghouses and healthcare providers (termed "Covered Entities" in the HIPAA regulations).[169]

Compliance by Covered Entities with regulations issued under HIPAA is not mandatory until two years after a given regulation becomes final.[170] DHHS published the final privacy regulation ("Privacy Rule") on December

[163] See, e.g., PAG APP 2 (Internet Communications Security and Appropriate Use Policy and Guidelines for HCFA Privacy Act-protected and other Sensitive HCFA Information, HCFA Internet Security Policy Bulletin, U.S. Health Care Financing Admin. (24 Nov. 1998), hereinafter "HCFA Security Bulletin"), (formalizing policy and guidelines for Internet transmission of individually-identifiable information by HCFA employees as well as private parties acting as HCFA contractors, and State agencies serving as HCFA agents, etc.).

[164] *See* PAG APP 2 (*Privacy Act of 1974*, 5 U.S.C. § 552, hereinafter "Privacy Act of 1974").

[165] *See* HCFA Security Bulletin, *supra* note 163.

[166] *Id*.

[167] *See* PAG APP 2 (*Health Insurance Portability and Accountability Act of 1996*, 42 U.S.C. §§ 264, 1320d-4(b) (1996), hereinafter "HIPAA"). The material portions of this complex act are found at Title II Subtitle F, §§ 261 - 64, entitled "Administrative Simplification."

[168] Note that in actual implementation, "EDI" is deemed to include any form of electronic transaction.

[169] Note that the privacy and security regulations apply to all such individually-identifiable health information, not just that which may be related to claims

[170] *See* HIPAA, *supra* note 167. Note that "small health plans" have three years to come into compliance. "Small health plan" is defined in a restrictive fashion so that few entities will fall into this category, so this issue is beyond the scope of this discussion. It will be assumed below, and in healthcare PKI assessment should be assumed that no "small health plan" is a party, unless the issue is raised and the categorization proven.

28, 2000 and the rule became final on April 14, 2001.[171] Compliance with the Privacy Rule will therefore be mandatory as of April 15, 2003.

DHHS is required to issue a separate security regulation, and as of the date of the publication of this document has issued a proposed rule but not the final rule ("Security Rule").[172] Informal statements from DHHS sources to date have indicated that the final Security Rule is scheduled to be published some time in Summer 2001, which would make compliance with the Security Rule mandatory some time after compliance with the Privacy Rule becomes mandatory in 2003.[173]

Neither HIPAA nor any of the regulations issued under it requires the use of PKI, digital certificates or digital signatures. HIPAA does direct DHHS to "adopt standards specifying procedures for the electronic transmission and authentication of signatures with respect to [claims transactions,]" and specified that compliance with this standard "shall be deemed to satisfy Federal and State statutory requirements for written signatures with respect to" such transactions.[174] DHHS published a draft electronic signature standard along with the draft Security Standard.[175]

This draft standard was stated to be applicable "[i]f an entity elects to use an electronic signature in a [claims transaction], or if an electronic signature is required by a transaction standard adopted [by DHHS under HIPAA.]"[176] For such purposes, the draft standard stated that "[t]he standard for electronic signature is a digital signature."[177] It is not clear what the status of the draft electronic signatures standard is in light of E-SIGN, and informal statements from DHHS sources indicate that a final standard may not be published.

The draft electronic signature standard may nonetheless be considered a reasonable indicator that digital signatures are an application likely to be considered acceptable for security functions under HIPAA. Covered Entities will be required to comply with the Privacy and Security Rules by development of plans, policies, procedures and contracts and the implementation of technological solutions which are appropriate to their size, capitalization and operational needs, but which must include data access controls. PKI is likely to be considered a valuable approach to access control by many Covered Entities. The disclosure or use of protected information in violation of the Privacy or Security Rule may be grounds for criminal penalties, which may be very substantial in some cases.[178]

Since the right or privilege to access individually identifiable health information will depend principally upon the user's professional and/or organizational roles, the support provided by the PKI implementation to role definition will ordinarily be an important factor. The assessor should also consider the means by which a given user is identified and user identity is authenticated, and whether the level of assurance provided is appropriate to the sensitivity of the information which may be made accessible.

[171] *See* DHHS Privacy Rule, *supra* note 114. The final date was extended due to an initial failure to transmit the rule to Congress as required by the Congressional Review Act.

[172] *See* DHHS Security Rule, *supra* note 114.

[173] As of the date of publication there was some Congressional discussion of the desirability of legislation harmonizing these compliance dates but no specific legislation had been introduced.

[174] *See* HIPAA, *supra* note 167, § 1320d-2(e).

[175] *See* DHHS Security Rule, *supra* note 114.

[176] *Id*., § 142.310(a).

[177] *Id*., § 142.310(b). Note that section (c) of the proposed rule sets forth certain required and certain optional implementation features.

[178] *See* HIPAA, *supra* note 167, § 1320d-5. (Criminal penalties of up to ten years imprisonment, $250,000 fine per violation). Civil penalties are also available, and violations may also affect entity accreditation status or lead to private claims under some circumstances, but these are beyond the scope of this discussion.

The question of the level or type of assurance which may be desirable or prudent for access to a given system or set of protected information is primarily an issue for relying parties in a healthcare PKI. A covered entity which is a relying party accepting digital certificates for access to sensitive information resources must assume the primary obligation of making this determination, since it has the primary obligation to protect the information.

HIPAA and its attendant regulations do not supersede state laws which are "more strict' in their protections.[179] HIPAA also has a complex relationship with other federal laws, and DHHS has indicated that if there is a conflict the more specific law should apply, unless legal analysis indicates that one of the laws is an "implied repeal" of the other.[180]

It is therefore critical for CAs in PKIs using the PKI for transactions involving individually identifiable health information, or its equivalent as defined under state or other applicable federal laws, to analyze their obligations and documentation in light of the complex web of laws which apply to the subscribers and relying parties. Subscribers and relying parties must themselves be responsible for ensuring that their PKI activities are consistent with their obligations, since a CA will not generally be in a position to determine whether a given activity is legally appropriate.

C.5.3.6 COPPA[181]

In the case of children under the age of 13, the Children's Online Privacy Protection Act of 1998 ("COPPA")[182] prohibits web sites from collecting, using or disclosing personal information from such children without verifiable parental consent. COPPA, which was enacted January 23, 2000 and became effective April 21, 2000, was implemented by final regulations (the "Final Rule")[183] adopted by the Federal Trade Commission on November 3, 1999. Under COPPA, web site operators who have actual knowledge that a person from whom they seek information is a child, or who operate a website "directed to children" must comply with a variety of requirements, such as posting a privacy policy and notifying parents that they wish to collect information from their children. During the process of identifying certificate applicants, CAs might typically require information such as a name, address, social security number, and e-mail address to be furnished, all of which are items falling within the definition of "Personal Information" to which the Final Rule applies. On the other hand, a CA's or RA's website for identifying certificate applicants is certainly not automatically "directed to children,"[184] and a CA or RA would not normally have direct knowledge that a certificate applicant is a child under the age of 13. If a CA or RA happens to learn that it has collected personal information from a child under 13 (unlikely, but theoretically possible), the prudent course under COPPA would be to make certain that such information is not disclosed to any third party, and to seek verifiable parental consent to retain and use the information for normal PKI functions.

[179] *See* DHHS Security Rule, *supra* note 114.

[180] *See* DHHS Privacy Rule, *supra* note 114.

[181] There is confusion between COPPA and COPA (Child Online Privacy Act of 1998). COPA was declared unconstitutional in *ACLU v. Reno*, 217 F.3d 162 (3rd Cir. 2000), *available at* <http://www.epic.org/free_speech/copa/3d_cir_opinion.html>.

[182] *See* PAG APP 2 (*Children's Online Privacy Protection Act*, 15 U.S.C. §§ 6501-6505 (2000), hereinafter "COPPA").

[183] *See* PAG APP 2 (*Children's Online Privacy Protection Rule*; Final Rule, Part III, Federal Trade Commission, 16 C.F.R. pt. 312 (3 Nov. 1999), hereinafter "COPPA Final Rule").

[184] It may be prudent for a CA or RA to prominently post or publish electronically a notice stating that children under 13 are not permitted to apply for a certificate.

C.5.3.7 Government Use – Privacy Act of 1974

The Privacy Act of 1974[185], an amendment to the Freedom of Information Act (FOIA), aimed at increasing the privacy protections of the FOIA. While the primary goal of the FOIA is to make government information available to the public, it also contains exceptions that restrict disclosure of certain information in an effort to protect privacy. The Privacy Act was created to further prevent the government from disclosing computer database records maintained on an individual for any other purpose than that originally intended without consent. The act was amended by the Computer Matching and Privacy Act of 1988[186]. Government-owned or operated PKIs, or private PKIs that perform certification services on behalf of federal government entities, must remain mindful of the provisions and limitations of the Privacy Act, as amended, insofar as the law may affect how the PKI must fashion and conduct its respective information practices.

C.6 Risk Management and Insurance Principles

This section reviews the risk management process and identifies risk management and insurance legal issues to be considered by those that will deploy or use PKI. The emerging PKI insurance market is also discussed, along with some existing tort law reasoning that may well be used by attorneys and judges involved in early decisions involving PKI risk management.

In contrast with ideal hypothetical examples, in the real world of e-commerce, involving transactions of real value among real people, it is unrealistic to expect any system to provide perfect security, legal certainty, and freedom from risk. Accordingly, when faced with a need to increase the security of e-commerce, organizations need to apply sensible risk management principles and processes. Risk management analysis is useful for the initial assessment of whether or not to deploy or depend upon a PKI, as well as the weighing of practical options within a PKI environment.[187]

Key elements of risk management in the PKI context include:

1) Identification of PKI-oriented risks. Examples might include risks such as:

- **CASE A:** the risk of a CA inadvertently issuing a certificate linking a subscriber's distinguished name to the public key of an imposter who is then able to spoof the subscriber's digital signature by using his own private key;
- **CASE B:** the risk of the subscriber inadvertently losing control of her private signing key to an imposter who is then able use the subscriber's private key to spoof the subscriber's digital signature; or
- **CASE C:** the risk that the subscriber's certificate has been revoked by the CA since the last time the relying party checked the status of the certificate in the CA's repository.

2) Analysis of alternatives for managing the identified risks. This includes:

[185] *See* Privacy Rule of 1975, *supra* note 164.

[186] *See* PAG APP 2 (*Computer Matching and Privacy Act of 1988*, 5 U.S.C. § 552a (1994), hereinafter "Computer Privacy Act").

[187] *See* PAG APP 2 (*Risk Management Guide – Computer Security*, NIST Special Publication 800-30 [1st Public Exposure DRAFT] June 2001, p. 1, hereinafter "NIST Guide"). "Risk management is the process that allows managers to balance operational and economic costs of protective measures with the resulting gain in mission effectiveness. This process is not unique to the IT environment; indeed it pervades our decision-making on a daily basis. Take the case of home security. Many people decide to have security systems installed and pay a monthly fee to a service provider to have these systems monitored. Presumably, the homeowners calculated the cost of installation and monitoring against the values of their household goals and their family's safety, a fundamental 'mission' need." *available at* <http://csrc.nist.gov/publications/drafts.html>.

- **Risk avoidance.** The three PKI-oriented risks in the example above could of course be avoided by not implementing a PKI environment. This would then require a fresh examination of how the underlying security risks can be managed in the absence of the PKI environment. Within a PKI, it is a relatively simple matter to substantially avoid the risk in CASE C if the relying party always checks the status of a certificate in an authoritative repository immediately before relying upon it. The risks under CASE A and CASE B, on the other hand, are by their nature less susceptible of avoidance.

- **Risk assumption.** A risk, once identified, if not avoided, can be voluntarily, involuntarily, or unknowingly accepted. For example, under CASE C, a relying party might check the status of a subscriber's certificate upon caching it on the relying party's server, and not subsequently check the certificate before relying on it, thus voluntarily and knowingly accepting the risk that the subscriber's certificate has been revoked since the relying party cached it. If the rules of the particular PKI require the CA to post revocation notices no more frequently than within 24 hours after CA's receipt of revocation request, then by following the practice of not checking cached certificates, the relying party is involuntarily accepting the risk that revocation might have occurred as much as 24 hours before reliance, and is voluntarily accepting the risk of revocation between the time of cache and 24 hours before reliance.

- **Risk control.** A risk, once identified and accepted, may be controlled by minimizing the probability that an undesirable incident will happen, and/or by mitigating the severity of the incident or the damages caused as a consequence of the incident.[188] For example, the risk of the CA misidentifying the subscriber in CASE A and the risk of the subscriber losing her control of the private key in CASE B are both risks that cannot be entirely avoided and thus are involuntarily accepted by all participants to some extent. But the risks under CASE A and CASE B are most definitely subject to risk *control* as to both probability or occurrence and severity of consequences by a variety of techniques presented by the PAG, particularly in PAG § D.5 (Management, Operational and Physical Security Controls), and in PAG § D.6 (Technical Security Controls). In addition, PAG § D.1 (Community and Applicability), describes how the severity of consequences of an incident can be limited by a closed business model that allows only certain classes of entities to be relying parties; it is also possible to limit the amount of assumed risk by monetary caps upon the amount of permissible reliance.

- **Risk transfer.** Risk, once identified and accepted, may then be transferred to another person or entity. PAG § D.2.1 explains how such transfer can be accomplished among the PKI participants by a variety of contractual methods, covenants, representations and warranties, and indemnification provisions. PAG § E discusses other methods of shifting responsibility, such as tort law, *see* PAG § C.1 (Sources of Law), § C.2 (Agency Principles), and § C.5 (Consumer Issues and Privacy). An insurance policy is a special type of contractual indemnity that is attractive as a flexible vehicle for the transfer of risk *from* risk-adverse parties *to* an insurance company that is in the business of accepting risk. The risk-adverse parties are willing to pay a small insurance premium spread over an extended period of time, to be freed of a small probability of a potentially large unknown risk. See the discussion of PKI insurance coverage below in this section.

Risk Management and Tort Law

The common sense principles and practices of risk management are familiar themes in judicial decisions seeking to apportion tort liability. The famous case of *U.S. v. Carroll Towing Co.*[189] is instructive. A tugboat had broken loose from its mooring in a harbor during a storm, causing severe damage to other boats in the harbor. Judge Learned Hand articulated the following legal standard by

[188] *Cf.*, *U.S. v. Carroll Towing Co.*, 159 F.2d 169 (2d Cir. 1947).

[189] *Carroll Towing*, 159 F.2d 169.

which the jury might decide whether the owner of the tugboat was liable for the damage caused to the other boat. Both the terminology and the reasoning foretell the kind of risk management analysis that lawyers and judges are likely to use in arguing and deciding early litigation involving the liability of PKI participants:

> The owner's duty, as in other similar situations, to provide against resulting injuries is a function of three variables: (1) The probability that she will break away; (2) the gravity of the resulting injury, if she does; (3) the burden of adequate precautions. Possibly it serves to bring this notion into relief to state in algebraic . . . terms: if the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: i.e., whether B is less than PL.[190]

Insurance for PKI

Traditional products liability insurance provides "third-party" coverage for tort claims of third parties against the insured for bodily injury, personal injury, and tangible property damage. Errors and omissions insurance ("E&O"), on the other hand, is the traditional means by which insurers provide tort liability protection to suppliers of technology solutions against claims of economic or financial damages.

E&O insurance tailored to the special needs of CAs is increasingly becoming available from a limited number of leading insurers who specialize in PKI risks. Because of the technical and novel nature of PKI and the risks associated with it, it is understandable why such coverage is now becoming available. Insurers use a variety of methods to evaluate risks and how well risks are managed, in order to determines availability, limits, terms, and costs – but the most reliable method of underwriting a risk is *experience* with many insureds over a period of time lengthy enough to allow the law of big numbers to average out.

A certification authority may choose to tailor its warranty responsibilities to meet its needs and those of its community of interest, or the purposes for which the certificates are used. In this event, it is advisable to discuss with its insurer how coverage may be tailored to meet its needs. There is no inherent reason why, given enough experience, that all the risks of all the participants to a PKI might not ultimately be insurable, so that contingent risk exposure can be reduced to a predictable periodic premium.[191]

There appears some possibility that organizations adopting a PKI for some portion of their activities might actually reduce their overall E&O insurance premiums because of the ability to demonstrate reduced company-wide risk because its information security awareness has been heightened generally.

D. PAG PROVISIONS

This section of the PAG contains the provisions that constitute the main body of the document. This section closely follows the framework set out in RFC 2527. As a very brief review, RFC 2527 (and the PAG provisions in this section that follow) contain eight sections:

1) Introduction

2) General, Legal, and Business Considerations

3) Initial Validation of Identity and Authority

[190] *Id.*

[191] *See, e.g.*, VeriSign's NetSure Protection Program and Digital Signature Trust's TrustID Warranty plan, which provide a limited monetary amount of insurance-backed protection against a variety of PKI risks, *available at* <http://www.verisign.com/repository/netsure/index.html> and DST's program is described at <http://www.digsigtrust.com/certificates/warranty.html>.

4) Certificate Lifecycle Operational Requirements

5) Non-technical Security and Management Controls

6) Technical Security Controls

7) Certificate and CRL Profiles

8) Specification Administration

The PAG provisions provide a comprehensive set of information regarding the various elements of a PKI specified in RFC 2527 and a detailed commentary on each of those elements that should be considered when establishing or assessing a PKI or a PKI component. Each of these subsections within each section provides information that should be useful to entities both assessing and implementing PKIs.

The subsections within section D, with the exception of certain general headings, contain a common format to present guideline information about PKIs and their components. First, subsections contain an "Issue Summary." The Issue Summary is meant to state an issue without making specific recommendations. The issue dealt with by a particular section in this section D is the issue within the corresponding section of a PKI document, most likely a certificate policy or certification practice statement.

As an illustration, PAG § D.3.1.1 (Types of Names) begins, "This section concerns requirements or disclosures for how subject names must be or are composed within certificates issued by a CA." The reference to "this section" in this sentence means the section of a CP, CPS, or other PKI document covering types of names. If the PKI document follows the RFC 2527 framework, that section will be numbered 3.1.1. If not, the reference refers to the discussion of types of names appearing within a PKI's documentation regardless of the section number. In short, the issue summary is meant to raise an issue described in the corresponding section of a PKI's documentation.

Second, subsections in this section contain a discussion of "Relevant Considerations." The Relevant Considerations sections include background information about a particular issue or topic. They may also present a range of the possible options that a PKI may choose to adopt in response to an issue. Relevant Considerations are meant to be descriptive of what PKIs are doing. Finally, Relevant Considerations may also inform assessors what information they may wish to seek and what analyses they may wish to perform concerning an issue as part of their assessments. As with the Issue Summary sections, Relevant Considerations discussions do not provide specific recommendations.

Third, subsections of section D contain discussions entitled "Appropriate Requirements and Practices." Here, the PAG does provide recommendations as to a specific issue. These recommendations may be based on what are considered "best practices" within the industry or may refer to what PKIs typically do in response to an issue. Often, what is appropriate for a PKI will be highly dependent on the context in which the PKI operates, the applications for which the certificates issued are intended, the assurance level provided by the certificates, security requirements, needs for interoperability, and a host of other factors. If so, the "Appropriate Requirements and Practices" will note these variations, as well as the factors bearing on the issue.

In other cases, however, certain practices are so critical to PKI that PKIs will almost certainly want to adopt them, unless there is a very good reason to not to adopt them or to ignore the issue. An example is a subscriber's responsibility to safeguard the subscriber's private key. A core assumption in the use of a PKI is that subscribers will keep their private keys private. PKIs should ignore this issue only if they have a very good reason for doing so. Practices such as these are recommended in stronger terms than others that may depend on the circumstances of the PKI.

D.1 Introduction

This section introduces the applicable parties and policies within the PKI environment. It also defines the applicability of this guideline to stated application or business processes.

D.1.1 OVERVIEW

Issue Summary. This section provides an overview of the PKI, what kinds of certificates it offers, their purpose, and the participants within the PKI. This section may be used as an executive summary. Furthermore, it may also address the PKI's business model (*see infra* PAG APP 3 (Tutorial)), the context in which the PKI operates, and the PKI's ability to communicate this information through its marketing information and contracts. This section can also address the effectiveness with which the PKI's practice documentation introduces the nature, scope, and offerings of the PKI; its document architecture; and its adherence to standards. Finally, this section may address the PKI's treatment of certificate assurance levels or applications.

Relevant Considerations. Having a clear picture of a PKI's business model is the first step in any assessment process. At a minimum, the business model will dictate the level of security and assurances appropriate for the various aspects of the PKI's operations. It will also dictate how a PKI identifies the entities within it and allocates rights and obligations among them. Therefore, the assessor should, before doing anything else, identify the application for the PKI and identify the PKI's business model for securing the application (i.e., the computer information system or process that should, with a properly implemented PKI, accomplish the stated business objective).

Assessors should also obtain documents relevant to the PKI's business model, the most important of which are likely to be the PKI's CP or CPS. Other relevant documents include subscriber agreements, relying party agreements, vendor agreements, security policies, operational guides, and paper and electronic marketing materials and collateral. Assessors should review these documents to determine the way in which the PKI communicates its business model to participants in the PKI. Among possible questions to ask are:

- Do the documents clearly describe basic business terms and the nature and scope of the business model?
- Do the documents clearly describe the service or product offerings of the PKI?
- Are the documents suitable for the PKI? Do they accurately describe the nature of the PKI and the business model?
- Does the PKI communicate its documented architecture? That is, does the PKI identify the documents setting forth PKI requirements, how entities must meet these requirements, and entities' legal rights and obligations? Does the PKI disclose which documents are publicly available?

Finally, assessors should take note of overviews and summaries within PKI practicedocumentation. They should determine whether they clearly introduce and accurately describe the nature of the PKI and its purpose.

Appropriate Requirements and Practices. Overviews are appropriate locations for PKIs to summarize the applicability of certificates to specific assurance levels or applications. For example, a PKI offering multiple classes of certificates may place a description of the classes and the basic differences among them within a CP's overview. Other PKIs may have a CP for a specific industry or community of interest. In this case, the CP's overview is an appropriate place to disclose the relevant industry or community of interest, the security applications contemplated, and state that the certificates in the CP are appropriate for these applications. In

general, overviews within documentation are a good place to discuss a PKI's product and service offerings at a high level.

PKIs should communicate the nature and scope of their business models clearly and effectively in their CPs, CPSs, and marketing materials. They should utilize clear and precise agreements among the parties (such as subscriber agreements or relying party agreements) to communicate basic business terms, as well as the parties' respective rights and obligations.

D.1.2 POLICY IDENTIFICATION

Issue Summary. This section addresses the PKI's efforts to identify its policy and practice documentation and to state how and where the documentation is registered.

Relevant Considerations. Assessors should check the PKI's CP and/or CPS to see how it identifies its policies and documentation. A PKI may have a single policy or a single set of practices and may designate a name for it. A PKI may also have multiple policies or sets of practices. These multiple policies and practice sets may appear in a single document naming the discrete policies or practice sets, or the PKI may use multiple documents to set forth these policies and practices.

Appropriate Requirements and Practices. PKIs should clearly identify their applicable policy documentation. If a PKI has multiple policies or sets of practices, as in the case of multiple classes of certificates, the PKI should identify each policy or practice set and whether or not they appear in a single document or multiple documents. The PKI should explain the relationship among the different policies and practice sets.

D.1.2.1 Alphanumeric identifier

Issue Summary. This section addresses the PKI's efforts to identify its policy and practice documentation in text. More precisely, it concerns the PKI's use of document titles or the names of a policy or set of practices within one or more documents.

Relevant Considerations. Assessors should check the PKI's CP and/or CPS to see if its documentation has appropriate titles. Assessors should determine if the PKI identifies its documentation to interested persons. If the PKI has multiple policies or practice sets, the assessor should check to see if they appear in a single document or in multiple documents. If they appear in a single document, assessors should check to see how the PKI identifies the multiple policies or practice sets with a title within the document. If multiple policies or practice sets appear in multiple documents, the assessor should check to see if the PKI identifies these multiple documents. Once an assessor has identified the relevant titles, the assessor should determine whether the titles are accurate and descriptive of the policy or practice, as well as its context.

For example, if a PKI has a set of high-level requirements for the PKI in a document that approximates a CP, does the title actually say the document is a CP? In other words, policies for certificates having various levels of assurance for use with the Government of Canada would best appear in a document entitled something like "Digital Signature and Confidentiality Certificate Policies for the Government of Canada Public Key Infrastructure." Policies for various levels of assurance within that document would best have titles matching the application and level of assurance. By contrast, a title like "XYZ, Inc. Certification Practice Statement" would obviously not be appropriate in this context.

Appropriate Requirements and Practices. PKIs should clearly identify policy and practice documentation with titles that match the context of the PKI. If a PKI has multiple policies or practice sets, as in the case of multiple classes of certificates, the PKI should identify each policy or practice set with an appropriate alphanumeric title and clarify whether they appear in a single document or multiple documents.

D.1.2.2 Object Identifier (OID)

Issue Summary. This section addresses the PKI's efforts to identify its policy and practice documentation or the policies or practices within the documentation using an object identifier (OID) or multiple OIDs.

Relevant Considerations. Assessors should determine if the PKI makes proper use of OIDs to identify its policy and practice documentation. An OID is a unique number designated by a PKI based on a root number registered within the American National Standards Institute within the United States or, outside the United States, within the applicable national registration authority.[192] A PKI may wish to place the OID of the applicable CP within an X.509 version 3 certificate. The certificate policies extension within the X.509 specification is intended to contain the OID of the applicable CP.[193]

By placing an OID of a CP within a certificate's certificate policies extension, the CA issuing it is asserting that the CP is the policy under which the certificate was issued and the certificate is appropriate for the applications described in the CP.[194] The OID can facilitate the use of machine processing of certificates by relying parties. That is, if a relying party wants to accept only certificates that adhere to a certain CP, the relying party can program its software and devices to allow only subscribers having certificates containing the OID of the appropriate CP to interact with the relying party's software or device.[195] The relying party can also program its software and devices with a list of acceptable OIDs to permit subscribers having a certificate with any one of the acceptable OIDs to interact with the relying party's software or device.

An example of this process is the use of digital signatures and a certificate to make a large purchase or a funds transfer, which would require high-assurance certificates and a corresponding high-assurance CP. The PKI may issue certificates to subscribers who are customers of the organization operating the PKI. In this case, the certificates will contain an OID corresponding to the PKI's CP, which sets forth the policies relating to the use of digital signatures on records of these high-value transactions. When a browser submits a signed transaction to a server of the organization operating the PKI, the application on the server will attempt to look up the user's certificate or examine the certificate presented. A necessary condition of proceeding with the transaction would be a check to ensure that the user's certificate contains the proper OID of the PKI's high-assurance policy.

The X.509 specification's establishment of the certificate policies extension was for the purpose of facilitating this kind of application. PKIs may, however, be unable to take advantage of this kind of process for several reasons. First, this process assumes that the relying party has done an analysis to develop or determine an appropriate policy, has chosen one or more CPs as stating appropriate policy, and has programmed its software or devices to require the presence of the OIDs corresponding to these CPs as a necessary condition of processing the transaction. Alternatively, the relying party could require the presence of an acceptable internal policy and, through the policy mappings extension, declare an external policy to be the equivalent to an internal policy. In either case, however, a critical assumption is that the relying party has identified a set of policies that would be acceptable. None of the foregoing assumptions may be true, though. With strangers interacting over the Internet for the first time in a transaction, the relying party's application may not recognize the OID in the

[192] *See* Ford, *supra* note 31 at 219.

[193] *See* Internet X.509 Public Key Infrastructure Certificate and CRL Profile, available at: <http://www.ietf.org/ids.by.wg/pkix.html>.

[194] As discussed *supra* PAG § D.7.1.6 (Certificate Policy Object Identifier), § D.8.1 (Specification Change Procedures), and § APP 3.3 (Tutorial on PKI Documentation). As a practical matter it would be very difficult for any community using the CP-OID processing features of the X.509 standard if all members of the community were required to change over their certificates and applications to a new OID to accommodate minor changes in the CP. Thus, when a CA asserts an OID in a certificate, the CA is asserting that the certificate was issued in accordance with the provisions of the policy in force at the time of issuance, but that it is being managed in accordance with the current version of the CP. For example, if a CP in the year 2001 states that identification proofing for a medium assurance certificate is performed using face-to-face registration using two picture IDs, and then the CP is changed in the year 2002 to require three picture IDs, the CA should not need to assert a new OID.

[195] See *supra* note 187.

certificate policies extension of certificates received in messages or other transactions as an acceptable policy. The persons configuring the application may not have included any given certificate's policy OID on the list of acceptable OIDs. Also, it may not be possible to track down the document corresponding to the OID. And the relying party may not be able to anticipate which OIDs to program into its relying party software even if the relying party hoped to do so.

The second reason why the use of OIDs may not be possible is that most relying parties, such as individuals using S/MIME or providing credit card information to web sites using SSL, likely neither have the skills nor the interest in programming their applications to configure software to check for specific OIDs. They may not understand what an OID is, to say nothing of configuring software to seek particular OIDs as a step in the process of reliance. Machine programming by relying parties is much more likely when the relying party is an organization that has the resources and inclination to program servers interacting with a large number of subscribers.

Third, most client software[196] has not developed to the point where it can easily process OIDs. The placement of OIDs in certificates is meant to facilitate the automated processing of OIDs by the relying party software. Commonly used client software, however, may not perform these functions. Even if a relying party tried to process the OID manually by looking at the OID within an extension and matching it against a list of acceptable OIDs (which is not the intended method of processing OIDs), the software may not even be capable of displaying the OID at all. Other software may display the correct OID, but may not explain what it is. Also, the software would not point to the document to which the OID refers. The software may merely show the number. Consequently, even if a relying party wanted to check an OID manually to determine if it corresponds to an acceptable policy, the relying party may be unable to do so.

Finally, a PKI may not have the need or ability to place the OID of a CP in the certificate policies extension. For example, the PKI may have no CP at all. In this case, the PKI may wish to place the OID of its CPS in the certificate policies extension. In addition, for some low-assurance or limited-use PKIs, the CA may perceive no need to populate extensions at all, including the certificate policies extension. The need to populate the certificate policies extension with an appropriate OID will depend on the assurances that the PKI hopes to provide.

Appropriate Requirements and Practices. If a PKI is intended to facilitate the use of machine processing of OIDs by relying party applications, the PKI should ensure that the OID appears in the certificate policies extension of the certificates it issues and should document the identity of the OID in its CP and/or CPS. If the PKI does not know whether or not relying parties will be processing OIDs, or it wishes to give relying parties the flexibility to do so, the PKI may find it helpful to place the OID of the CP in its certificates and document the OID in the CP and/or CPS.

Assuming the PKI uses OIDs, the PKI should ensure OIDs related to the specific CP (or other document) are unique and are registered with a recognized OID registration body (ANSI, OSI). In addition, a CA's CPS should disclose the CPs that the CA supports, as well as the OIDs corresponding to these CPs.

D.1.3 COMMUNITY AND APPLICABILITY

Issue Summary. This section addresses a PKI's business model in depth. It concerns the PKI's identification of the parties participating within the PKI, such as certification authorities, registration authorities, subscribers, and relying parties. This section also describes the possible applications for certificates within the PKI. Specifically, it identifies the applications for certificates within the PKI. The section may address approved applications, permitted applications, restrictions on the use of certificates to certain applications, or prohibited applications for which certificates shall not be used.

[196] *See infra* PAG APP 5 (Proposed Guidance for Development of Compatible End-User Products).

Relevant Considerations. Two main topics are tied directly to a PKI's business model, namely the "community" of participants within a PKI and the "applicability" of certificates used by that community.

"Community" refers to the different parties participating within a PKI. As part of an assessment of a PKI and its business model, assessors should identify the parties that are acting in the role as certification authorities, registration authorities (if any), subscribers, and relying parties. Assessors may find that a PKI contains more than one kind of CA, RA, subscriber, or relying party. In addition, some of the functions of certification authorities and registration authorities may be divided among different entities, such as customers and outsourcing vendors. For example, in some business models, there may be a certificate manufacturing authority or repository service separate from a CA. The PKI should document any such divisions of responsibility. In any case, assessors should determine whether the PKI clearly communicates to interested parties who the participants within the PKI are. In this regard, assessors should read the PKI's CP and/or CPS to review the descriptions of these various participants. More details concerning specific categories of these participants appear in the subsections below.

"Applicability" refers to the applications for certificates issued within the PKI. A good place to discuss applicability is in a CP. The X.509 standard defines a CP as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with a common security requirement."[197] In other words, with respect to "applicability," part of a CP's purpose may be to designate that certificates issued within the PKI are intended, good, acceptable, and so on for certain specified applications. Assessors should review a CP or other PKI documentation to determine if it clearly states the applications for which certificates are intended.

Beyond the context of a CP, assessors should review the PKI's other policy and practice documentation to determine what they state about possible applications for certificates. Does the documentation describe the applications for which certificates are intended? Some PKIs may permit a range of possible applications. Therefore, assessors should determine if the PKI discloses a range of permissible applications for certificates. In some PKIs, the PKI may wish to limit the use of certificates to certain applications. In this case, assessors should review the PKI's documentation to determine if limitations on the use of certificates are stated clearly. A PKI may also wish to prohibit certain applications explicitly. In that case, assessors should review the documentation of such prohibitions and determine if the PKI has stated these prohibitions clearly.

Appropriate Requirements and Practices. A PKI's documentation should, in general, help potential users and customers understand the PKI's business model. If made publicly available,[198] CPs and CPSs should give readers enough information about a PKI's business model to permit them to make informed evaluations and decisions. For example, in the case of a CPS used by relying parties to determine if they want to trust certificates issued pursuant to it, the CPS should disclose enough of the PKI's business model to permit relying parties to make an informed trust decision.

More specifically, a PKI's documentation should identify the participants within the PKI and the applications for which certificates may or should be used. If the PKI has a need to limit the use of certificates to certain applications or to prohibit certain applications, the PKI should clearly document these limitations or prohibitions and ensure that subscribers and relying parties have adequate notice of them.

[197] *See* RFC 2527, *supra* note 193.

[198] A PKI policy document (particularly a CPS) may contain a significant amount of confidential information and thus may not necessarily be appropriate to release publicly. Despite this fact, a CA still should provide enough information to relying parties to permit a decision of whether or not to trust digital signatures from a subscriber from that CA's PKI.

D.1.3.1 Certification authorities

Issue Summary. This section addresses entities playing the role of a certification authority (CA) within a PKI. Specifically, it addresses how a PKI allocates CA functions to one or more entities and how it communicates the allocation of functions among these different entities.

Relevant Considerations. The universe of possible CA functions is generally considered to include:

1) Key management functions, such as the generation of CA key pairs, the secure management of CA private keys, and the distribution of CA public keys;

2) Establishing an environment and procedure for certificate applicants to submit their certificate applications (e.g., creating a web-based enrollment page);

3) The identification and authentication of individuals or entities applying for a certificate;

4) The approval or rejection of certificate applications;

5) The signing and issuance of certificates in response to approved certificate applications;

6) The publication of certificates in a repository, where certificates are made available for potential relying parties;

7) The initiation of certificate revocations, either at the subscriber's request or upon the entity's own initiative;

8) The revocation of certificates, including by such means as issuing and publishing Certificate Revocation Lists ("CRLs") or providing revocation information via Online Certificate Status Protocol ("OCSP") or other online methods; and

9) The identification and authentication of individuals or entities submitting requests to renew certificates or seeking a new certificate following a re-keying process, and processes set forth above for certificates issued in response to approved renewal or re-keying requests.

In certain simple PKI business models, there may only be three parties: a subscriber, a relying party, and a CA acting as a trusted third party.[199] Under this model, the CA has the responsibility to perform all of the functions above. Although all of these responsibilities can be performed by a single entity, PKIs are being developed and implemented in which some of these responsibilities are performed by one or more different entities.

For example, CA responsibilities can be divided into "front-end" functions involved with having direct contact with certificate applicants and subscribers, and "back end" functions involved with key operations and management, and certificate management. Front-end functions include facilitating the submission of certificate applications, identification and authentication, certificate application approval or rejection, the initiation of revocations, and the approval or rejection of renewal or re-key requests. Back-end functions can include key management, the signing and issuance of certificates, repository functions, and the revocation of certificates including the generation and publication of revocation information.

In some PKIs, the CA may separate front-end from back-end functions by delegating front-end functions to a Registration Authority and retain for itself the back-end functions. An example of this business model would be a CA that retains an RA service to perform front-end functions for it. Alternatively, the RA may be a customer of the CA purchasing certificates in bulk, which takes on registration authority functions to leverage

[199] An even simpler variation on this model is where the relying party and the CA are the same entity, such as, for example, a government CA.

identification and authentication information that it holds through its close relationship with certificate applicants and subscribers.

In other PKIs, an entity may want to have the nominal status of CA, perhaps for the purpose of having its branding information within certificates, but may not wish to perform back-end functions itself. The entity may feel comfortable only performing front-end functions. In that case, the entity may agree to perform all the functions of CA, but would outsource back-end functions to a PKI vendor. The entity is left with performing the remaining CA functions, that is, the front-end functions. The outsourced vendor performs the back-end CA functions of minting the certificates. Since the entity outsourcing this function to the vendor is the nominal CA, the vendor cannot be called the CA. In this context, the vendor is sometimes referred to as the "certificate manufacturing authority."

In yet other PKIs, different divisions of responsibility are possible. For instance, the repository functions of publishing certificates and revocation information may be separated from the remaining CA functions and performed by another entity. In addition, a CA may delegate RA functions to an entity that approves or rejects certificate applications, but the RA functions are further subdivided so that a notary or other entity with a relationship to the certificate applicant that is even closer than the RA's performs the identification and authentication functions. In some contexts this entity is, in essence, a sub-RA or Local Registration Authority ("LRA").

Regardless of how these responsibilities are divided or denominated, assessors should read the PKI's policy and practice documentation (along with related documents) to see how the CA functions are identified and allocated among various entities. The assessor should determine if the relevant entities are identified and if their respective roles are clear. The assessor should also review agreements to determine if all CA functions are accounted for and if they clearly state the respective roles of the entities performing CA functions.

Appropriate Requirements and Practices. PKIs should carefully consider whether the responsibilities of a certification authority must be performed by separate entities. For example, a CP that allows the CA-related responsibilities to be performed by one or more entities enables the widest variety of certification authorities to implement the CP. On the other hand, mandating a specific CA implementation model, such as the management of the registration authority and repository responsibilities by a separate entity,[200] will prevent certification authorities who do not conform to such a model from being able to comply with the CP. While CPs do not need to specify the use of a specific CA-implementation model, writers of CPSs will more than likely want to specifically address whether the responsibilities of a certification authority will be performed by a single entity, or whether they will be performed by separate entities such as registration authority, certification manufacturing authorities, and a repository.

Regardless of the CA-implementation model, the PKI should clearly disclose which entities are performing CA functions and how these functions are allocated. The PKI's agreements should implement these functional allocations. The roles of all entities performing CA functions should be clear.

D.1.3.2 Registration authorities

Issue Summary. This section addresses the entities that act as registration authorities within a PKI. Specifically, it can address how a PKI allocates functions between CAs and RAs and how it communicates the roles of entities performing CA and RA functions.

Relevant Considerations. As discussed above, registration authority functions are a subset of certification authority functions. There are nine CA functions, of which five are identical to RA functions in this section. In

[200] *See* PAG APP 2 (*Certificate Authority Rating and Trust (CARAT*) *Guidelines*, §§ C.2.1, C.2.5 *et seq*., NACHA Internet Council (27 Oct. 1998), *available at* <http://internetcouncil.nacha.org/projects/default.html>, hereinafter "CARAT Guidelines").

many, if not most contexts, RA functions are considered to be "front-end" functions involving direct contact with certificate applicants and subscribers that leverage the RA's greater knowledge of the certificate applicants and subscribers (compared to the CA) and its direct relationship with them. The five CA functions that are also RA functions are the following:[201]

- Establish an environment and procedure for certificate applicants to submit their certificate applications (e.g., creating a web-based enrollment page);[202]
- The identification and authentication of individuals or entities who apply for a certificate;[203]
- The approval or rejection of certificate applications;[204]
- The initiation of certificate revocations, either at the subscriber's request or upon the entity's own initiative;[205] and
- The identification and authentication of individuals or entities submitting requests to renew certificates or seeking a new certificate following a re-keying process and processes set forth above for certificates issued in response to approved renewal or re-keying requests.[206]

As mentioned in section D.1.3.1, in simple PKI models, there may not be any separate RAs, that is, entities that perform RA functions separate from the CA. Or, the CA may perform all the CA functions listed in section D.1.3.1, including the RA functions. Nonetheless, in some business models, there may be a need for separate RAs.

Regardless of how these responsibilities are divided, assessors should read the PKI's policy and practice documentation to see how the RA functions are identified and allocated among various entities. Assessors should determine if the relevant entities are identified and if their respective roles are clear. Assessors should also review agreements to determine if all RA functions are accounted for and if they clearly state the respective roles of the entities performing RA functions.

Appropriate Requirements and Practices. PKIs should carefully determine whether it makes sense to have RAs and should allocate roles and responsibilities between CAs and RAs in a way that achieves the goals of the PKI's business model. Regardless of the business model, the PKI should clearly disclose which entities are performing RA functions and how these functions are allocated. The PKI's agreements should implement these functional allocations. The roles of all entities performing RA functions should be clear.

D.1.3.3 End entities

D.1.3.3.1 Subscribers

Issue Summary. This section addresses the identity of the permitted individuals or organizations that may be subscribers, and possibly the individuals authorized to control the private key of a device, application, or role.

[201] All of these functions are the covenant type of responsibility rather than the representation/warranty type, in accordance with the distinction among these set forth below in PAG § D.2.1 (Apportioning Legal Responsibilities and Potential Liability Among the Parties to a PKI Transaction).

[202] *See* PAG § D.1.3.1 (Certification Authorities) corresponds to CA function #2.

[203] *Id*., corresponds to CA Function #3.

[204] *Id*., corresponds to CA Function #4.

[205] *Id*., corresponds to CA Function #7.

[206] *Id*., corresponds to CA Function #9.

Relevant Considerations. A subscriber is a person who (1) is the subject named or identified in a certificate issued to such person, and (2) holds a private key that corresponds to a public key listed in that certificate.[207] As a "person," a subscriber may be either a natural person, that is, an individual human being, or a legal person, such as a corporation.[208] When a certificate is issued to a device, such as a web server, the device may be the one named in the certificate and the one holding the private key. Therefore, the device could be considered a subscriber,[209] although from a legal perspective, it may be preferable to consider the subscriber to be the organization that controls the device.

Other persons that may be discussed in this section include:

- Individuals who are authorized to control the private key of a device or application. Although, it is possible to deem that the organization controlling a device or application is the subscriber, the organization can only act through individuals. Therefore, if only a special or a restricted class of individuals is permitted to operate the device or application controlling a private key, it may be helpful to mention that class here.

- Individuals who are authorized to control the private key assigned to a role. A certificate may be issued to a role, such as "Officer on Deck" in the naval context. There may be three shifts of personnel controlling a ship, each of which has an Officer on Deck. It may be helpful, depending on the PKI, to give each of the three individuals who could be Officer on Deck during a day control of a certain private key and issue a certificate to that role, which all three individuals share.

Assessors should check to determine if the PKI identifies the types of persons who are subscribers within the PKI. The types of persons that are permitted to become subscribers will vary depending on the type of PKI. PKIs established to provide widely deployed services to the general public might not have any restrictions on who may apply for a certificate. By contrast, PKIs intended to service the members of a specific community of interest, such as a company, university, club, or other organization may restrict the class of permissible certificate applicants to these members.

In performing this analysis, assessors may want to obtain answers to the following questions:

- Are the subscribers individuals or organizations?

- If the subscribers are organizations, what are the devices or applications that operate the private key whose corresponding public key appears in the certificate?

- Is there a business need for imposing a requirement that subscribers have some kind of an affiliation with the CA or RA?

- Are certificates issued to a role, and if so, what is the class of persons who can fill that role?

Appropriate Requirements and Practices. A PKI should make it clear who are the parties permitted to apply for and obtain certificates within its domain. For example, a PKI encompassing a university may want to document potential subscribers by the following policy statement, "Subscribers within the University X PKI include the faculty, staff, students, and alumni of University X." If the subjects of certificates are not natural persons, then the PKI should clarify who the subscriber is for purposes of the PKI. Where certificates are issued to roles, the PKI should describe the persons who fit the roles.

[207] *See* DSG, *supra* note 2, § 1.31.

[208] *Id*., § 1.23.

[209] *Id*.

When certificates support e-mail applications, subscribers are generally the persons who send digitally signed e-mail and receive encrypted e-mail. For applications requiring digitally signed transactions, the subscribers are the persons indicating assent to the transaction through a digital signature. With respect to authentication, subscribers are the persons being authenticated. They may be persons using client software or servers, depending on the application. Client authentication may be used to control access to protected information, and server authentication (*e.g.*, SSL) is used to authenticate the server to provide assurances of the identity of the organization operating the server.

D.1.3.3.2 Relying Parties

Issue Summary. This section addresses the identity of the permitted individuals or organizations that may be relying parties within a PKI. Where devices or organizations are relying parties, there may also be a discussion concerning the individuals who can act on behalf of the organization or who can operate the devices that perform relying party functions.

Relevant Considerations. A relying party uses a certificate to obtain the public key within it and is in a position to rely upon the assurances of the certificate that the public key is associated with a certain identity and/or attributes. When an individual is relying on a certificate for his own business or personal use, the individual is the relying party. When an individual is acting on behalf of an employer or other principal, however, the employer or principal is the relying party, and devices and applications relying on certificates are purportedly under the control of an organization and individuals acting on behalf of that organization. In that case, while the device or application performs relying party functions, it may be preferable from a legal perspective to say that the controlling organization is the relying party.

Assessors should determine whether the PKI has stated which classes of persons, either individuals or organizations, are permitted to rely upon certificates within the PKI. There may be a range of possible relying parties depending upon the business model of the PKI. In an open PKI, there are no restrictions on who may act as a relying party. In specific, a relying party is not required to be a subscriber of a certificate within the PKI. Within other PKIs, the class of potential relying parties may be limited to members of a certain organization or class, or to people bound to the CA by contract. It is also possible for the relying party to be the CA itself or a RA.

The purpose of specifying the intended relying parties (in the CP (and identifying the CP in the certificate) is to put third party strangers on notice and protect the CA and other participants in the PKI from claims for damages resulting from misplaced reliance by such third parties on the certificate. For example, if the CP states that certificates are issued to employees and intended to be relied upon only by the employer, and then a third party suffers a major loss because of reliance on the certificate (e.g., employee's fraud on a third party unrelated to the employer's business), then the employer may be protected based on lack of privity with the third party. *See* PAG § C.1 (Sources of Law) *supra.*

Appropriate Requirements and Practices. A PKI should make it clear who are the parties permitted to rely upon certificates within its domain. For example, a PKI encompassing a university may want to document relying parties by a policy statement such as, "Relying parties within the University X PKI include the faculty, staff, students, and alumni of University X."

When certificates support e-mail applications, relying parties are generally the persons who must verify digital signatures on digitally signed e-mail and send encrypted e-mail. Often, relying parties in the secure e-mail context are themselves subscribers so that mail can be sent back and forth, but having a certificate is not necessary to become a relying party. For applications requiring digitally signed transactions, the relying party who receives the digitally signed transactions must act in reliance on the digital signature. With respect to authentication, relying parties are those granting access to protected information based on a certificate or entering into a transaction with the organization operating a server in reliance on the certificate.

D.1.3.4 Applicability

Issue Summary. This section relates to the general purpose as well as particular environment, business function, or specific application for which the certificates may be used.

Relevant Considerations. This section permits the reader to clearly know permitted uses of the certificate. This involves a description of two elements. The first element is the "nature" of certificate use (i.e. digital signature or confidentiality); the second element is a list or description of approved or prohibited applications.

Appropriate Requirements and Practices. This element should contain a description of: (a) the general type of applications or business functions that are suited to the use of certificates issued under this policy, (b) the specific applications or business functions where the use of certificates issued under this policy is approved, and (c) the specific applications or business functions where the use of certificates issued under this policy is specifically prohibited.

The following is an example:

> This policy is suitable for the integrity and authentication of transactions or communications. Certificates issued by the CA may be used for the following types of applications:
>
> 1. Information Publication;
> 2. Forms Submission;
> 3. Correspondence;
> 4. Application work-flow;
> 5. Electronic commerce.
>
> Certificates issued under this policy may be used only with applications that, as a minimum, meet the following requirements:
>
> 1. Correctly establish, transfer and use the public and private keys;
> 2. Are capable of performing the appropriate certificate validity and verification checking; and
> 3. Report appropriate information and warnings to the Subscriber.

If considered appropriate, this element could be further broken down into three subsections: suitable applications, approved or restricted applications, and prohibited applications.

D.1.4 CONTACT DETAILS

D.1.4.1 Specification Administration Organization

Issue Summary. This element describes the organization that is responsible for drafting and updating the CP, CPS, or other document.

Relevant Considerations. The purpose of this section is to provide readers of a CP, CPS, or other PKI-related document with the identity of the organization that drafted the document. Such information would enable the reader to know who is imposing requirements or making disclosures in the document. It would also enable the reader to contact the organization in the event the reader had a question or concern. Assessors should check this section of the PKI's documentation to ensure that the PKI provides accurate and complete information concerning the organization administering the CP, CPS, or other document.

Appropriate Requirements and Practices. PKIs will generally want to disclose the name of the organization administering a CP, CPS, or other PKI-related document. Naming the organization amounts to disclosing the author of the document. Knowing the author, the reader can know who is responsible for it and the associated PKI. Also, where a reader finds it necessary to cite or quote the document, the reader can know to whom to attribute the document.

Some PKIs may want to establish a committee or group to manage the document. Some PKIs, for example, utilize a "policy management authority" or "PMA." Where the document is the result of a process of consensus among various organizations, it may be useful to have an umbrella organization like a PMA in charge of a practice document. In other instances, such as a PKI that serves a single organization, a PMA is unnecessary. The organization itself can write and maintain the document. Whether a PMA or committee is helpful to draft the document will depend on the context.

D.1.4.2 Contact person

Issue Summary. This section addresses the contact information of a person that interested parties can contact to obtain copies of a CP, CPS, or other policy and practice information, or ask questions concerning such a document or this information.

Relevant Considerations. Assessors should determine whether a PKI has provided the name of a person to contact in case the reader has questions or concerns about a CP, CPS, or other document. Assessors may find it helpful to determine if the contact person is someone with direct responsibility over the particular document, or someone who can readily get questions answered. Finally, assessors should determine if this section provides enough information to allow readers to contact this person conveniently.

Appropriate Requirements and Practices. In general, it is helpful for a PKI to provide the name of a person that a reader of one of its documents can contact with questions or comments. In particular, it may be helpful to coordinate this section with the section calling for a contact for purposes of providing notice (*see* PAG § D.2.4.2 (Miscellaneous Provisions)), or with the section relating procedures by which amendments to a document can be proposed to a PKI (*see* PAG § D.8.1 (Specification Change Procedures). In addition, it is more helpful to name as contact person someone with direct responsibility over the document, since readers may pose detailed questions concerning the document. Although the means by which a contact person needs to be reached will vary with the PKI, this section should generally contain the person's position or title, and the person's phone number and e-mail address.[210] A physical address would be helpful as well.

D.1.4.3 Person determining CPS suitability for the policy

Issue Summary. The purpose of this section is to identify the person who will be comparing a CPS with a policy document, *i.e.* a CP, and determining whether the CPS is "suitable" for the CP. In this context, "suitable" means that the practices adopted by a CA and documented in its CPS fulfill the requirements defined in the CP.

Relevant Considerations. This section is useful in the context of interoperation, either through cross-certification, unilateral certification, or other forms of interoperation.[211] When a CA wishes to begin interoperation with an existing PKI, the PKI will want to undertake procedures to ensure that this CA meets the

[210] Depending on the circumstances, it may or may not be appropriate to identify an individual by name. A CP or CPS should not require modification merely because a person is rotated out of a job or is no longer the contact person. Rather, a role (e.g., General Counsel, Director, etc.) might be appropriate in such circumstances.

[211] The process of submitting a CPS may be looked at as part of a four-step process: 1) the CP is the requirements document (e.g., the RFP), 2) the CPS is submitted as a proposal defining the CA's implementation of the requirements, 3) the CPS is evaluated as deficient or compliant in meeting the requirements of the CP, and 4) an audit of the actual implementation is performed using the CP and CPS references.

PKI's trustworthiness requirements. Under § D.8.3 of the PAG (Approval Procedures for CPSs and Other Practice Documents), the PKI may require the CA to submit its CPS to the PKI for approval. This approval process will be based in part on whether the practices of the CA documented in its CPS meet the requirements of the PKI's CP. The purpose of this section is to identify the person who will be doing this comparison and analysis. The person determining suitability of a CPS for a policy makes the ultimate determination of whether the CA to whom the CPS applies will be permitted to interoperate with the PKI and issue certificates that purport to comply with the PKI's CP.

Of course, if interoperation is not taking place and no CA's CPS will be compared with another organization's CP, this section and PAG § D.8.3 (Approval Procedures for CPSs and Other Practice Documents) will likely not apply. Therefore, assessors should first determine whether this section needs to be utilized at all. If so, assessors should check to see if a person, group, or organization is named in this section. In addition, appropriate considerations for a PKI assessor regarding the person determining CPS suitability could include: whether the person has a strong PKI background, whether the person will be working individually in making the suitability determination or whether it will be a team of people, and whether the person was involved in the original authoring of the CP. Finally, assessors should determine whether or not this section provides enough information to allow CAs interested in submitting a CPS for approval to contact this person conveniently.

Appropriate Requirements and Practices. This section of PKI documentation should be used only where it is appropriate, that is, in the context of procedures relating to interoperation where a CA submits a CPS to a PKI for its review to determine if the CPS complies with a specific CP. The person named in the section should also have sufficient training and experience with PKI to make a judgment as to whether or not the practices of a CA disclosed in its CPS comply with the applicable CA. Moreover, while the means by which a potential CA can contact this person will vary depending on the PKI, at a minimum, this section should contain a phone number and e-mail address for the person receiving and evaluating CPSs of CAs wishing to interoperate with the PKI. A physical address would be helpful as well.

D.2 General, Legal, and Business Provisions

Section D.2 of the PAG considers certain legal and business issues of PKI. Throughout this section, the emphasis is primarily upon legal and business-oriented issues, in contrast to the more technical focus and tone beginning in PAG § D.3 (Initial Validation of Identity, Authority and/or Other Attributes). This is not to suggest only lawyers and business management should consult § D.2, or that PAG §§ D.3 through D.8 are only for technologists. To the contrary, all of these sections constitute the core of PKI principles essential to a practical understanding of them by all interested communities. In order to better suit the presentation of the subject matter, the format of this section differs somewhat from the format of corresponding § D.4.2 (General Provisions) of "the checklist of topics for consideration by the certificate policy or CPS writer" set forth in RFC 2527[212].

D.2.1 APPORTIONING LEGAL RESPONSIBILITIES AND POTENTIAL LIABILITY AMONG THE PARTIES TO A PKI TRANSACTION

Issue Summary. The purpose of this section is to introduce additional legal terminology and give an overview of the legal *responsibilities* and potential *liability* of the various participants in a PKI transaction: CAs, RAs,

[212] *See* RFC 2527, *supra* note 193.

subscribers, relying parties, repositories, and others.[213] Drawing on principles introduced in PAG § C.1 (Sources of Law), *supra*, this section distinguishes between *contractual responsibilities* that participants voluntarily accept by agreement, and *tort responsibilities* that may be imposed on participants by tort law. *Representations*, *warranties*, and *covenants* are three different types of contract clauses used to create contractual responsibility. They are found in PKI agreements as well as in CPs, CPSs and other PKI documents that are *incorporated by reference* in PKI agreements. Finally, this section deals with the potential liability of participants that results from breached responsibilities, including any contract provisions that can serve to limit *liability*. The individual subsections D.2.1.1 through D.2.1.5 set forth the responsibilities and liability-related provisions applicable to the individual participants within a PKI transaction, with particular emphasis upon the content in (or incorporated by reference in) PKI agreements that determine contractual responsibilities and potential liability.

Relevant Considerations. Parties to an agreement typically accept contractual responsibilities by contract clauses having three different types of content: *representations*, *warranties* and *covenants. Representations and warranties* are promises that a statement is correct, or a state of affairs exists, as of a particular time identified in the agreement. Representations and warranties of a party are usually lumped together in the same section of an agreement, but there are differences. Representations usually refer to the correctness of a statement or the existence of a state of affairs as of a past or a present time, and warranties usually refer to a continuation of correctness or the continued existence of a state of affairs into the future.[214] *Covenants* of a party, on the other hand, are promises as to future *conduct* of a party, either a promise to do certain things (an affirmative covenant) or to refrain from certain conduct (a negative covenant).[215]

In a PKI agreement (or in a CP, CPS or other document incorporated by reference in an agreement), the elements of PKI functionality assigned to PKI participants under PAG § D.1.3 (Community and Applicability) *supra*, are best converted to legal responsibilities when expressed by the *covenant* type of clause rather than by representations and warranties. This is true because covenants in a PKI document are promises as to future conduct, namely promises to perform[216] particular PKI functions in the future. Accordingly, the list of a particular participant's covenants in PKI agreements and other documents can elucidate the architecture or business model of the PKI, and is a good place for an assessor to begin when reviewing a PKI.

Assessors should also consider the *representations and warranties* made by each participant in a PKI agreement or in other documents incorporated by reference in a PKI agreement. Unlike PKI covenants (promises of what functions the participant will perform), PKI representations and warranties tend to express criteria for determining the adequacy of such performance.

For example, a CA or an RA might covenant to perform the function of identification and authentication of entities applying for a certificate. That same participant might also represent and warrant to relying parties that such identification and authentication of certificate applicants is and will in the future be (and possibly also has been in the past) *accurate*, or that the function of identification and authentication will be *performed*

[213] The use of the phrase "PKI transaction" is intended to refer to a PKI-created record, whether or not "relating to a transaction" governed by E-SIGN §101(a), and notwithstanding the distinction between transactions and records under E-SIGN § (d)(2). "PKI transaction" also includes any use of a PKI system. *Id*.

[214] An example of a representation would be, "seller represents that the equipment is free of defects, as of the date of this Agreement." An example of a warranty, by contrast, would be, "seller warrants that the equipment will be free from defects for a period of two years starting on the date of this Agreement." Yet usage may vary. If there is a time lapse between the date of the Agreement (i.e., when it is signed) and the date of closing (i.e., when both sides of the Agreement are performed), the seller might represent that "the equipment is free of defects as of the date of this Agreement and also as of the date of closing," and warrants that "the equipment will be free from defects for a period of two years following the date of closing."

[215] Examples of affirmative and negative covenant are respectively: "seller promises to keep the equipment in good repair at seller's expense" and "both parties promise not to hire or attempt to hire the employees of the other party."

[216] Although PKI functions will typically be stated as affirmative covenants, covenants may also be negative covenants—promises to refrain from doing a particular action.

accurately. Thus these covenants and representations and warranties effectively give that participant the contractual responsibility not only to identify and authenticate certificate applicants, but also to do it accurately, with the effect that the identification and authentication, is, will be, and has been, accurate. Syntactically, a covenant promises to do (a verb) a function (an object), and a representation or warranty promises how or with what quality (an adverb) the function will be done, or that the function performed has been, is, and will be of a certain quality (an adjective).[217]

As discussed in PAG § C.1 (Sources of Law), *supra*, a participant acquires *liability* as a result or consequence of breaching a responsibility. The contract may also contain contractual limitations upon contractual liability (*liability-limiting provisions* or *provisions for the limitation of liability).* Provisions for the limitation of liability can be either *specific* or *general.* Specific limitations upon liability narrow the scope of certain specified responsibilities by language contained within the responsibilities themselves. General *limitation* of liability provisions fall into one of three categories: *disclaimer*, limitations on the *elements of damages* recoverable, and limitations on the *amounts of damages* recoverable.

Disclaimers are provisions that deny that certain warranties exist, deny liability from certain warranties, or deny all liability for certain other contractual responsibilities. A typical use of a disclaimer is to deny that certain warranties apply to a contractual relationship, in order to avoid or prevent an inference that they exist or that they arise under the agreement by implication or by operation of law. For example, implied warranties of "merchantability" and "fitness for a particular purpose"[218] are commonly disclaimed. Limitations on the *elements of damages* provide that certain categories of damages are not recoverable. For instance, agreements commonly provide that consequential and incidental damages are not recoverable by one or both parties.[219] Finally, limitations on the *amount of damages* (commonly known as liability "caps") provide that if any damages are recoverable, such damages shall be limited to a certain monetary amount, either a stated sum certain, or determined by a formula, such as one referring to the total amount of consideration paid or payable by the aggrieved party under the contract.

As discussed under PAG § C.1 (Sources of Law), *supra*, a participant can be burdened with legal responsibility under *tort* law, and thus be subject to *tort liability*, without ever being party to any agreement accepting such responsibility.[220] In such a case, the participant is free of *contractual liability*, but by the same token, may or may not be able to count on the terms of the contract to limit potential tort liability or reduce the amount of damages payable.[221] If the participant has a contract with the party to whom the party is liable, and is liable

[217] The syntax of covenants, representations and warranties can also be extended to the remedies suitable for the breach of various responsibilities. Some contracts provide that the remedy at law (i.e., an action for monetary damages) is inadequate if a responsibility is breached by a party, and authorize additional equitable remedies (such as a court order for affirmative specific performance of an action promised by a covenant, or a negative injunction prohibiting a particular action) in the event of a breach. Extending an equitable remedy of this type may be appropriate for redressing the breach of a covenant (a promise of a verb and object), but money damages are usually the only remedy available to redress a breach of representation or warranty (a promise of an adverb or adjective).

[218] *See* U.C.C. §§ 2-314 - 2-315.

[219] "Incidental damage resulting from the seller's breach include expenses reasonably incurred in inspection, receipt, transportation and care and custody of goods rightfully rejected, any commercially reasonable charges, expenses or commissions in connection with effecting cover and any other reasonable expense incident to the delay or other breach." U.C.C. § 2-715(1). "Incidental damages to an aggrieved seller include any commercially reasonable charges, expenses or commissions incurred in stopping delivery, in the transportation, care and custody of goods after the buyer's breach, in connection with return or resale of the goods or otherwise resulting from the breach." *Id*., § 2-710. "Consequential damagers resulting from the seller's breach include . . . any loss resulting from general or particular requirements and needs of which the seller at the time of contracting had reason to know and which could not reasonably be prevented by cover or otherwise; and . . . injury to person or property proximately resulting from any breach of warranty." *Id*., § 2-715(2).

[220] *See* PAG § D.2.1.4 (Responsibilities and Liability of Relying Party) for a discussion of how relying parties that are not initially parties to a contract between CA and subscriber, can become so. *See also* PAG § C.1 (Sources of Law).

[221] *But see*, PAG § C.1 (Sources of Law) introducing the concept of third party beneficiary, where a non-party can be indirectly affected by a contract between two other parties. Not being a party, the third party beneficiary cannot have contractual

under a tort theory, the participant may be able to assert a contractual clause limiting tort as well as contractual liability. If, however, the participant is liable to another party under a tort theory and no contract exists between them, the participant would not be able to rely on such a clause to limit the participant's liability.

Rounding out the different types of typical contract clauses, a *condition* is a versatile type of limitation clause that can be applied to either responsibility or liability clauses, to postpone or prevent the effectiveness of the clause until after the occurrence of some other action or state of facts. For example, the responsibility of a party to perform a particular covenant, or to give a particular representation or warranty, can be conditioned upon the prior satisfaction of certain responsibilities of another party, such as: payment of the purchase price; the correctness of representations and warranties given by such other party; or the delivery of an audit report confirming such correctness. Or a condition could be imposed directly upon the liability of a first party resulting from the first party's undisputed breach of a responsibility owed to a second party. For example, the first party's liability may be subject to a condition that the second party's responsibilities to the first have not been breached, or a *de minimis* condition that the first party's breach shall have caused damages at least equal to a stated threshold amount.

The contractual liability of a PKI participant, once determined as the result of a breach of contractual responsibilities, subject to any conditions upon such responsibilities, subject further to any conditions or limitations upon contractual liability, is still further modified by any *indemnity* provisions *transferring* or *shifting liability* to another person. For example, an indemnity clause is commonly used in a situation where the CA has delegated (outsourced) to an RA the CA function of authenticating the identity of certificate applicants. Pursuant to the delegation itself, the RA might have assumed responsibility for the accurate performance of this function by agreeing to a covenant to perform the authentication function, plus representations and warranties to the relying party, that the authentication will be accurate (or the authentication function will be performed accurately). Some sort of liability of CA to the relying party is the typical consequence of the relying party suffering damages from a failure to perform this responsibility adequately.[222] An *indemnity* provision[223] typically accompanies a CA's delegation of responsibility for PKI functions to an RA, to protect the CA from potential claims by the relying party against the CA arising from errors caused by the RA.[224] The CA may be liable to the relying party in the first instance, but may be able to shift the liability to the RA, the party that actually made the error.

No matter how thorough the description of reimbursement of the CA that is provided by the RA's indemnity clause, the RA's indemnity is only worthwhile if the RA is solvent. Accordingly a CA delegating functions to an RA might attempt to cut off theories of liability running from the CA to the relying party to the full extent possible, so as to transfer the risk of RA's breach followed by insolvency, from the CA to the relying party.

---

responsibilities imposed upon him, but nonetheless can acquire benefits from the agreement if the parties to the contract intended non-parties to be covered. If the third party beneficiary acquires benefits under the agreement, those benefits can be expressly limited by the contract.

[222] This can be a direct contractual claim if the relying party is a party to the contract and thus in contractual privity with the RA. If there is no privity between the RA and the relying party, the relying party's claim for the RA's breach of responsibility (and thus liability) might be based upon a number of alternate theories: (i) tort liability: the RA made a negligent misrepresentation upon which relying party reasonably relied to its detriment; (ii) indirect contract liability: the relying party is a third party beneficiary of the contract between the CA and RA; or (iii) hybrid contract/tort liability: some form of estoppel. *See* PAG § C.1 (Sources of Law).

[223] *See infra* note 243.

[224] Depending upon the applicable regime, the terms of the agreement, and whether contractual privity exists, the relying party might argue a variety of theoretically possible grounds for such a claim against the CA, including: (i) direct contractual responsibility and liability of CA to the relying party (or indirectly to the relying party as third party beneficiary), if expressly or implicitly stated in the contract and not subject to any conditions or provisions limiting the CA's liability; (ii) derivative liability of the CA as principal, for the acts of the RA as agent, under the agency principles involving vicarious liability (see PAG § C.2 (Contract and Agency Principles)), including any acts of the RA that create liability under the alternative theories. (*See supra* note 222.)

An attractive alternative for all parties and participants is to manage such risks by transferring them to an insurance company, in exchange for regular payment of an insurance premium that is absorbed as a routine cost of doing business. The emerging PKI insurance industry is discussed in PAG § D.2.2 (Risk Management and Insurance), *infra.*

An assessor seeking to determine the legal responsibilities and potential liability of particular PKI participants should examine all of the following PKI documents that exist: CP, CPS, subscriber agreement, relying party agreement, PDS, with attention given to any agreements that incorporate by reference other documents such as the CP or CPS. A sample checklist for the review of this documentation is set forth below. The checklist is intended as a starting point to focus the attention of the assessor on the general considerations discussed above in this section while reviewing the particular issues relevant to each different PKI participant discussed in PAG §§ D.2.1.1 through D.2.1.5.

Documentation Review - Checklist of Legal Responsibilities and Liability

1) Name or Role of PKI Participant (prepare separate checklist for each participant)
   a) CA – *see*, PAG § D.2.1.1 (CA Responsibilities and Liability),
   b) RA – *see* PAG § D.2.1.2 (RA Responsibilities and Liability),
   c) Subscriber – *see* PAG § D.2.1.3 (Subscriber Responsibilities and Liability),
   d) Relying Party – *see* PAG § D.2.1.4 (Relying Party Responsibilities and Liability), and
   e) Repository – *see* PAG § D.2.1.5 (Repository Responsibilities and Liability).
2) Is this PKI participant a party to an agreement with any other PKI participants? – *see* PAG § C.1 (Sources of Law); if NO; skip to Paragraph 9 in this checklist.
3) Contractual responsibilities assumed by this PKI participant (Representations, Warranties and Covenants):
   a) List Covenants[225] made by this participant, and
      i) Participant(s) benefited by the covenants of this participant
      ii) Any conditions upon effectiveness of particular covenants
   b) List representations and warranties made by this participant,
      i) Participant(s) benefited by the representations and warranties of this participant
      ii) Any conditions upon effectiveness of particular representations or warranties
4) Contractual Liability (resulting from this participant's breach of contractual responsibilities):
   a) List any conditions upon this participant's liability, and
   b) List any limitations upon this participant's liability (disclaimers, limitations on extent, or limitations on amount),

[225] In stating the contractual responsibilities of a party in a typical commercial, corporate, or technology agreement, experienced drafters tend to list representations and warranties ahead of the section of the document that contains covenants, because that is the temporal order of the content of such clauses. On the other hand, in a PKI agreement (oranother PKI document incorporated by reference in a PKI agreement) conceptual clarity may be enhanced by dealing with covenants in the document ahead of representations and warranties. This is true because of the close equivalence between the list of a participant's PKI functions (*see supra* PAG § D.1.3.1 (Certification Authorities) and the list of the participant's covenants (*see supra* PAG § D.2.1 (Apportioning Legal Responsibilities and liability Among the Parties to a PKI Transaction). As an aid to assessors therefore, drafters of PKI agreements (and other documents incorporated by reference in a PKI agreement), might consider positioning covenants as near as possible to the top of the agreement or other document, immediately following preamble material and identification of the parties. The Checklist follows this approach.

5) Any transfers or shifting of contractual liability:
   a) Any contractual indemnities and conditions upon them,
   b) Any applicable insurance -- *see* PAG § D.2.2 (Risk Management and Insurance),
6) Governing Law -- *see* PAG §§ C.1 (Sources of Law) and D.2.4 (Interpretation and Enforcement)
7) Effect of any applicable consumer provisions or other overriding principles -- *see* PAG §§ C.5 (Consumer Issues and Privacy), C.2 (Agency Principles), C.3 (Evidence) and C.4 (Presumptions)
8) If this PKI participant is NOT a party to an agreement with any other PKI participants – *see* PAG § C.1 (Sources of Law):
   a) Governing law -- *see* PAG §§ C.1 (Sources of Law) and D.2.4 (Interpretation and Enforcement),
   b) Effect of any Applicable consumer provisions or other overriding principles -- *see* PAG §§ C.5 (Consumer Issues and Privacy), C.2 (Agency Principles), C.3 (Evidence and Expert Witnesses), and C.4 (Presumptions)
   c) Any benefits of this participant as a third party beneficiary of an agreement between other PKI participants, subject to any conditions or limitations upon such benefits -- *see* PAG § C.1 (Sources of Law),
   d) Responsibilities of this participant under tort law -- *see id*,
   e) Applicable tort standard (negligence, recklessness, strict liability, or intentional tort) -- *see id*, and
   f) Any transfers or shifting of liability by indemnities or insurance – *see* PAG § D.2.2 (Risk Management and Insurance).

Assessors should review the CP, CPS, PKI disclosure statement (PDS), and agreements used within the PKI. They should determine whether all necessary responsibilities are set forth and whether the responsibilities of each of the parties are clearly delineated. Assessors should also determine the scope of any conditions or limitations upon these responsibilities. Note that in some PKIs, there may be no separate RA or repository functions because RA and repository functions may all be performed by a CA

Depending upon the assessment context, and upon the role of the party assessors represents, an assessor may also want to review the representations and warranties to protect the rights of the party benefiting from them. For example, an assessor acting on behalf of a subscriber or relying party community may wish to determine whether the representations and warranties provided by a CA or RA are sufficient to protect the subscribers or relying parties in their use of certificates. In contrast, assessors may wish to determine that the responsibilities stated in the documents are not unnecessarily expanded. For instance, an assessor acting on behalf of a CA may wish to determine whether the responsibilities of the CA set forth in its subscriber and relying party agreement provide reasonable protection for subscribers and relying parties without exposing the CA to excessive liability.

An analysis of *liability-limitation provisions* is similar, and mirrors the analysis of responsibilities. While assessors acting on behalf of subscriber and relying party communities will want to determine whether warranties are expansive enough, they will also determine whether liability limitation provisions are narrow enough in scope to permit subscribers and relying parties to have meaningful and robust remedies. Similarly, assessors acting on behalf of CAs or RAs may want to ensure that liability limitation provisions are robust enough to protect the interests of the CAs or RAs.

Appropriate Requirements and Practices. The distribution of responsibilities among the various PKI components and participants will ultimately determine the manner in which liability for loss or damage is apportioned among them. Higher-assurance PKIs will likely seek to legally bind all PKI participants by some sort of agreement that applies requirements set forth in a CP or CPS to these participants. CAs and RAs have an interest in committing themselves to reasonable responsibilities (representations, warranties, and covenants)

to ensure the trustworthiness (and thus marketability) of their services. At the same time, they have an interest in avoiding exposure to excessive liability by including specific limitations upon the scope of these responsibilities as well as all three types of general liability-limitation provisions (disclaimer, limitations on the elements of damages recoverable, and limitations on the amounts of damages recoverable).

Subscribers and relying parties tend to have interests that are adverse to each other (*see supra* PAG §§ C.3 (Evidence and Expert Witnesses), C.4 (Presumptions) and C.5 (Consumer Issues and Privacy), and *infra* §§ D.2.1.3 (Subscriber Responsibilities and Liability) and D.2.1.4 (Relying Party Responsibilities and Liability)). On the other hand, with respect to certain issues, these parties may be allied in a common position adverse to the CA and RA. The common interests of subscribers and relying parties might appear to be advanced by seeking contractual terms providing the broadest possible responsibilities for CAs and RAs, and the narrowest liability-limitation provisions, at the cheapest possible fee. On the other hand, the enlightened self-interest of a subscriber and relying party community might well lie in a more moderate position on all issues, to ensure that CAs and RAs remain willing to provide their services.

D.2.1.1 CA Responsibilities and Liability

Issue Summary. This section focuses on the particular situation of the CA as a participant in a PKI, following the same pattern of analysis used in the more general PAG § D.2.1 (Apportioning Legal Responsibilities and Potential Liability Among the Parties to a PKI Transaction). The PAG's use of "CA Responsibilities" in this section D.2.1.1 is equivalent to RFC 2527's use of "CA Obligations." This section addresses in turn: CA responsibilities expressed by CA covenants; CA responsibilities expressed by CA representations and warranties; and finally CA liability and limitations upon liability. Elements of CA functionality commonly expressed in CA covenants are listed, some of which could be performed either by the CA, or by a separate RA or CMA to whom the CA outsources elements of CA functionality.

D.2.1.1.1 CA responsibilities expressed primarily in CA covenants

Issue Summary. This section deals mainly with CA responsibilities that are expressed primarily in CA *covenants*, the type of contract clause which the assessor will normally find best suited to describing the CA functions that the CA promises to perform. Different drafting approaches to the organization and expression of CA responsibilities (expressed by covenants as well as representations and warranties) are identified and discussed. The drafting approach illustrated by the PAG is one that includes within PAG § D.2.1.1 miscellaneous responsibilities not included in other sections, plus cross references to the many more specific CA responsibilities that are likely to be found under other sections of the PKI documents. This section also expresses a drafting preference for listing both CA and RA functions as CA responsibilities (expressed by covenant) even though RA functions may upon occasion be delegated by the CA to a separate RA.

Relevant Considerations. Assessors should carefully review the responsibilities of the CA stated in the PKI's practice documents and agreements. CA responsibilities, however, may or may not appear within a single section of the document, and may also arise by implication or by operation of law from sources outside the four corners of the document.[226] If a CA is bound to meet these requirements, these requirements become *responsibilities* in a legal sense, but it may be duplicative to repeat them all in a "CA Responsibilities" section that corresponds to the RFC's "CA Obligations" section. Therefore, Assessors may find that a particular CP or CPS under review uses the "CA Obligations" section simply to refer to those responsibilities that may arise by

[226] *See supra* PAG §§ C.1 (Sources of Law) and D.2.1 (Apportioning Legal Responsibilities and Liability Among the Parties to a PKI Transaction) (discussion of tort law). *See also* Michael. S. Baum, Federal Certification Authority Liability and Policy, NIST-GCR-94-654, June 1994, *available at* <http://www.verisign.com/repository/pubs/index.html>.

implication or operation of law, as well as to provide cross-references to other, more specific CA responsibilities in other sections, rather than attempting to provide an exhaustive list of CA responsibilities.[227]

Accordingly, assessors will likely see that practice documents treat the "CA Obligations" section (hereinafter referred to as the "CA Responsibilities" section) in one of five ways:

1) "CA responsibilities" simply refers to other, more specific CA responsibilities in other sections of the PAG. In this case, assessors should focus on CA responsibilities when they review these other sections.

2) PAG § D.2.1.1.1 on CA responsibilities attempts a comprehensive listing of CA responsibilities. In this case, assessors should look to the RFC and this document to ensure that all necessary topics are covered in light of the business model of the PKI. Assessors should also determine whether the document as a whole places responsibilities of the proper scope on CAs.

3) PAG § D.2.1.1.1 on CA responsibilities contains a summary and brief listing of, or series of cross-references to, CA responsibilities set forth in the rest of the document. This approach is a blend of the first two. The authors may be attempting some compromise between the first two approaches. In this case, assessors should determine whether the summary or brief listing is consistent with the CA responsibilities in the rest of the document. They should also determine, in light of the applicable business model, whether the combination of the summary or brief list and CA responsibilities in the rest of the document covers all necessary topics in light of the particular business model involved, and whether the document as a whole contains CA responsibilities of the proper scope.

4) PAG § D.2.1.1.1 on CA responsibilities does not attempt to cover all CA responsibilities, but does set out some general responsibilities and leaves the remaining CA responsibilities for the remainder of the document. The authors may recognize that some CA responsibilities do not fit neatly within one of the RFC 2527 sections and therefore fit best within the general CA responsibilities section. Here, assessors should again check to see if the document as a whole covers the necessary topics and if the responsibilities are of the proper scope in light of the business model.

5) Some combination of the above approaches.

Assessors should determine which approach is implemented within the PKI's documentation and whether the documentation successfully carries out that approach.

Appropriate Requirements and Practices. As discussed above under Relevant Considerations above, the draftsman might take one of five common approaches to laying out CA responsibilities in PAG § D.2.1.1.1. In most circumstances, approach (2) is impractical and redundant, since most of the entire PAG or RFC 2527 framework contains CA responsibilities. A comprehensive statement of such responsibilities within this section would almost require repeating the rest of the document within one section. Approach (1) is a legitimate one, and has brevity as a virtue. It may, however, omit certain miscellaneous responsibilities that do not fit unambiguously and well within other portions of the PAG or RFC 2527 framework. Approach (3) may be a nice compromise between the first and second, but assessors may find that the effort to summarize all CA

[227] RFC 2527 has a specific section for "CA Obligations," yet the entire RFC 2527 Framework itself furnishes an extensive list of items a CA should do. These items could be characterized as business, technical or legal "obligations" ("responsibilities" in the rubric of the PAG). For example, implementing validation procedures, meeting certificate lifecycle operational requirements, applying technical and non-technical security and management controls, issuing certificates and CRLs with a certain format, and administering practice documents in accordance with applicable policies, can all be viewed as CA obligations (responsibilities). *See* RFC 2527, *supra* note 193, §§ 3-8; *see also* PAG §§ D.3 – D.8. They may well likely comprise most of the remainder of the CP or CPS that follows. (*Id.*, § 2; *see* PAG § D.2 (General, Legal and Business Provisions).

responsibilities is either futile or misleading, and not worth the effort. Approach (4) is also legitimate, but without a reference to other CA responsibilities elsewhere, may mistakenly leave readers with the impression that the list of miscellaneous responsibilities in PAG § D.2.1.1.1 is exclusive. For that reason, a combination of approach (4) (a brief list of miscellaneous responsibilities), coupled with approach (1) (a reference to CA responsibilities elsewhere in the documentation), may prove to be the most effective choice.

The following is a list of some common CA responsibilities (covenant type) that assessors may well encounter in this section if the PKI's practice documentation takes approach (4) above. The PKI documents may find these CA responsibilities appropriate to mention because they do not fit well in other RFC sections:

- A general covenant for the CA to use trustworthy systems. While a general trustworthiness requirement is applicable in the context of more specific sections of a practice document, the PKI may wish to place a generally-applicable trustworthiness requirement in this section to avoid the need for repeating the requirement elsewhere.

- A general covenant for the CA to perform its services in accordance with applicable law. For example, the PKI may need to satisfy certain licensure laws, or meet the requirements of laws governing the export or import of cryptographic hardware or software.

- A general covenant of the CA to meet the requirements of a specific standard (if any apply).

A combined approach, (4) and (1), would then complete section 2.1.1.1 with brief summaries and cross-references to all other sections of the PKI documents that contain covenants corresponding to the applicable CA functions (out of a potential universe of nine CA functions) listed under PAG § D.1.3 (Community and Applicability).

Under RFC 2527, drafters of CPs, CPSs and related agreements could reasonably organize provisions relating to CAs and RAs in one of two different methods: by functionality (i.e., CA functions in section D.2.1.1 and RA functions in section D.2.1.2), or by entity (i.e., the CA's responsibilities in section 2.1.1 and the RA's responsibilities in section 2.1.2), or some variation. Although either approach might be reasonable for drafting CPs and CPSs, the latter (entity) approach has been chosen for the PAG as a method similar to the way a careful lawyer would approach the issue. The intent is to focus the drafter's attention upon the full checklist of responsibilities that could impose liability upon the CA entity to the extent such responsibilities are not delegated or outsourced to a separate RA entity, much the same way that a careful lawyer would analyze the responsibilities of a CA entity that is a client. Those responsibilities of the CA described in section 2.1.1 of the practice documents that are delegated to an RA would then be repeated in summary fashion in section 2.1.2. (RA Responsibilities and Liability).

D.2.1.1.2 CA Responsibilities Expressed Primarily in Representations and Warranties.

Issue Summary. This section focuses upon CA responsibilities express primarily in representations and warranties. In a PKI issuing certificates providing relatively low levels of assurances, there may be only a modest set of representations and warranties or none at all. In a PKI issuing certificates offering higher levels of assurances, more rigorous CA representations and warranties are more likely to be required by subscribers and relying parties, and are also likely to be preferred by a CA that provides the PKI as a main business, in order to increase the comfort level of its customers. The use of insurance-backed CA warranties is discussed, and a list of CA representations and warranties typical in a higher assurance setting is provided.

Relevant Considerations. Depending on the context of the assessments, assessors may want to check the documents to make sure that CA responsibilities expressed in representations and warranties provide enough assurances to protect the party benefiting from them, and further that the representations and warranties are commensurate with the applicable assurance level.[228] On one hand, an assessor acting on behalf of a subscriber

[228] *See* PAG APP 1, § 1.1 (Glossary), definition of "assurance level".

or relying party community may wish to determine whether the representations and warranties provided by a CA are sufficient to protect the subscribers or relying parties in their use of certificates. On the other hand, assessors acting on behalf of a CA may wish to determine whether CA representations and warranties are greater in scope than necessary for the CA's business purposes. Such an assessor may be charged with ensuring that the representations and warranties provided by the CA in its subscriber and relying party agreement provide reasonable protection for subscribers and relying parties, while at the same time are not so broad that the CA is open to excessive liability, given the assurance level.

More generally, assessors should be aware of any external requirements in a CP or applicable law requiring certain CA representations or warranties to be in the CPS. If there are such requirements, assessors should determine whether they appear in the PKI's documentation.

Appropriate Requirements and Practices. The scope of CA representations and warranties will vary considerably depending on the context. In the context of PKIs offering lower assurance certificates, CAs may well utilize agreements containing simple covenants without any representations or warranties at all, particularly if rudimentary applicant validation procedures make it difficult for the CA to be sure of accurate binding between the public key and the subject of the certificate. Similarly, if the PKI is secondary to the CA's main business, the purpose of the certificates may be limited, making expansive representations and warranties unnecessary.

In the context of PKIs offering higher assurance certificates, however, subscribers and relying parties may require a more demanding set of representations and warranties. Moreover, CAs may wish to offer a greater set of representations and warranties to users of the PKI. In particular, if the CA provides the PKI as its main service, it will want to encourage people to feel comfortable in using that service, to enhance the CA's competitive advantage. Having robust representations and warranties is one method of providing that comfort.

CAs may also wish to provide additional benefits by beginning a warranty program backed by insurance. Such a warranty program could provide defined assurances concerning the use of certificates by subscribers and relying parties and permit them to file warranty claims to obtain compensation for their losses covered by the program. Subscribers and relying parties would feel comfort in using certificates because of the warranties, and also in knowing that their protection does not depend on the solvency of the CA, in light of the insurance coverage backing the warranties.[229]

In any case, some of the common representations and warranties that may be helpful for CAs to provide in the context of higher assurance certificates include:

- A warranty that the information confirmed by the CA and placed within certificates that it issues is accurate,
- A warranty that the certificates issued by the CA do not contain errors or inaccuracies caused by the CA,
- A warranty that the CA has conformed to its own CPS in issuing certificates, and
- A representation that a CA meets certain CA standards or requirements imposed on the PKI by law or contract.

CAs should also meet any requirements placed on them by law or contract to make or not make representations and warranties in their documentation.

[229] *See supra* PAG § D.2.1 (Apportioning Legal Responsibilities and Liability Among the Parties to a PKI Transaction) and *infra*, PAG § D.2.3 (Financial Responsibilities).

D.2.1.1.3 CA Liability and Limitations upon CA Liability

Issue Summary. This section addresses the maximum or minimum disclaimers of warranty or responsibility applicable to CAs, CA limitations on the elements of damages, and limitations on the amount of damages that a CA must pay.

Relevant Considerations. The assessor's understanding of the extent of the CA's liability depends upon an analysis of the CA's responsibilities (representations, warranties and covenants) and any liability limitation provisions. While assessors acting on behalf of subscriber and relying party communities will have an interest in ensuring that the CA responsibilities are expansive enough, they also will have an interest in limiting the scope of disclaimers and liability limiting provisions to permit subscribers and relying parties to have meaningful and robust remedies. Similarly, assessors acting on behalf of CAs or RAs may seek liability limitation provisions that are robust enough to reasonably protect the interests of the CAs or RAs, yet do not emasculate those remedies.

Assessors should check to determine if any CA liability provisions are either required or prohibited by the governing law of the applicable jurisdiction. For example, some PKIs may require subordinate CA entities to include in their agreements disclaimers or liability limitations that run in favor of a superior CA entity higher in a PKI hierarchy. If so, assessors should determine whether the requisite provisions appear in the documentation. Nevertheless, applicable law may limit or prohibit the ability of a CA to disclaim warranties or limit the type or amount liability. Assessors should be aware of these limitations and determine whether the CA disclaimers or limitations exceed these limits.

At a minimum, most U.S. and other jurisdictions require that liability disclaimers and material limitations upon liability be adequately disclosed. There may be additional requirements, such as a requirement that the disclaimer be *conspicuous*, through techniques such as a distinctive font or all capital letters.[230] Moreover, there are limits upon the enforceability of unreasonable disclaimers of warranties or liability limitations in certain jurisdictions. For example, a limitation that causes an exclusive or limited remedy to "fail of its essential purpose" may be ineffective to the extent the UCC or UCITA is applicable to the transaction.[231] In the French civil law context, an organization's liability policy must be disclosed to its competitors under an anti-monopolist statute. Also, in the civil law context, limitations of liability are generally less effective against consumer parties to a contract, or against the party to an "adhesion" contract who has the lesser bargaining power.[232] *See supra* PAG § C.5.3.2 (EU E-Signatures Directive and EU Privacy Directive), regarding stringent privacy rules that may not be disclaimed under the EU Data Privacy Directive.

In the United States, UCITA was promulgated by the National Conference of Commissioners on Uniform State Laws in July of 1999[233] and as of this writing has been adopted by only a few States.[234] UCITA prohibits variance in certain terms of a "mass-market" license, and will not enforce choice of law clauses in a consumer contract that would change rules that could not be varied in the absence of those clauses.[235] U.S. courts

[230] *Cf.*, UCC § 2-316(2)(20xx)("[L]anguage to exclude the implied warranty of merchantability . . . must mention merchantability and in case of a writing must be conspicuous, and to exclude or modify any implied warranty of fitness the exclusion must be by a writing and conspicuous.")

[231] *See* UCITA, *supra* note 110, § 804(b)(applicable to transactions in computer information), *see also supra* note 229.

[232] *See* Quebec Civil Code, art. 179.

[233] *See* UCITA, *supra* note 110; *see also* Annual Meeting Draft (2000) <http://www.law.upenn.edu/bll/ulc/ulc.htm#ucita>.

[234] *See* PAG APP 2 (*Uniform Computer Information Transactions Act*, VA. CODE ANN. §§ 59.501.1 (Michie 2001), *available at* <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+TOC59010000043000000000000>, hereinafter "Virginia UCITA") and (*Uniform Computer Information Transactions Act*, MD. CODE ANN., Commercial Law § 21 (implemented Oct. 1, 2000), *available at* <http://mlis.state.md.us/cgi-win/web_statutes.exe?gcl&22-101>, hereinafter "Maryland UCITA").

[235] *See* UCITA, *supra* note 110, §§ 113(a)(3), 109(a).

sometimes do not enforce disclaimers. Legislation may require disclaimers to be stated in clear and/or conspicuous manner, or communicated by way of a particular medium.[236]

Appropriate Requirements and Practices. Just as the scope of representations and warranties will vary depending on the kind of PKI involved, the type of disclaimers and limitations will also vary. In the context of a PKI offering lower assurance certificates, CAs may wish to disclaim all warranties and place strict limits on the types of damages for which they may be liable. Certain disclaimers, not otherwise enforceable in a consumer context, may nonetheless be appropriate for low-value transactions or where the CA is issuing free or nominal-cost certificates. In very rudimentary PKIs, with little by way of formal documentation, though, the CA may feel that the risk is constrained enough to make long agreements full of disclaimers and limitations unnecessary.

In higher assurance settings, a CA may find it desirable to make certain express warranties and disclaim all other express or implied warranties or conditions, perhaps with a limitation on aggregate monetary liability and exclusions of categories of damages (such as incidental and consequential damages (such as loss of profits), as well as punitive damages). Often, implied warranties, such as warranties of merchantability and fitness for a particular purpose, are disclaimed. In the context of a PKI offering higher assurance certificates, larger amounts are at stake, making litigation a cost-effective possibility. CAs will likely be concerned with preventing the possibility of unconstrained liability, due to implied warranties, and unlimited judgments arising from incidental and consequential damages.

Regardless of the environment, CA disclaimers and liability limitations should not exceed the limits imposed by applicable law. In addition, CAs should include in their documentation any disclaimers or limitations required by contract. It would also be helpful for this section to account for any laws that impose immunities on CAs, such as sovereign immunity.

D.2.1.2 Responsibilities and Liability of a Registration Authority

Issue Summary. This section addresses the scope of the responsibilities (representations, warranties and covenants) and liability of a Registration Authority (RA) or other ancillary service provider to whom "front-end" CA functions have been delegated, as stated in the relevant agreements and other documents. This section lists what a RA does or should promise to do, although the description is often at a high level. Some CA functions already described in detail in section D.2.1.1 are also RA functions, in which case the description in this section is typically limited to a concise summary and a cross reference to the corresponding portion of section. This section also addresses the representations and warranties made by RAs. Finally, the section addresses the maximum or minimum disclaimers of warranty or responsibility, limitations on the elements of damages, and limitations on the amount of damages that a RA imposes or must impose on other participants in the PKI.

D.2.1.2.1 RA responsibilities expressed primarily in RA covenants

Issue Summary. This section discusses responsibilities expressed primarily in RA covenants, and further discusses different approaches to listing RA functions when there is or is not a separate RA.

Relevant Considerations. As mentioned in PAG § D.1.3.2 (Registration Authorities), the CA itself may perform RA functions, or the CA can delegate or "outsource" them to one or more persons or entities that have agreed to accept and perform such functions by covenanting to perform them. These functions are primarily the establishment of enrollment procedures and mechanisms, confirmation (or disconfirmation) of the identity of the certificate applicant and information in the certificate application, approval or denial of the certificate application, initiating revocation on the RA's own initiative or at the subscriber's request, and approving or

[236] *See* UCC § 3-316(2); *cf.*, *see* E-SIGN Act, *supra* note 73, § 101(c)(1)(B), *see also* PAG §§ D.1.3.1 and D.1.2.1 (different ways to present CA and RA Covenants).

denying requests for certificate renewals or rekeying. If the CA retains front-end RA functions because there is no separate RA, the discussion of RAs in this section might be handled merely by a cross reference to the five RA functions listed by section D.1.3.2. together with a statement that there is no separate RA. If there is a separate RA, those RA functions delegated to the RA should be set forth as RA covenants.[237]

Where the CA delegates or outsources front-end functions to an RA, the RA serves as the intermediary between a CA and certificate applicants (some of whom become subscribers) through the performance of specific "front-end"[238] CA functions assigned to it by the CA. Any assessment of a CA and/or RA should involve an examination of all relevant service contracts between CAs and all service providers such as RAs to whom critical CA functions are delegated. The assessment should determine what functions have been delegated.

There is often an "RA agreement" entered into between the CA and the RA, in which the CA and RA will allocate responsibilities among themselves consistent with the applicable CP, CPS, and other applicable policies of the CA. The RA agreement will often contain an indemnity provision stating that any breach by the RA in the performance of those duties will entitle the CA to seek indemnification from the RA for any loss or damages suffered by the CA by reason of claim by a third party or otherwise. The RA Agreement may also specify whether or not the RA is considered to be the agent of the CA for certain purposes.[239] If the RA is designated in a limited sense as an agent of the CA then the RA may execute the End Entity Agreement on behalf of the CA. In some cases there may also exist a separate agreement between the Subscriber and the RA which agreement will contain the terms and conditions governing the relationship between the RA and the subscriber. This is presented diagrammatically in Figure D-1 as follows:

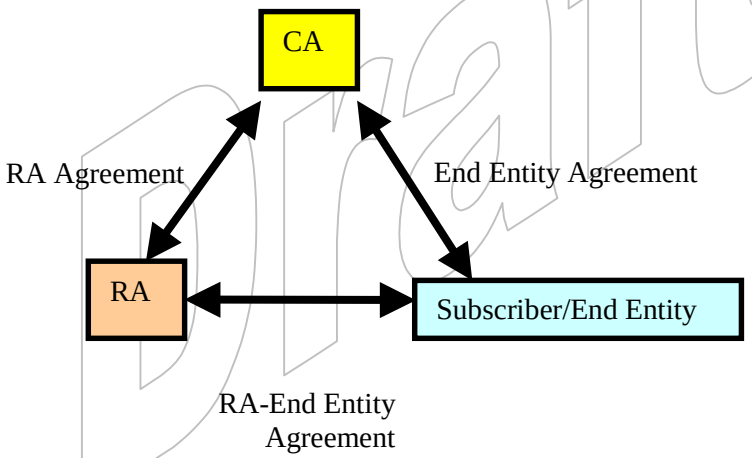


Figure D-1.

Following a consideration of the relationship between the CA and the RA, assessors should review RA responsibilities created by covenants in the PKI's practice documents and agreements. As with CA responsibilities, RFC 2527 has a specific section for "RA responsibilities," even though RA responsibilities appear throughout documents conforming to RFC 2527. Therefore, assessors may find that a PKI's practice documentation takes one of the approaches listed in section D.2.1.1: (1) simply referring to other sections for more specific RA responsibilities, (2) comprehensively listing all RA responsibilities, (3) summarizing or

[233] *See* PAG § D.1.3.1 and D.1.3.2. (different ways to present CA and RA Covenants).

[238] Delegation or outsourcing of front-end CA functions to an RA is to be distinguished from the outsourcing of "back end" CA functions such as the maintenance of system hardware and software for certificate management, the provision of system security for certificate signing keys, or the maintenance of a repository. The outsourcing of such back-end CA functions is a practical method for a business entity to serve in the role of a CA without the need to replicate or re-invent sophisticated PKI technology. The CA will outsource the nuts and bolts of CA back end functions by becoming a licensee of the necessary technology. In effect, the CA is "virtually" issuing certificates with its own name or any agreed name as the Object of the certificate -- the so-called "private branding" or "co-branding" of certificates.

[239] *See supra* PAG §§ C.2 (Agency Principles) and note 243, *infra*.

briefly listing RA responsibilities, (4) listing only general or miscellaneous responsibilities, or (5) a combination of the above. Assessors should determine which approach is used, and whether the PKI documentation succeeds in implementing that approach.

Appropriate Requirements and Practices. Among the five common approaches for setting forth RA responsibilities, (1) referring to more specific responsibilities in other sections, (2) a comprehensive listing, (3) a brief summary or list of cross-references, (4) listing only general or miscellaneous responsibilities, or (5) a combination of the above, that analysis of appropriate requirements and practices is likely to be the same as CA responsibilities. The second approach is likely to be impractical and redundant, and the third approach may not be practical either (or at least not worth the effort). The first and fourth approaches are more practical, and a combination of the two may be the most effective approach.

As with CA responsibilities, a number of miscellaneous responsibilities expressed as covenants may be appropriate for section D.2.1.2:

- A general covenant for the RA to use trustworthy systems. A trustworthiness obligation can appear in more specific sections elsewhere, but some PKIs may, for the sake of brevity, want to include the covenant just once in this section.
- A general covenant requiring the RA to perform its services in accordance with applicable law. For example, the PKI may need to satisfy privacy laws in connection with the gathering and maintenance of enrollment information.
- A general obligation of the RA to meet the requirements of a specific standard (if any apply).

D.2.1.2.2. RA responsibilities expressed primarily in RA representations and warranties

Issue Summary. This section discusses RA responsibilities, expressed primarily in RA representations and warranties. Assessment of these responsibilities is similar to an analysis of CA representations and warranties, except that the CA and the RA are likely to have different views as to the scope of the RA representations and warranties.

Relevant Considerations. An assessor's analysis of RA representations and warranties will be similar to an analysis of CA representations and warranties in PAG § D.2.1.1. Subscriber and relying party communities may have an interest in expanding the scope of RA representations and warranties, while the party making them, here the RA, may have an incentive to limit their scope. The difference here, however, is that the CA may also have an interest in requiring expansive RA warranties in order to place ultimate responsibility for RA errors on the RA.[240] In addition, as with CA representations and warranties, assessors should determine whether any requirements on the CA by law or contract within a PKI require that the RA make certain representations and warranties. If so, assessors should determine if such representations and warranties appear in the RA's documentation.

Appropriate Requirements and Practices. As with CA representations and warranties in PAG § D.2.1.1 (CA Responsibilities and Liabilities), the scope of RA representations and warranties will depend on the circumstances. In the context of a PKI offering lower assurance certificates,[241] the PKI may want both CAs and

[240] It is possible for a CA to delegate front-end responsibility to an RA while still maintaining legal responsibility for RA functions as against other parties such as the subscriber and relying party, with the RA ultimately responsible for RA functions by indemnification of the CA under the RA Agreement. In such case, the other parties may not even be aware of the delegation of duties to the RA. If a reputable CA is financially responsible and stands behind all actions of the RA as a principal responding for the actions of its agent, perhaps there is less need for assessors to separately assess the trustworthiness of the RA, although most likely the CA should disclose the RA delegation to the assessors so they can make such independent investigation of the RA as they deem appropriate. *See supra* PAG § D.2 (General, Legal and Business Provisions).

[241] *See* PAG § D.2.1 (Apportioning Legal Responsibilities and Potential Liability Among the Parties to a PKI Transaction).

RAs to avoid making representations or warranties, especially where the PKI is not the major focus of the RA's business. By contrast, in the context of a PKI offering higher assurance certificates, especially where the CA and RA are, in combination, offering the service as their main activity, the PKI may wish to require robust warranties. RAs may also benefit from participating in the kind of warranty program discussed in section D.2.1.1, where the RA's warranties are backed by insurance.

Some common representations and warranties that may be helpful for RAs to provide in higher assurance settings include:

- A warranty that the information confirmed by the RA and provided to the CA for inclusion in the certificate is accurate;
- A warranty that the RA did not cause any errors or inaccuracies in the information provided to the CA for inclusion in the certificate;
- A warranty that the RA has conformed to the applicable CPS in performing its services; and
- A representation that the RA meets certain RA standards or requirements imposed on the PKI by law or contract.

RAs should also meet the requirements placed on them by law or contract to make representations and warranties in their documentation.

D.2.1.2.3 RA Liability and Limitations Upon RA Liability

Issue Summary. This section addresses the maximum or minimum disclaimers of warranty or responsibility applicable to RAs, RA limitations on the elements of damages, and limitations on the amount of damages that a RA must pay.

Relevant Considerations. An assessor's analysis of RA liability and limitations upon liability will resemble that of the CA. Assessors acting on behalf of subscriber or relying party communities have an interest in limiting the scope of disclaimers and liability limitations, while the party providing the services, the RA, has an interest in having robust disclaimers and liability limitations. Similarly, assessors should determine whether certain disclaimers or liability limitations are either required by the PKI or, on the other hand, whether they exceed limitations placed on exculpatory clauses by applicable law.

Appropriate Requirements and Practices. Just as the scope of CA liability will depend on the contact, as noted in PAG § D.2.1.1 (, the scope of RA liability will also depend on the nature of the PKI involved. In lower assurance environments, RAs may wish, if they use comprehensive PKI documentation, to disclaim all warranties and severely limit their liability. Such limits are more likely appropriate where the certificates are free or low-cost, and the PKI is secondary to the RA's main business. In rudimentary PKIs, the RA may feel that the risk of the service is low enough so that long agreements or documents, including those containing disclaimers and liability limitations, are unnecessary.

By contrast, in the context of a PKI offering higher assurance certificates, RAs may want to provide express warranties, but disclaim all other warranties, whether express or implied. Commonly, such provisions disclaim implied warranties of merchantability and fitness for a particular purpose. In this environment, RAs may also wish to limit the elements of damages recoverable, to exclude incidental, consequential, and punitive damages, and limit the amount of damages recoverable to a certain monetary amount.

Assessors should also ensure that these provisions do not exceed the limitations imposed by applicable law on the ability of parties to disclaim warranties and limit liability. On the other hand, if the PKI imposes contractual responsibilities on RAs to include certain liability terms, assessors should ensure that such provisions are

actually contained in the RA's documentation. Finally, any pertinent laws that impose immunities on RAs, such as sovereign immunity, might also be cited.

D.2.1.2.4 Indemnities given by the RA

Issue Summary. This section discusses indemnities commonly given by the RA to the CA to indemnify the CA against damages suffered from third party claims arising from the RA's failure to perform its RA responsibilities as required, such as the authentication of the identity of a certificate applicant.

Relevant Considerations. An indemnity clause is commonly used in a situation where the CA has delegated (outsourced) to an RA the CA function of authenticating the identity of certificate applicants. Pursuant to the delegation itself, the RA might have assumed responsibility for the accurate performance of this function by agreeing to a covenant to perform the authentication function, plus representations and warranties to the relying party, that the authentication will be accurate (or the authentication function will be performed accurately). Some sort of liability of RA to the relying party is the typical consequence of the relying party suffering damages from the RA's failure to perform this responsibility adequately.[242] An indemnity provision[243] typically accompanies a CA's delegation of responsibility for PKI functions to an RA, to protect the CA from potential claims by the relying party against the CA.

Appropriate Requirements and Practices. No matter how thorough the description of reimbursement of the CA that is provided by the RA's indemnity clause, the RA's indemnity is only worthwhile if the RA is solvent. Accordingly a CA delegating functions to an RA might attempt to cut off theories of liability running from CA to relying party to the full extent possible, so as to transfer the risk of RA's breach followed by insolvency, from the CA to the relying party. An attractive alternative for all parties and participants is to manage such risks by transferring them to an insurance company, in exchange for regular payment of an insurance premium that is absorbed as a routine cost of doing business. The emerging PKI insurance industry is discussed in PAG § D.2.2 (Risk Management and Insurance).

D.2.1.3 Subscriber Responsibilities and Liability

Issue Summary. This section addresses the responsibilities of subscribers[244] expressed in their covenants, representations and warranties, the liability resulting from a breach of their responsibilities, and limitation of liability provisions applicable to them. This section also discusses indemnities that subscribers are required to provide as a remedy for redressing damages caused by their intentional misconduct (e.g., misrepresentations in

[242] This can be a direct contractual claim if the relying party is a party to the contract and thus in contractual privity with the RA. If there is no privity between the RA and the relying party, the relying party's claim for the RA's breach of responsibility (and thus liability) might be based upon a number of alternate theories: (i) tort liability: the RA made a negligent misrepresentation upon which relying party reasonably relied to its detriment; or (ii) indirect contract liability: the relying party is a third party beneficiary of the contract between the CA and RA. *See supra* PAG § C.1 (Sources of Law).

[243] A typical indemnity clause in such a situation might read as follows: "The RA covenants and agrees to indemnify and hold harmless the CA from any and all loss or damage (including reasonable attorneys' fees) suffered by reason of third party claims (whether or not successful) against the CA arising from any actions or omissions of the RA in connection with the RA's performance, nonperformance or inadequate performance of any of RA's covenants hereunder or in connection with RA's breach of any representations or warranties hereunder, upon condition that the CA shall promptly notify RA of any such claims, shall cooperate reasonably with the RA in the defense of such claims, and shall allow the RA to have reasonable control over the settlement of such claims."

[244] Note that for purposes of obligations and liability, a reference to a "subscriber" means the person who applied for and was issued a certificate, and does not necessarily refer to the person named in the certificate (the subject of the certificate). In the event of fraud or certificates not purporting to provide assurances of identity, the certificate application may have used someone else's name on the certificate applicant and it is that other person's name that appears in the certificate. Subscriber obligations and liability in this case apply to the actual certificate applicant and key pair holder, not the person named in the certificate (the subject) who had nothing to do with the certificate application.

certificate applications), or negligence (e.g., in failing to take reasonable measures to protect their private keys from compromise).

D.2.1.3.1 Subscriber responsibilities expressed primarily in Subscriber covenants

Issue Summary. This section discusses subscriber responsibilities expressed primarily in subscriber covenants. Depending upon the relationship between the CA and subscribers, and the applicable assurance level of the PKI, subscriber covenants may be expressly set forth in detailed agreements, or may be set forth more informally.

Relevant Considerations. Unless imposed by applicable law, the responsibilities, representations and liability of the subscriber to other parties will likely be set forth in any express agreements between such parties. Assessors should review subscriber covenants within a PKI's CP, CPS, PKI disclosure statement, and subscriber agreement.[245] Subscriber responsibilities might not be imposed or evidenced by a formal agreement. In a corporate setting where a CA is part of the organization, certificates may be issued to a subscriber who is an employee with the terms and conditions of use set out in an "employee use" policy, the breach of which becomes an employment law or an agency law issue. The assessor should be alert to the possibility that there are other such documents governing subscriber responsibilities that require review.

The section of a CP or CPS containing subscriber covenants may refer to other sections of the document for more detailed responsibilities, attempt a comprehensive listing of subscriber responsibilities, seek to summarize or briefly list subscriber responsibilities, list some generalized or miscellaneous responsibilities, and place specific responsibilities elsewhere, or utilize a combination of these approaches. Assessors should determine which approach the PKI's documentation takes and whether the documentation properly implements that approach.

Appropriate Requirements and Practices. Again, subscriber responsibilities appear scattered throughout the RFC 2527 framework, and a PKI's documentation may (1) refer to other sections containing more specific subscriber responsibilities, (2) comprehensively list all subscriber responsibilities, (3) summarize or briefly list via cross-references to subscriber responsibilities, (4) list some general or miscellaneous responsibilities, or (5) a combination of the foregoing. In contrast with CA or RA responsibilities, there are fewer subscriber responsibilities within the RFC 2527 framework. Accordingly, it is much more feasible to take the second or third approach when writing a CP or CPS. In fact, a comprehensive listing of subscriber responsibilities would aid in the subsequent drafting of a subscriber agreement. As with CA and RA responsibilities, the first and fourth approaches are also valid. CP and CPS drafters, therefore, have somewhat more flexibility in drafting sections on subscriber responsibilities.

The following is a list of some common subscriber responsibilities normally expressed as covenants. Whether these responsibilities or others should appear within PKI documentation will depend on the circumstances. For example, in rudimentary PKIs, the risks relating to the PKI may be limited enough such that a simple list of user instructions may be sufficient. In the context of PKIs offering higher assurance certificates, however, setting forth responsibilities is usually important, and the following provisions are considered the core responsibilities of a subscriber:

[245] Normally the Subscriber is in contractual privity with the CA by reason of a Subscriber Agreement entered into between the Subscriber and the CA at the time of applying for issuance of a Certificate or subsequently accepting an issued Certificate. If (as is usually the case) the Relying Party is not a party to the Subscriber Agreement between the Subscriber and the CA, then obligations owed by the subscriber to the relying party can be expressed indirectly as obligations owed to the CA, with the relying party considered to be the "third party beneficiary" of the subscriber's obligations. It is a good idea to provide a clause in the subscriber agreement that expressly states whether or not the relying party is entitled to rely, as a third party beneficiary, upon promises made to other parties. A third party beneficiary is a "person who, though not a party to a contract, stands to benefit from the contract's performance. For example, if Ann and Bob agree to a contract under which Bob will render some performance to Chris, then Chris is a third-party beneficiary." BLACK'S LAW DICTIONARY 149 (7th ed. 1999). Other potential theories for a Relying Party to obtain the benefit of the Subscriber's obligations include tort and contract doctrines such as estoppel. *See supra* PAG § C.1 (Sources of Law).

- A covenant to provide accurate certificate application information. Subscribers should provide complete, accurate and truthful information in their certificate applications.

- A covenant to generate the subscriber's private key securely and safeguard it. PKI documentation will likely set requirements for the hardware or software subscribers must use to generate and safeguard their private keys.[246] As stated in the DSG, " . . . the subscriber shall not compromise the private key corresponding to a public key listed in such certificate."[247]

- A covenant to use certificates appropriately. PKI documentation will likely contain provisions stating the proper uses of certificates, whether usage is restricted to certain environments or applications, and whether some uses are prohibited. *See* PAG § D.1.3.4 (Applicability). Commonly, PKI documentation requires subscribers to use their certificates consistent with these provisions.

- A covenant of subscriber to request revocation of a certificate when appropriate. When a subscriber discovers that the subscriber's private key has been compromised, the subscriber has a responsibility to promptly notify the CA that issued the certificate, or the RA that approved the certificate application, and request revocation of the certificate. The purpose is to mitigate or avoid the potential damages resulting from use of the compromised private key. In addition, subscribers may be required to request revocation where information in the certificate is inaccurate or no longer accurate. For example, a subscriber agreement may provide that a subscriber should inspect his or her newly-issued certificate to make sure the information in it is correct and, if not, notify the CA or RA in order to obtain a replacement with the correct information. Also, a subscriber may be required to request revocation where the subscriber's name changes, the subscriber's affiliation with the CA or RA ends, or other changes occur.

- A covenant to assent to the terms of the applicable subscriber agreement. A CP, CPS, or PKI disclosure statement may include an obligation by the subscriber to indicate assent during enrollment to the terms of the applicable subscriber agreement. The documentation may, at a minimum, condition the CA's or RA's service responsibilities upon such assent.

- A covenant to use only key pairs bound to valid certificates. A key pair should not be used unless it is bound to a valid certificate. Under DSG § 1.36, a "valid certificate" is "a certificate which (a) a certification authority has issued, and which (b) the subscriber listed in it has accepted." A certificate is not valid until it has been both issued and accepted, and accordingly it, and the key pair to which it is bound, should not be used before the subscriber has accepted it. Such a requirement is intended to prevent the following scenario: a certificate applicant generates a key pair and enrolls for a certificate; the CA issues the certificate and makes it available to the subscriber for pickup; in the meantime, the subscriber has used the private key to enter into a transaction; the subscriber obtains the benefit of the transaction, but tries to repudiate it based on the fact that the certificate is not valid because the subscriber has not yet accepted it.

- A covenant to cease use of the private key after revocation or expiration of the certificate. PKI documentation may require subscribers to stop using their private keys if the certificate containing the public key corresponding to that private key becomes inoperable through expiration or

[246] A subscriber who wishes to delegate authority to sign should not share a single private signing key, but should instead arrange for separate key-pairs to be generated by, and certificates to be issued to, each authorized person (the special case of a shared role), *see supra* PAG § D.1.3.3 (End-Entities), with such person's distinguished name to be listed as subject of a separate certificate. On the other hand, there are situations (e.g., shared role and escrow of decryption key by a responsible organization such as an employer) where practical necessity may require the sharing of a private decryption key used to decrypt encrypted messages. *See infra* PAG § D.6.2.3 (Private Key escrow) (where the same concepts are discussed in a technical context).

[247] *See* DSG, *supra* note 2, § 4.3.

revocation. Key pairs have defined usage periods (*see* PAG § D.6.3.2 (Usage periods for the public and private keys). PKIs set the usage period with a view to the fact that after a certain point in time and after a certain level of expected usage, private keys become vulnerable to cryptanalytic attacks. PKIs may set the operational period of the certificate equal to that of the key pair in order to require a rekey and new certificate at the end of such usage period (*see* PAG § D.4.7 (Processing a request for a new key pair)). The obligation to cease use of the private key after revocation or expiration of the certificate containing the corresponding public key prevents the use of a certificate and the key pair beyond its operational period.

D.2.1.3.2 Subscriber Responsibilities Expressed Primarily in Subscriber Representations and Warranties

Issue Summary. This section discusses subscriber responsibilities expressed primarily in subscriber representations and warranties. The extent of subscriber representations and warranties will be determined by the applicable assurance level of the PKI.

Relevant Considerations. The assessment of subscriber representations and warranties will mirror the image of the analysis of CA representations and warranties. On one hand, assessors acting on behalf of a subscriber community are likely to have an interest in limiting subscriber representations and warranties to a reasonable scope that do not expose subscribers to excessive liability. On the other hand, assessors acting on behalf of a CA will likely want to ensure that subscriber representations and warranties are broad enough to protect the CA. Assessors should also determine if there are any requirements or restrictions imposed by contract or applicable law regarding the representations and warranties made by subscribers and whether these requirements or restrictions are properly implemented.

Appropriate Requirements and Practices. As with CA and RA representations and warranties, the scope of requirements placed on subscribers will vary depending on the PKI. In the context of PKIs offering lower assurance certificates, where subscriber agreements may be minimal if not non-existent, risks may be sufficiently manageable to permit omission of subscriber representations and warranties. By contrast, where a PKI offers higher assurance certificates, PKI documentation is likely to contain at least some subscriber representations and warranties. Common representations and warranties include:

- A representation that the information submitted by the subscriber on the subscriber's certificate application was accurate, and a warranty that such information will continue to be accurate during the operational period of the certificate, unless the subscriber notifies the CA or RA that information in the certificate has changed.

- A representation that the subscriber's private key has not been shared or otherwise compromised, and a warranty that during the operational of the period of the certificate the subscriber will have exclusive control over the private key, unless the subscriber notifies the CA or the RA as to a compromise.

- In the case of certificates used only for a certain application or set of uses, a warranty that the subscriber's use of its private key is only for that application or set of uses.

D.2.1.3.3 Subscriber Liability, Limitations Upon Liability, and Indemnities

Issue Summary. This section discusses subscriber liability, limitations upon subscriber liability, and Indemnities given by subscribers. Two examples of potential subscriber liability that may result in the indemnification of other participants, are liability arising from breach of the certificate applicant's representations regarding the subscriber's identity, and liability arising from breach of a subscriber covenant to safeguard the private key from compromise.

Relevant Considerations. With respect to subscriber liability, it is unlikely that CA or RA documentation includes subscriber disclaimers and liability limitations since subscribers are receiving rather than providing PKI services. CA and RA documentation may, however, place indemnity responsibilities on subscribers, for

example to make CAs and RAs (and perhaps relying parties, directly or indirectly as third party beneficiaries) whole for losses arising out of subscriber misrepresentations on their certificate applications[248] or negligence from breach of subscriber covenants to protect their private keys from compromise. At least one jurisdiction outside the U.S. has specified by law that by accepting a certificate, a subscriber undertakes to indemnify the issuing CA for any loss or damage caused by the issuance or publication of the certificate in reliance upon a false and material representation of fact by the subscriber or the failure by the subscriber to disclose a material fact.[249] Assessors acting on behalf of subscribers, however, might want to ensure that sufficient conditions upon such indemnity[250] are in place to ensure that subscribers are not open to excessive liability.

Assessors should determine if any subscriber liability provisions are either required or prohibited by applicable law or contract. For example, a CP may require that certain subscriber liability terms appear in CPSs of CAs issuing certificates that comply with the CP. If requirements or limitations apply, assessors should determine whether the documentation satisfies the requirements or stays within applicable limits.

Appropriate Requirements and Practices. Again, the scope of subscriber liability provisions in a PKI's documentation will vary depending on the nature of the PKI. In the context of a PKI for lower assurance certificates, the CA may find it unnecessary to use much documentation at all and therefore may omit any liability terms applicable to subscribers. In PKIs providing higher assurance certificates, however, liability terms are more common. Assessors acting on behalf of a CA will want to ensure that sufficient representations and warranties and indemnification of the CA for damages caused by their breach, are in place to protect the CA. CAs and RAs may be concerned about claims against them that actually arise out of subscriber or relying party error or even fraud, and representations or warranties may help CAs and RAs defend such claims. Similarly, an assessor acting on behalf of a subscriber community will likely want to limit the scope of subscriber warranties to ensure that they are not excessive.

Finally, subscriber liability provisions should meet any requirements or stay within any limitations imposed by contract or applicable law. For example, if a CP requires that subscribers indemnify CAs and RAs for their misrepresentations, assessors should make sure such a provision appears in the CPS and subscriber agreement. It may also be necessary for this section to account for any immunity applicable to subscribers, such as sovereign immunity in the case of organizational or individual government subscribers.

[248] This would include the case of a misrepresentation by the certificate applicant as to the identity or name of the certificate applicant, but in this case an action seeking indemnity for damages caused by breach of that identity misrepresentation would need to be brought against the imposter (if identified and subject to service of process) rather than against the subscriber falsely named in the certificate. *Cf., See* UETA, *supra* note 15, § 9(a)("An electronic record or electronic signature is attributable to a person if it was the act of the person. . . ."

[249] *See* Malaysia's Signature Act, *supra* note 55, (provides that by accepting a certificate, a subscriber undertakes to indemnify the issuing CA for any loss or damage caused by issuance or publication of the certificate in reliance on "(a) a false and material representation of fact by the subscriber; or (b) the failure by the subscriber to disclose a material fact, if the representation or failure to disclose was made either with intent to deceive the licensed certification authority or a person relying on the certificate, or with negligence." The Law further provides that this indemnity may not be disclaimed or contractually limited in scope. As discussed in note 248, *supra*, such an indemnity running from the subscriber to the CA would appear inappropriate in the case of a subscriber whose identity was spoofed by an imposter certificate with no involvement by an innocent subscriber.

[250] For example, conditions upon such indemnity might range from reasonable notice from the CA to the subscriber and the CA's reasonable cooperation with the subscriber in the defense and settlement of any third party claims against CA, to proof by the CA that the subscriber's act or omission was a proximate cause of a mistaken issuance of the certificate to an imposter. *But see* DSG, *supra* note 2, § 3.14, (liability of complying certification authority), which purports to exculpate a CA from liability to a blameless subscriber if the CA "complies with these Guidelines and any applicable law or contract."

D.2.1.4 Relying Party Responsibilities and Liability

Issue Summary. This section discusses the issue of contractual privity as it affects responsibilities of the relying party expressed as covenants or imposed by law, the representations and warranties of the relying party, and liability provisions, and liability limitation provisions. This section also covers indemnities that the relying party is required to make.

D.2.1.4.1 The Effect of Contractual Privity Upon Relying Party's Responsibilities Expressed as Covenants or Imposed by Law

Issue Summary. This section discusses the issue of whether the relying party is in privity of contract with the other PKI participants. The resolution of this issue affects whether the relying party's responsibilities are primarily expressed as contractual covenants, or imposed by law as, for example, responsibilities under tort law. This section then discusses the nature of the responsibilities accepted by the relying party under contract covenants, or imposed upon the relying party under tort law or other applicable laws.

Relevant Considerations. At the threshold is the question of whether the PKI attempts to create contractual privity between the CA and the relying party. If the first contact between a relying party and the CA is the relying party's receipt of a digitally signed message verifiable by reference to a certificate issued by the CA, there is an apparent gap between CA and relying party, raising the question of whether or how privity can exist between the CA and the relying party.

There are a number of techniques and arguments to bridge this gap. First, under current law governing "clickwrap" acceptance of website contracts,[251] a website can be configured so that the relying party is deemed to accept the terms of a relying party agreement, to which the relying party knowingly assents when (for example) the relying party accesses the CA's website to access and check the status of a certificate in the repository. Second, in many PKIs, the relying parties are also subscribers, for example when members of a subscriber base use certificates to send secure e-mail back and forth to each other. When relying parties are also subscribers, privity with the CA exists because these subscribers will already have agreed to a subscriber Agreement. Third, the certificate itself may incorporate by reference terms and conditions in it, which by operation of that incorporation, are binding on relying parties.[252] Finally, a CA may offer a warranty program or third party and first party liability insurance products to relying parties, which they may wish to utilize. If they accept the benefits of such programs, privity will necessarily exist. *See supra* PAG § D.2.1.1 (CA Responsibilities Expressed Primarily in Representations and Warranties) and *infra* PAG § D.2.2 (Risk Management and Insurance).

The purpose of the privity analysis is to determine the means by which relying party responsibilities, (representations, warranties and covenants) and liability, liability-limiting, and indemnity provisions, can become contractually binding on relying parties through the normal PKI documentation. If no privity exists between the relying party and the CA or RA, then CA or RA requirements are not normally[253] enforced via a contract. In these cases, the only responsibilities placed on relying parties would arise through applicable law. Applicable law, for example, may make terms in a CA's CPS binding on relying parties even without an agreement between the CA and the relying party.[254] Alternatively, relying parties may have relying party functions (such as the responsibilities discussed below) imposed on them by tort law, because their failure to take reasonable steps to perform these functions may act as a defense by the CA or RA to a tort claim. For

[251] *See supra* note 117; *cf.* UCITA, *supra* note 110, § 210-213. *See also* PAG § C.4.5 (Effect of E-SIGN on Digital Signature Presumptions), *supra*.

[252] See generally PAG APP 2 (Incorporation by Reference and Public Key Infrastructures: Moving Beyond the Paper-Based World, Wu, S., 38 JURIMETRICS 317 (1998), hereinafter "Wu").

[253] *But see supra* PAG § D.2.1 (Apportioning Legal Responsibilities) and C.1 (Sources of Law), (discussion of third party beneficiary).

[254] *See* DSG, *supra* note 2, §§ 5.1 - 5.6.

example, the relying party's failure to check the status of a certificate may be deemed unreasonable, preventing the relying party from establishing "justifiable reliance"[255] on the CA's assertions in the certificate as an element of a claim for intentional or negligent misrepresentation. Such a failure may also act as the relying party's own contributory or comparative negligence, which the CA can assert as a defense against an action for negligence or negligent misrepresentation against the CA.[256] Accordingly, a tort analysis may involve a comparison of the actions of the parties to determine their reasonableness.[257]

If privity does exist between the CA and the relying party, thereby causing responsibilities in the PKI's documentation to be directly binding on the parties (including on the relying party), assessors should examine the documentation to determine the scope of these responsibilities. The relying party covenant section of a CP or CPS may contain a simple reference to other portions of the document for more detailed responsibilities, set forth a comprehensive listing of relying party responsibilities, summarize or briefly list relying party responsibilities, list only those generalized or miscellaneous responsibilities that don't appear in specific responsibilities elsewhere, or make use of a combination of these approaches. Assessors should determine which approach the PKI's documentation takes and whether the documentation is successful in implementing that approach.

As with subscriber responsibilities, relying party responsibilities need not be evidenced by a formal relying party agreement. For example, in a PKI used for internal corporate e-mail, relying parties may be subscribers whose use of certificates may be governed by an "employee use" policy to be interpreted in light of applicable employment or agency law. In addition, in some PKIs the CA and the relying party are one and the same. If so, a relying party Agreement between the CA and the relying party would not be necessary. Assessors should be alert to the possibility of such informal agreements or policies, and review any that are located and are applicable.

Appropriate Requirements and Practices. As with the covenants made by other PKI participants, it is necessary for the PKI to decide how to present relying party covenants; unlike other participants, however, relying party covenants tend to be small enough in number to make it feasible to list in this section, or perhaps cross reference.[258] The appropriate extent of relying party responsibilities will depend on the circumstances of

[255] *See supra* PAG § D.2.1 (Apportioning Legal Responsibilities) and C.1 (Sources of Law); *see also* DSG, *supra* note 2, § 5.4.

[256] *See* Wu, *supra* note 252, at 328.

[257] Where recovery of damages is sought to compensate a loss alleged to have been caused by reliance on a certificate following a private key compromise, some of the factors to be considered by the trier of fact may include the following:

To what extent did subscriber safeguard the private key under DSG § 4.3?

To what extent did subscriber promptly request revocation of Certificate after discovering the compromise?

Did the relying party refresh certificate status information to catch the revocation if the subscriber had requested it promptly?

To what extent was any lack of care of the parties immaterial to the loss of either?

To what extent should the relying party have considered the digital signature unreliable under DSG § 5.3?

To what extent was relying party's reliance reasonable under DSG § 5.4?

To what extent did subscriber and relying party exercise potential capabilities for mitigating the damage caused to the other?

Which party had a better opportunity to avoid the loss, in a case such as a compromise of the subscriber's private key?

Possible standards for a dispute resolution to apply in this weighing process include a baseline of practices dictated by technology standards and the intended community of interest and intended uses as defined in the PKI's documentation.

[258] Relying party "obligations" appear in several places within the RFC 2527 framework, and a PKI's documentation may (1) refer to these other sections with specific relying party responsibilities, (2) restate all relying party responsibilities in full, (3) summarize or briefly list cross-references to relying party responsibilities, (4) list some general or miscellaneous responsibilities, or (5) a combination of the foregoing. Relying party responsibilities are limited enough in number so that a comprehensive list of them under the second or third approach would be feasible. In fact, having at least a reference to all relying party responsibilities in one section of a CP or CPS would aid in the later drafting of a relying party agreement. It is

the PKI. For instance, rudimentary PKIs may not feel the need to have any relying party documentation at all if the application creates little risk and the amounts at stake are low or nonexistent. PKIs issuing higher assurance certificates will, however, likely require responsibilities to be placed on relying parties. The following provisions are considered the core relying party responsibilities:

- A covenant to perform cryptographic operations properly. PKI documentation commonly requires a relying party to perform the intended cryptographic operations successfully using software and hardware appropriate to the applicable assurance level as a condition of relying on a certificate DSG § 5.6(2) requires the digital signature to be "verified by reference to the public key listed in a valid certificate" before the rebuttable presumption arises that the digital signature is the digital signature of the subscriber listed in that certificate.[259] If the relying party uses a system incapable of verifying the digital signature, or the relying party's system of hardware and software indicates that the signature is invalid, the relying party should not rely on the signature.

- A covenant to rely on certificate for intended purposes only. Before relying on a certificate, a relying party may be required to make sure that the certificate is appropriate for the relying party's intended application. If so, the relying party should consult the applicable CP or CPS to determine the applications for which the certificate is intended and any limitations on usage. *See* PAG § D.1.3.4 (Applicability). For example, if a certificate is issued pursuant to a certificate policy (reflected in the certificate policies extension[260] in the certificate) that states the certificate may not be relied upon for transactions where the purported subscriber is other than the employer of the relying party, any attempted reliance upon the certificate for transactions with other entities would be unreasonable.[261] An appropriate result in such a case would be to shift to the relying party, the risk of any damage caused to the subscriber or the CA resulting from such reliance.

- A covenant to check certificate status. PKI documentation may require a relying party to check the status of a certificate prior to relying on it. Some certificate-enabled software used by relying parties (e.g., SSL – "Secure Sockets Layer") will automatically check whether a certificate has been issued by a trusted CA and whether the certificate has expired according to its own terms. In addition, however, relying parties may be required to make sure that all certificates on which they rely have not been revoked. Relying parties, under such a requirement, may be required to consult the most recent certificate revocation list (CRL) or query an online database of information, for example through the Online Certificate Status Protocol (OCSP).

- A covenant assenting to the terms of the applicable relying party agreement. A CP, CPS, or PKI disclosure statement may require, as a condition to relying on a certificate, the assent of the relying

---

also feasible to have a simple reference to other sections where relying party responsibilities appear under the first approach, or list some miscellaneous responsibilities in this section and leave other responsibilities for other sections. *See* RFC 2527, *supra* note 193.

[259] *See* DSG, *supra* note 2, § 1.37. Specifically, the definition of "verify a digital signature and message integrity" under DSG is:

Verify a digital signature and message integrity

In relation to a given digital signature, message and public key, to determine accurately:

(1) that the digital signature was created during the operational period of a valid certificate by the private key corresponding to the public key listed in the certificate; and

(2) the message has not been altered since its digital signature was created.

[260] A relying party may be able to accept certificates governed by a specific CP and, if the relying party is satisfied that all such certificates issued under that CP meet the relying party's requirements, the relying party may want to program its software to accept certificates containing the object identifier corresponding to the CP in its certificate policies extension.

[261] *See* DSG, *supra* note 2, § 5.4.

party to the applicable relying party agreement. The documentation may, at a minimum, condition the CA's or RA's responsibilities to provide services, such as certificate status information, on such assent.[262]

D.2.1.4.2 Relying Party's Representations and Warranties

Issue Summary. This section discusses the Representations and Warranties of the Relying Party.

Relevant Considerations. The assessment of relying party representations and warranties will be the similar to that of subscribers' representations and warranties. An assessor acting on behalf of a relying party community has an incentive to limit relying party representations and warranties to a reasonable scope so that relying parties are not exposed to excessive liability. Assessors acting on behalf of a CA, however, may want robust representations and warranties to protect the CA. Assessors should also account for any requirements or restrictions imposed by contract or applicable law relating to relying party representations and warranties and should determine whether these requirements or restrictions are followed.

Appropriate Requirements and Practices. The nature of any relying party warranties will depend on the type of PKI involved. The CA or RA documentation itself (i.e., the CP or CPS) might not include representations and warranties, since the major purpose of a certificate is to assert the binding of a public key to identity and/or other attributes. Those assertions are being made by the CA and not by the relying party. CAs and RAs, however, may require relying parties to warrant that they are using certificates for the purposes permitted by the PKI documentation--a warranty that is most appropriate when certificate use is intended only within a closed community.

D.2.1.4.3 Relying Party's Liability, Limitations upon Liability, and Indemnities

Issue Summary. This section discusses any provisions of liability, limitations upon liability, and indemnities affecting the relying party.

Relevant Considerations. Assessors should check whether any relying party liability provisions are either required or prohibited by applicable law or contract. A CP, for instance, may mandate that certain provisions appear in CPSs or relying party Agreements. If there are applicable requirements or limitations, assessors should see whether the PKI's documentation contains provisions meeting the requirements or that are within applicable limits.

As with subscriber liability terms, it is unlikely that CA or RA documentation will include relying party disclaimers and liability limitations since relying parties are receiving rather than providing PKI services.[263] Indeed, CA and RA documentation may place indemnity responsibilities on relying parties, for example to make CAs and RAs whole for losses arising out of a relying party's misuse of a certificate. Assessors acting on behalf of relying parties, however, will want to determine whether sufficient protections are implemented so that relying parties are not vulnerable to excessive liability.

Appropriate Requirements and Practices. The scope of liability provisions applicable to relying parties will depend on their context. PKIs providing lower assurance certificates may contain no liability provisions at all, if the CA believes that the lack of such provisions does not pose excessive risks. Such liability provisions, however, may be appropriate for PKIs providing higher assurance certificates. For example, if the relying party community is the driving force behind the PKI and is obtaining certificates from vendors that meets its needs, it may be able to impose disclaimers and liability limitations on the CA. In addition, if the CA is the only possible relying party in the PKI, the CA will likely manage liability in its dual role as CA and relying party. In these

[262] Whether such an obligation is binding or not will depend on whether the CA is able to create a contractual relationship with relying parties, as discussed above.

[263] CAs also functioning as relying parties will likely have liability terms. *See supra* PAG § D.2.1.1 (CA Responsibilities and Liability).

cases, assessors acting on behalf of the relying parties may want to ensure that enough protections are in place to manage relying party liability, while other parties may want to limit the scope of any relying party disclaimers or liability limitations.

Finally, relying party liability provisions should meet the requirements or conform to the limitations created by contract or applicable law. A CP, for example, may require that certain terms appear in CPSs and relying party Agreements. Likewise, applicable law may limit the scope of disclaimers and liability limitations made by relying parties, and the PKI documentation should be consistent with such limitations. It may also be necessary for this section to account for any immunity applicable to relying parties, such as sovereign immunity in the case of governmental relying parties.

D.2.1.5 Repository Responsibilities and Liability

Issue Summary. This section discusses the scope of responsibilities (covenants, representations and warranties), and liability of repositories or other ancillary service providers to whom "back-end" CA functions involved with publication of certification information may have been delegated, as provided in the relevant agreements and other documents. This section lists, often at a high level, what repository service providers do or must promise to do. Representations and warranties either made by or required of repository service providers also appear in this section. Finally, the section discusses liability limitations that a repository imposes or should impose on other participants in the PKI.

D.2.1.5.1 – Responsibilities of the Repository Expressed Principally by Covenants

Issue Summary. This section discusses responsibilities of the repository that are expressed principally by covenants.

Relevant Considerations. A repository is in somewhat the same position as the RA is under section D.2.1.2, (Responsibilities and Liability of a Registration Authority) *supra*. The maintenance of a repository for certificates, CPs, CPSs, and the like is a CA function that can be done by the CA itself, or it can be outsourced in whole or in part to a separate entity.[264] *See* PAG § D.1.3.1 (Certification authorities). While the RA function is a "front-end" CA function, the repository function is more of a "back-end" CA function. A CA's delegation of back-end functions to a repository, however, is somewhat less common than a CA's delegation of front-end functions to an RA. These functions are primarily the publication of certificates (making them available for use by relying parties), practice and policy documents (e.g., CPs, CPSs, PKI disclosure statements, and agreements), and certificate status information (e.g., certificate revocation lists, OCSP responses, and information available via HTTP (hypertext transfer protocol) and lightweight directory access protocol (LDAP) queries). If the CA retains back-end repository functions, there may be no discussion of a separate repository service provider at all.

Where there is a separate repository in the PKI, and the CA delegates or outsources these functions to it, the repository serves as a provider of specific publication-related "back-end" CA functions assigned to it by the CA. Any assessment of a CA and/or repository must include a review of all relevant service contracts between CAs and all service providers such as repositories to whom critical CA functions are delegated. The assessment should determine what functions have been delegated by the agreement between the CA and repository.[265] To

[264] *See* CARAT Guidelines, *supra* note 200. The CARAT Guidelines suggest an implementation model in which the repository function is given a status which appears to be equal to that of the CA, with its primary focus on serving the Relying Party's interests rather than those of the Subscriber.

[265] Following a review of the contractual relationship between the CA and the repository, assessors should review repository responsibilities in the PKI's practice documents and agreements. As with CA and RA responsibilities, RFC 2527 has a specific section for "Repository Responsibilities," even though repository responsibilities appear in several other sections in documents conforming to RFC 2527. Accordingly, assessors may find that a PKI's practice documentation takes one of the approaches listed in PAG § D.2.1.1 (CA Responsibilities and Liability): (1) merely referring to these other sections for more specific repository responsibilities, (2) listing all repository responsibilities in full, (3) summarizing or briefly listing repository responsibilities, (4) listing only general or miscellaneous responsibilities, or (5) a combination of the above. Assessors should

the extent that there is access to identifiable nonpublic private information in the repository, and the repository is not synonymous with the CA, the CA should contractually bind the repository to (i) abide by the CA privacy practices, and (ii) maintain the confidentiality of the information and (iii) provide appropriate security and access controls to protect the private information. These requirements may not always be taken into account in implementing and planning general security and access controls, as they may impact the availability of information to employees of the repository as well.

Appropriate Requirements and Practices. If the CA performs repository functions and there are no separate repositories, the only provision in this section that may be necessary is a statement to that effect and a cross-reference to the repository functions performed by the CA. Where there is a separate repository service provider, however, the general statement of repository responsibilities in this section, as with the other PKI participants, may fall into one of five patterns: (1) merely a reference to responsibilities in other sections, (2) a full listing of all repository responsibilities, (3) a brief summary or listing of cross-references to repository responsibilities, (4) listing only general or miscellaneous responsibilities, or (5) a combination of the above. It is repetitive and may be impractical to take the second approach, since there are several sections devoted to repository functions elsewhere in the RFC 2527 framework. But it may be practical to have a summary of repository responsibilities or a list of functions with a cross-reference, in accordance with the third approach. The first and fourth approaches are also practical. Also, as with CA and RA responsibilities, some useful general or miscellaneous responsibilities to place in this section include: a general covenant for the RA to use trustworthy systems, a general covenant to perform its services in accordance with applicable law, and a general covenant to meet any applicable standards.

If the PKI documentation, however, attempts a more comprehensive listing of covenants, it is likely to list some or all of the following core functions, depending on the allocation of responsibilities between the CA and the repository:

- A covenant to accurately publish information. A repository's publication functions may include:
    - Publishing and archiving certificates;
    - Publishing and archiving the PKI's certificate policies, the CA's certification practice statement, the CA's PKI disclosure statement, and the CA's agreements, such as subscriber and relying party agreements; and
    - Publishing the status of certificates through certificate revocation lists, OCSP servers, and information available via http and lightweight directory access protocol queries.

In contrast to the RA function, which can be and is usually performed on a decentralized, geographically distributed basis, a repository can be managed on a centralized basis.

- A covenant as to availability. A repository will be available to the CA, subscribers, and relying parties during the period of availability specified in the PKI's documentation.
- Covenants relating to the promptness or frequency of publication. A repository may be under an obligation to publish its information within certain time limits and publish CRLs with a certain frequency. *See* PAG §§ D.2.6 (Publications and Repositories) and D.4.9.7.1.1 (Notification of Certificate Revocation to Others).
- A covenant to secure the repository and control access to it. The PKI documentation may place an obligation on repositories to provide security for their systems and control access to the

determine which approach the PKI documentation takes, and whether the documentation succeeds in implementing that approach.

information they publish to prevent unauthorized access and tampering.[266] *See infra* PAG §§ D.2.6 (Publications and Repositories) and D.2.8.3 (Privacy).

D.2.1.5.2 Responsibilities of the Repository Expressed Principally by Representations and Warranties

Issue Summary. This section discusses responsibilities of the repository expressed principally in Representations and Warranties.

Relevant Considerations. An assessor's analysis of repository representations and warranties will be similar to the analysis of RA representations and warranties. Subscriber and relying party communities have an interest in expanding the scope of assurances provided by repositories in their representations and warranties, while the repository itself may have an interest in limiting them to a reasonable scope. The CA's practice documentation may also reflect the CA's interest in obtaining a reasonable scope of assurances from the repository. Assessors should determine whether any requirements on the repository by law or contract require that repository make certain representations and warranties. If so, assessors should determine if the repository portions of the documentation include the required representations and warranties.

Appropriate Requirements and Practices. The scope of repository representations and warranties will depend on the circumstances. Where repository functions are performed by the CA itself or in the context of PKIs providing lower assurance certificates, there may be no repository representations or warranties. By contrast, in the context of PKIs issuing higher assurance certificates, the PKI may wish to require robust warranties.

Some representations and warranties that may be helpful for repositories to provide in higher assurance settings include:

- A warranty that the repository has not caused any errors or inaccuracies in the information it holds in the repository,
- A warranty that the repository has conformed to the applicable CPS in performing its services, and
- A representation that the repository meets certain standards or requirements imposed on the PKI by law or contract.

Repositories should also meet any requirements imposed upon them by law or contract to make representations and warranties in their documentation.

D.2.1.5.3 Repository Liability, Liability Limiting Provisions, and Indemnities

Issue Summary. This section concerns provisions of liability, limitations upon liability, and indemnities affecting repository service providers.

Relevant Considerations. As with an assessor's analysis of RA liability, an assessor acting on behalf of subscriber or relying party communities have an interest in limiting the scope of any repository disclaimers and liability limitations, while the party providing the services, the repository, has an interest in having robust disclaimers and liability limitations. Similarly, assessors should determine whether certain disclaimers or liability limitations are either required by the PKI or, on the other hand, whether they exceed limitations placed on exculpatory clauses by applicable law.

[266] For example, to the extent a repository contains personally identifiable information of individuals whose confidentiality is critical (e.g., personal healthcare information under the Health Care Privacy and Portability Act (HIPAA) and U.S.-EU Safe Harbor Principles dated July 27, 2000), the repository will also have an obligation to maintain the security of the repository against invasion from hackers. This may be viewed as a responsibility that is no greater than the general requirement of trustworthiness for the security services expected of PKI systems in general.

Appropriate Requirements and Practices. The scope of repository liability will depend on the nature of the PKI involved. In the context of PKIs providing lower assurance certificates, there may be no separate repository or little if any documentation relating to a separate repository function. The risks may be manageable enough so that long agreements or documents, including those containing disclaimers and liability limitations, are unnecessary. Where risks are greater, but assurances are still low, the repository may wish to disclaim all responsibility and warranties, and strictly limit liability.

In the context of PKIs providing higher assurance certificates, however, repositories may want to provide express warranties, but disclaim all other warranties, whether express or implied. Commonly, such provisions disclaim implied warranties of merchantability and fitness for a particular purpose. In this environment, repositories may also wish to limit the elements of damages recoverable, to exclude incidental, consequential, and punitive damages, and limit the amount of damages recoverable to a certain monetary amount. These disclaimers and liability limitations may be combined with similar provisions by the CA.

Assessors should also ensure that these provisions do not exceed the restraints imposed by applicable law on the ability of parties to disclaim warranties and limit liability. On the other hand, if the PKI imposes contractual responsibilities on repositories to include certain liability terms, assessors should ensure that such provisions are, in fact, set forth in the repository's documentation. A PKI may also find it helpful to account for any immunity applicable to the repository, such as sovereign immunity.

D.2.2 RISK MANAGEMENT AND INSURANCE[267]

Issue Summary. This section presents any requirements or disclosures relating to insurance coverage or risk management measures that a PKI undertakes or must undertake.

Relevant Considerations. PAG § C.6 (Risk Management and Insurance Principles), *supra*, discusses the general principles underlying risk management and insurance as they relate to PKI. PKIs have at their disposal various mechanisms for risk avoidance, risk assumption, risk control, and risk transfer. Risk managers, including those affiliated with insurance carriers, may establish loss prevention programs. They may educate PKI participants about steps they can take to identify risks and implement procedures for risk avoidance and risk control purposes.

One risk management mechanism at the disposal of a policy making authority or PKI is the requirement of obtaining and posting a bond as a condition of beginning operations. Currently, some state law regimes for licensing CAs include a requirement that a CA wishing to obtain a license obtain a bond in an amount deemed appropriate to provide a reasonable level of financial responsibility to respond to claims lodged against the CA.[268]

Moreover, errors and omissions ("E&O") insurance is increasingly available to provide protection against losses incurred in connection with PKI activities. E&O insurance can provide *third party coverage* for PKI participants who incur liability to others. In addition, the market for insurance services will likely mature over time, to permit parties to obtain *first party* protection for their own losses caused by the conduct of others. In addition, future insurance offerings may include insurance where, on a transaction-by-transaction basis, a subscriber or relying party can obtain protection against losses incurred in a particular transaction or series of transactions. Such a program would be akin to postal or shipping insurance that can be obtained in connection with the shipping of a package to protect against accidental loss or destruction.

[267] *See* RFC 2527, *supra* note 193, § 2.2, (deals with the subject matter of "Liability"). The PAG combines the subject matter of both sections 2.1 and 2.2 of RFC 2527 in PAG § D.2.1 (Apportioning Legal Responsibilities and Liability Among the Parties to a PKI Transaction).

[268] *See* PAG § D.2.3 (Financial Responsibility), *infra*.

An assessment of a PKI should include an analysis of whether policy makers within the PKI have established appropriate insurance and risk management requirements in light of the PKI's business needs. Assessors should be aware of externally-imposed requirements to carry E&O or other insurance, or to abide by the requirements of a risk management program. Assessors should determine whether or not the appropriate requirements or disclosures appear in the PKI's documentation. Finally, assessors should determine whether PKI participants have actually received the insurance coverage they are required to obtain and whether they have undertaken the risk management steps that are required by the PKI's documentation.

Appropriate Requirements and Practices. The need for a minimum insurance requirement and the need for a PKI to require its participants to undertake formal risk management programs will depend on the applications for which the certificates are used and the assurance levels provided by the certificates. PKIs offering low assurance certificates for low-value transactions typically have no such requirements since the risks of loss and liability are relatively low. By contrast, where high-assurance certificates are used for high-value transactions, it is common for PKIs to require CAs and RAs to carry a certain minimum level of E&O insurance. The amount of needed protection will again depend on the circumstances of the PKI.

Formal risk management programs are less common. Nonetheless, as the insurance industry's efforts to provide coverage to PKI participants mature, it is likely that insurance carriers will establish such programs to educate their customers on risk avoidance and risk control techniques. Informal risk management efforts will assist PKI participants in identifying risks and implementing internal controls to manage those risks.

In general, entities establishing a PKI will want to set requirements for minimum E&O insurance amounts and risk management programs that are appropriate in light of the business needs of the PKI and the assurances provided by its certificates. PKI participants should abide by any requirements placed on them to obtain such levels of insurance and to manage their risks. The PKI's documentation should clearly articulate its insurance and risk management requirements and practices, and PKI participants should obtain coverage and manage their risks in accordance with the documentation.

D.2.3 FINANCIAL RESPONSIBILITY[269]

Issue Summary. This section discusses the *financial* responsibility of a PKI participant, as a guide to an assessor in determining whether the participant has sufficient resources to perform its responsibilities. There are two groups of responsibilities: one consisting of routine duties that are part of daily operations, and the other consisting of potential contingent responsibilities to reimburse damage if there is liability for failure to perform the first group of responsibilities adequately. This section explores the various sources of financial resources available to a PKI participant, and provides a guide to the assessment of financial responsibility for both types of liabilities, as elements in an assessment of whether a particular PKI participant can be trusted.

Relevant Considerations. To review earlier discussion, PAG § D.2.1 (Apportioning Legal Responsibilities and Liability Among the Parties to a PKI Transaction) apportions the responsibilities and liability of PKI participants within roles assigned to the participants by the underlying business model. Viewed from the perspective of financial resources, the participant's responsibilities can be grouped into two subsets, operational liability and third-party liability.[270]

[269] The title of this section agrees with the corresponding section of RFC 2527, *but* PAG § D.2.3 does not replicate the subject matter of the second level headings of RFC 2527 § 2.3, namely (a) Indemnities; (b) Fiduciary relationships; (c) Administrative processes. *See* RFC 2527, *supra* note 193.

[270] *See* DSG, *supra* note 2, § 3.3, (which also recognizes two categories of responsibilities: "3.3 Financial Responsibility – A certification authority must have sufficient financial resources (1) to maintain its operations in conformity with its duties, and (2) to reasonably able to bear its risk of liability to subscribers and persons relying on certificates issued by the certification authority and digital signatures verifiable by reference to public keys listed in such certificates"). *See also* PAG APP 2 (*General Usage for International Digitally Ensured Commerce (GUIDEC),* Section on Financial Resources, Information

The first group of responsibilities consist of *covenants*, the functional responsibilities the participant has committed to perform as part of operations. *See supra* PAG § D.2.1 (functional PKI responsibilities expressed by contractual responsibilities are *covenants*, namely promises to do or refrain from certain actions over a period of time into the future). Most of these contractual covenants are promises to perform items of PKI functionality that are listed in section D.2.1, and are spelled out in more operational detail in PAG §§ D.3 through D.6.

The second group of responsibilities tends to be expressed by contractual clauses of the type called *representations and warranties*, if a contract is involved. Representations and warranties are promises that a particular state of facts has existed in the past, does exist, or will exist in the future.[271] The failure to adequately perform the second group of responsibilities leads to the question of whether that participant has *liability* to reimburse another participant for damages caused by the breach.

An assessment of financial responsibility is important to the first group of responsibilities. To state the obvious, a PKI participant responsible for performing certification functions and running a PKI, particularly a CA, will not be able to perform the challenging functions involved with running a PKI reliably and competently for very long, unless there are sufficient resources, particularly a cash flow stream, to finance the routine performance or outsourcing of the many PKI functions the participant has agreed to do by contractual covenants. In addition, the participant should have a reasonable cushion of net assets to enable an orderly transition of operations to a successor participant in the event the participant is suddenly required to terminate its services activities.[272]

Even if the participant is highly experienced and competent, if its financial resources are inadequate to support routine responsibilities, then the participant might continue to perform its functions flawlessly, but bankruptcy or the threat of it will obviously cause disruption to the other participants in the PKI. Worse still, skimpy financial resources might cause the participant to take risky shortcuts, gradually degrading the quality and performance of its PKI functions, increasing the risk of a catastrophic breach of its responsibilities. Even if it is determined that the participant is clearly liable to reimburse damages caused other participants, such a determination is worth little if the participant has insufficient resources to pay a judgment or is on the edge of bankruptcy.

Financial responsibility is important to the assessment of various PKI participants. In a case where the CA chooses to delegate front-end responsibilities to an RA, for instance, the CA should be concerned about the RA's financial responsibility to perform on the RA's indemnification of the CA for the RA's breach of its contractual responsibility. If a relying party or a subscriber is damaged by the RA's breach, the damaged party will seek reimbursement from the RA and/or the CA. If the PKI documents or other applicable agreements disclaim liability of the CA for acts of the RA as agent of the CA or otherwise, then the relying party and subscriber need to be as concerned about the financial responsibility of the RA as they are about the financial responsibility of the CA.

Even if there is an adequate cash flow stream to support trustworthy PKI operations indefinitely, an assessment of the financial resources of a PKI participant should also include review of its balance sheet, plus any contingent liabilities, to determine the extent to which the participant would be able to pay any liability it may suddenly incur to other PKI participants. Thus, the assessment of the financial responsibility of a PKI participant, particularly a CA, should involve a review of both income statement and balance sheet, preferably prepared by an independent CPA and certified to be in accordance with generally accepted accounting principles. Assessors should be alert to the common practice of separately incorporating a CA subsidiary with modest assets, leaving substantial assets behind the corporate veil of the parent corporation. An assessment of financial responsibility should carefully look behind consolidated financial statements to determine whether the

Security Committee-Electronic Commerce Project of the International Chamber of Commerce (2000), *available at* <http://www.iccwbo.org/home/guidec/guidec.asp>, hereinafter "GUIDEC").

[271] *See* PAG § C.1 (Sources of Law) for a discussion of how responsibilities can also be imposed by tort law, code or statute if a participant is not in contractual privity with another party.

[272] *See* PAG § D.5.7 (CA Termination); *see also* DSG, *supra* note 2, § 3.13.

CA is a separately incorporated subsidiary, whose creditors will not have access to the assets of the parent corporation.

Assessors should determine whether a PKI's overall financial responsibility requirements or disclosures make sense in light of the business needs of the PKI and the assurance levels provided by its certificates. Assessors should review the PKI's documentation to see whether financial responsibility requirements or disclosures appear there. They should also be aware of any externally-imposed financial responsibility requirements. An assessment of a particular PKI participant should focus on whether the participant meets the financial responsibility requirements of the PKI or matches what the PKI has disclosed.

Appropriate Requirements and Practices. There is no industry standard about the amount of financial resources a CA or other PKI participant should have as a condition of beginning operations. The appropriate level of financial resources will depend on the applications for which the certificates are intended and the assurance levels provided by the certificates.

In cases where income statement and balance sheet assets of a PKI participant such as a CA are modest, there are many techniques for supplementing the financial responsibility that stands in back of its legal responsibility.[273] Here are some possibilities:

- Contractual Indemnity. As discussed in PAG § D.2.1 (Apportioning Legal Responsibilities and Liability Among the Parties to a PKI Transaction), liability for breach of responsibility can be shifted to another participant by a contractual indemnity. For example, if a CA outsources the determination of identity of certificate applicants to an RA, the RA agreement would likely require the RA to indemnify and hold the CA harmless from any third party claims against the CA for incorrect determination of the identity of certificate applicants.

- Contractual Guarantees and Similar Surety Devices. A substantial company establishing a relatively "closed" CA for use by its own employees or customers will frequently choose to use a subsidiary CA with minimal capital. Faced with a situation where interoperability or licensure requires greater financial responsibility, the parent corporation could agree to guarantee the debts of the CA subsidiary up to a certain amount, or purchase an irrevocable letter of credit from a bank or a surety policy from an insurance company.

- Piercing the Corporate Veil. If a PKI participant such as a CA has been incorporated as a thinly capitalized subsidiary of a more substantial parent entity, other PKI participants might attempt to expand the financial responsibility of the subsidiary involuntarily by attempting to enforce their claims directly against the parent entity. This legal technique, called "piercing the corporate veil," is based upon the theory that a stockholder (or limited partner or some other controlling entity with limited liability) is privileged to avoid the liability for the debts of a controlled subsidiary because the subsidiary is a separate entity, but under certain circumstances may be held liable for the debts of the separate entity. Normally a matter of state rather than federal law in the U.S., the factors required to support a piercing the veil vary from state to state. In general, in cases where the financial responsibility of thinly capitalized PKI subsidiaries might turn out to be inadequate, the parent corporation seeking to minimize the risk of a successful corporate veil-piercing claim should take care to demonstrate clear respect for corporate formalities such as meetings and minutes, board of director independence, and fiscal separateness of the subsidiary.

- Third Party Liability Insurance. As discussed in PAG §§ C.6 (Risk Management and Insurance Principles) and D.2.2 (Risk Management and Insurance), third-party liability insurance coverage resembles a contractual indemnity in that it shifts risk from one party to another. The advantage of

[273] Some jurisdictions have minimum financial responsibility ("suitable guaranty") requirements as part of their CA licensure laws, which can be satisfied in a number of ways. *See* Utah Signature Law, *supra* note 80, § 46-3-201 and Washington Authentication Act, *supra* note 82, § 19.34.100.

insurance is that risk-adverse PKI participants without a substantial cushion of cash flow and net worth can pay an acceptably small fixed premium in order to transfer a small mathematical probability of a large risk to an entity in the business of accepting risk. The insurance company avoids risk by aggregating the premiums and loss experience of large numbers of insureds to produce a predictable risk less than the premium it receives. A typical example of third party liability insurance is customized PKI errors and omission insurance maintained by a CA or RA to defend and pay any successful claims by third parties such as a relying party or subscriber damaged by the CA's or RA's alleged negligence or breach of warranty in determining the identity of a certificate applicant. A further example is a subscriber who is a health care provider faced with (i) HIPAA liability to its patients in the event a PKI system fails to protect the privacy of the patients, as well as (ii) a risk-averse CA that insists upon strong liability limitation provisions in the subscriber agreement, such as disclaimer of consequential damages, and monetary damages limited to the amount of fees paid.

- First Party Property Insurance Coverage. First party property insurance coverage in the PKI context resembles traditional fire insurance or valuable papers insurance, in that property damage done to property, and the loss of use and occupancy profits are reimbursed without regard to fault. This type of insurance can be used by a CA in a straightforward manner to insure against the risk of loss of cash flow during disaster recovery from destruction of computer facilities by a fire, flood, storm, or earthquake. An emerging use of first party insurance coverage, sometimes used in tandem with third party liability insurance coverage, is a policy purchased by a CA that covers all its subscribers and all those relying parties who are in contractual privity with the CA, for their risk of damage caused by compromise of the subscriber's private signing key. The CA would not ordinarily have any responsibility or liability for such a loss, but might carry parallel third party liability insurance to defend it and pay any successful settlement or judgment in the event an attempt is made to bring it into the dispute between the subscriber and relying party.

- Fiduciary Claims. Although it is a debatable practice for higher assurance PKIs (*see infra* PAG § D.6.2.3 (Private Key Escrow)), there may be situations in which the particular business model of the PKI requires the CA to generate a key pair used for confidentiality encryption by employees, and thereafter to continue to hold a copy of the private decryption key in escrow in accordance with certain standards to assure the employer's controlled access to encrypted messages sent to the employee. In the event the privacy of an employee is breached, one argument against the CA in some jurisdictions might be that the CA as escrow agent holds a copy of the employee's private decryption key as fiduciary for the benefit of the employee, in the nature of a beneficiary of a trust. Protection against this type of risk might require specialized insurance because of the fiduciary nature of the liability in some jurisdictions.

D.2.4 INTERPRETATION AND ENFORCEMENT

Issue Summary. This section addresses issues that do not create PKI-related legal responsibilities among PKI participants, but are nevertheless important to the protection and enforcement of the parties' legal rights. In particular, this section covers governing law and the law that applies to various PKI documents; "boilerplate" clauses relating to severability, survival, merger, and notices; and dispute resolution provisions.

Relevant Considerations. Interpretation and enforcement provisions may apply to the document in which they appear or may be in the nature of requirements for boilerplate content that must appear in other documents. For instance, a subscriber agreement that also serves the function of a modest CPS may want to address in this section of the subscriber agreement the interpretation and enforcement provisions applying to that subscriber agreement. By contrast, a PKI may place requirements in a CP stating that subscriber agreements and relying party agreements must contain certain minimum terms relating to interpretation and enforcement.

Assessors should review a PKI's CP, CPS, PKI disclosure statement, and agreements used within a PKI, especially Subscriber and Relying Party Agreements. They should determine whether all interpretation and enforcement terms required in the PKI, for example in a CP, are included within the PKI documents being assessed. Assessors should also review the content of these provisions to ensure that they meet the PKI's requirements and are consistent with applicable law.

When reviewing interpretation and enforcement provisions in the PKI's documentation, an important issue is whether or not the CP or CPS is part of a contract with a PKI's participants, such as subscribers or relying parties. A CP or CPS could become part of the contractual relationship with subscribers or relying parties, if, for example, the CP or CPS is incorporated by reference in a subscriber agreement or relying party agreement. When a CP or CPS is part of the contract, the interpretation and enforcement terms could refer to the interpretation and enforcement of the CP or CPS itself and the extent to which the contract takes precedence over the CP and CPS in event of inconsistencies.

If, however, a CP or CPS is not part of a contract, the interpretation and enforcement provisions of the CP or CPS could set requirements for provisions that would normally appear in the documents that are part of the contract. For example, a CP could set requirements for the minimum interpretation and enforcement terms that must appear in subscriber agreements and relying party agreements. Where a CP or CPS is incorporated by reference in an RA agreement or similar agreements among participants performing CA functions, it may still be helpful to focus interpretation and enforcement provisions in a CP or CPS on requirements for terms that must appear in subscriber or relying party agreements. Assessors should consider the remainder of this section and the subsections below in light of either interpretation and enforcement terms set forth in a CP or CPS or the interpretation and enforcement terms that a CP or CPS requires as minimum terms in a subscriber or relying party agreement.

As with sections governing responsibilities and liability, the adequacy of interpretation and enforcement provisions will depend on the PKI and the context of the assessment. Assessors acting on behalf of subscriber or relying party communities will have an interest in ensuring that these provisions are fair and reasonable for subscribers and relying parties. Assessors acting on behalf of CAs or RAs will have an interest in ensuring that CAs and RAs can enforce the relevant agreements to preserve the security of the PKI and, at the same time, do not unduly expose the PKI to enforcement problems such as inconsistent decisions by courts applying the law of different jurisdictions, litigation in scattered, far-flung jurisdictions, unenforceable provisions, and alleged oral modifications to their agreements.

Appropriate Requirements and Practices. PKIs providing higher assurance certificates will likely want to ensure that all participants within the PKI are bound by some sort of agreements that contain interpretation and enforcement provisions. CAs and RAs have an interest in setting forth reasonable interpretation and enforcement provisions in order to comply with applicable law and to avoid deterring people from using their services with onerous terms and conditions. At the same time, they have an interest in including provisions to protect their interests. Subscribers and relying parties, on the other hand, have an interest in limiting interpretation and enforcement provisions so that they have a fair opportunity to raise and litigate their claims against CAs or RAs. A subscriber and relying party community will likely want to limit the ability of CAs and RAs to impose unfavorable interpretation and enforcement provisions.

D.2.4.1 Governing law

Issue Summary. A fundamental question in a dispute regarding a contract or agreement is which law will govern the dispute.[274] This issue can affect the choice of law between jurisdictions, the enforceability of a contract under the applicable jurisdiction's laws, and/or the rules of interpretation of a contract.

[274] Issues related to the question of which law governs the dispute, are the issues of where the dispute will be resolved, and by whom. Dispute resolution clauses typically take the form of: (1) resolution by a court (commonly referred to as a "choice of

Relevant Considerations. In the case of any agreement involving more than one jurisdiction, it is advisable to include an "applicable law" clause, particularly those used in the PKI context. A choice of law clause not only enhances the predictability of the agreement's interpretation, but also may actually favor one party over another by choosing a particular body of substantive law.[275] In addition to the customary factors considered in selecting applicable law for traditional transactions (e.g., developed, stable, and commercially-sophisticated law; interaction with contractual dispute resolution mechanism such as place of arbitration), for electronic transactions, parties should also evaluate the various country laws relating to e-commerce such as electronic signatures, online privacy, and consumer protection.

Assessors should review the governing law clauses in the PKI's documentation, if any. They should determine whether or not any externally-imposed requirements dictate a choice of law. In rudimentary PKI's, there may be little by way of documentation and, if there were documentation, the documentation may not contain a discussion of governing law. In the absence of a governing law in the clause, the court in any litigation will likely apply the choice of law rules of the forum jurisdiction to determine which law should be used to interpret the contract. Choice of law rules vary from jurisdiction to jurisdiction, and the following are some of them:

- The substantive law of the forum jurisdiction itself,
- The law of the place where the contract was made (which might mean the place where the contract was "executed," if any),
- The law of the jurisdiction with which the transaction has the most significant contacts or involvement with the parties, or
- Mandatory law that, under principles of public policy of the forum, applies to the contract, for example, a forum jurisdiction's public policy that applies the law of the residence of a consumer. [276]

Appropriate Requirements and Practices. CAs will likely want to utilize governing law clauses in their agreements that apply the law of the CA's principal place of business, because a CA will be knowledgeable about the law of its own jurisdiction and accordingly will find it convenient to utilize such law in any disputes. With such a clause, the CA need not familiarize itself with the laws of the places where its customers, subscribers, and relying parties are located, and one set of laws will apply to the documentation, precluding the risk of inconsistent judicial interpretations of a single set of provisions due to the application of different jurisdictions' laws. By contrast, subscriber and relying party communities may want to negotiate with policy makers within the PKI for the absence of a governing law provision or an acknowledgement that the law of the jurisdiction of any claimant against the CA will apply to disputes.

PKIs offering lower assurance certificates may find less need for sophisticated PKI documentation with governing law clauses. With regard to PKIs offering higher assurance certificates, however, it is common for a PKI's documentation to include a governing law clause, either relating to the interpretation of a CP or CPS or a requirement for a governing law clause to appear in subscriber agreements or relying party agreements. Assessors acting on behalf of CAs will likely want to ensure that the laws of a single jurisdiction apply to the relevant agreements to promote uniformity in the interpretation of the agreements and make it more convenient for the CA to manage claims. The PKI documentation should meet the requirements placed on it by applicable

forum," "jurisdiction," or "venue" clause—e.g., a case where the parties consent to the exclusive jurisdiction of the forum court); (2) arbitration; and increasingly (3) non-arbitration forms of alternative dispute resolution ("ADR"). *See infra* PAG § D.2.4.3 (Dispute Resolution Procedures).

[275] For example, UCITA is widely considered to be relatively favorable to licensors in transactions to which it is applicable (licenses of computer information). Accordingly, a licensee in a proposed transaction governed by UCITA should be alert to a draft agreement offered by the licensor that specifies the governing law to be that of Virginia or Maryland, the two States where UCITA has been adopted as of this writing.

[276] *See infra* PAG § C.5.1.2 (Jurisdiction, Forum Selection and Governing Law).

law and contract. [277] For example, the documentation should not run afoul of any limitations on the ability to designate governing law established by consumer protection laws.

D.2.4.2 Miscellaneous Provisions

Issue Summary. There are several standard contract clauses that a PKI may wish to include in preparing its documentation. RFC 2527 identifies four such clauses: severability, survival, merger, and notice.

Relevant Considerations. The clauses addressed in this section concern the following issues:

Severability. What happens when a clause within an agreement is held to be invalid or unenforceable under applicable law?

Survival. When an agreement terminates, are there any provisions that continue in force and effect despite the closing or termination?

Merger. Does the writing embodying an agreement constitute the entire agreement among the parties, or were there side arrangements, either oral or written, that are not contained in the writing?

Notice. How should or can the parties communicate notices to each other? Should they be in writing? How must the writing be delivered?

Assessors should review the PKI's documentation to determine whether it contains miscellaneous provisions, including severability, survival, merger, and notice provisions. They should also determine whether these clauses are appropriate for the PKI. Again, terms within a CP or CPS may relate to the interpretation and enforcement of the CP or CPS itself, or may be requirements for minimum terms within Subscriber Agreements, Relying Party Agreements, or other agreements. They should then determine whether the clauses achieve their purposes and whether they meet any restrictions imposed under law or contract.

(a) Severability. Severability clauses are used to prevent an overall agreement from being invalidated when only one term is determined to be invalid or unenforceable. Clauses of this kind generally provide that if a portion of the agreement is unenforceable, a court may enforce the rest of the agreement if that portion was not an essential part to the agreed exchange.[278] Failure to have a severability clause can render the entire agreement unenforceable when that is not the parties' intention.[279]

(b) Survival. Survival clauses are used to ensure that particular provisions will survive the termination of the agreement in which they appear. Survival may be permanent or limited to a period of time.

(c) Merger. A "merger" or integration clause is used to confine the terms of an agreement to the document or record that sets forth the agreement. It prevents parties in a dispute from arguing that other prior or contemporaneous promises were made, whether oral or written, that are not included in the written agreement.

[277] Moreover, assessors may want to determine whether certain law applies automatically unless disclaimed by the parties, such as the United National Convention on Contracts for the International Sale of Goods (CISG). CISG is the uniform international commercial code of more than 50 countries. When a contact falls within the scope of the CISG, the contract is automatically governed by it, unless the parties exclude it. Absent special circumstances, it is frequently wise to exclude CISG from contracts because of the uncertainty of its application and potential surprises in jurisdictions where practitioners are accustomed to the principles of uniform laws such as the Uniform Commercial Code in the U.S.

[278] RESTATEMENT (SECOND) OF CONTRACTS § 184. *See also Mad River Boat Trips v. Jackson Hole*, 803 P.2d 366 (Wyo. 1990).

[279] See Machen, Inc., v. Aircraft Design, Inc., 828 P.2d 73 (Wash. 1992), overruled by Waterjet Tech. v. Flow Int'l, 996 P.2d 598, 602 (Wash. 2000).

(d) Notice. A notice clause sets forth the form in which parties to an agreement must communicate with each other, usually in writing. They also state how the communications are to be delivered, such as postal mail, fax, e-mail, and the like. They may also state the time on which a notice is deemed to be made, such as the date the recipient actually received it or a date of constructive notice, such as three days after a notice is mailed. Time of notice provisions are useful when notices must be made within certain deadlines.

Appropriate Requirements and Practices. The presence or absence of severability, survival, merger, and notice clauses depends on the nature of the PKI. In rudimentary PKIs offering low assurance certificates, there may be no need for complicated agreements or the "boilerplate" provisions that usually appear in them. In PKIs offering higher assurance certificates, however, such clauses are common and help clarify critical issues for the PKI.

Severability clauses are particularly helpful when there is some concern of the PKI that some of the provisions in its agreements may be determined by a court or other tribunal to be invalid or unenforceable. They can prevent such a determination from causing the invalidity or unenforceability from impairing the remainder of the agreements. Survival provisions help a PKI clarify which provisions of their agreements should continue in effect beyond the termination of the agreement. For example, confidentiality terms or terms establishing intellectual property ownership are often treated as permanent or lasting responsibilities that should be in effect even if a service has terminated. Merger clauses are useful for a PKI to control the content of the contractual relationship by focusing a court or tribunal only on the written contract. They cut off claimants' possible argument that side deals, especially hard-to-disprove oral agreements, should be considered part of the contractual relationship. Notice provisions are helpful for clarifying the mechanics of how the parties must communicate with each other.

A PKI will likely want to use the miscellaneous clauses described in this section to the extent needed by the business needs of the PKI. PKIs having a need to enforce certain requirements, smoothly interoperate with other parties, and minimize their liabilities will probably want to use such clauses in their agreements. To the extent such clauses are important for a PKI, it will generally want to impose in a CP or CPS the requirement on its participant to include these clauses in agreements they use, such as subscriber and relying party agreements. PKI participants should include any externally-required terms and the actual agreements they use should contain the terms required or disclosed in the PKI's documentation.

D.2.4.3 Dispute Resolution Procedures[280]

Issue Summary. This section addresses where and by whom disputes among PKI participants will be resolved, especially claims by subscribers or relying parties against the CA, RA, repository, or other service provider. This section may also address whether the PKI chosen arbitration or other alternative dispute resolution (ADR) mechanism for resolving dispute, or whether litigation be the default mechanism. If litigation is the dispute resolution mechanism, this section may identify a specific forum for the litigation in which claims must be asserted. Finally, this section may state whether there other procedural rules or acknowledgements of the parties that apply to dispute resolution procedures.

Relevant Considerations. Assessors should review the PKI's documentation and determine whether it provides for dispute resolution procedures. In the absence of any dispute resolution mechanisms, and if parties are unable to resolve a dispute through negotiation, the parties must resort to the court system and litigation to resolve their disputes, or voluntarily use other methods such as arbitration or mediation after the dispute has arisen. If the PKI documentation does contain dispute resolution mechanisms, assessors should determine whether these procedures accomplish their intended purposes for the PKI.

[280] *See generally* PAG APP 2 (International Arbitration and Forum Selection Agreements: Planning Drafting and Enforcing, Dispute Toolkit, Born, G. (1999), *available at* <http://www.linklaters.com/disputetoolkit/>, hereinafter "Born").

Before electing to use, or agree to an arbitration or mediation clause in a contract (or requiring such mechanisms in a CP, CPS, or PKI disclosure statement), a party should be aware of the advantages and disadvantages of arbitration and mediation. In considering whether or not to require arbitration, a CA or other parties should consider the following factors:

- The ability to appeal;[281]
- importance of publication of decisions;[282]
- size of dispute settlement body;[283] and
- the structure of the proceeding.

Moreover, if the documentation provides for ADR procedures, assessors should determine whether agreed procedures of this kind are enforceable under applicable law. In recent cases, claimants have challenged whether arbitration provides them with a full and fair opportunity to have their claims resolved.

Assessors should also check whether the PKI documentation includes a choice of forum, jurisdiction, or venue clause in its dispute resolution provisions. Statutes and rules governing licensed certifications authorities may require the subscriber agreement, CP, or CPS to include any mandatory choice of forum provision.[284] On the other hand, applicable law may limit the ability of a CA to impose such a clause on PKI participants, especially Subscribers and Relying Parties that are consumers.[285]

In addition, in the litigation context, PKI documentation may state that a certain forum has exclusive jurisdiction over the dispute. For example, if a CA brings an action against a Subscriber or Relying Party in a local forum, the Subscriber or Relying Party may claim that he, she, or it is not subject to the jurisdiction in which the CA is located. Litigation over jurisdictional issues, especially if the only contact with the forum jurisdiction by the party disputing jurisdiction is via the Internet, is ongoing.[286]

[281] It is generally not possible to appeal an adverse arbitral decision.

[282] Arbitral decisions are generally not published. The fact of publication establishes precedents, and consequently, a court rather than an arbitrator may be more willing to consider the long-term implications of a decision.

[283] The American Arbitration Association (AAA) rules require a panel of three arbitrators, if the size of the dispute is sufficiently large. Commentators dispute whether a three-arbitrator panel is desirable. Some contend that it leads to more consistent decisions, whereas others argue that a three-arbitrator panel is more expensive, and eliminates the obvious cost-saving benefits of arbitration.

[284] *See, e.g.,* PAG APP 2 (*Certification Practice Statements*, Minn. R. 8275.0045.E (2000) hereinafter "Minnesota Cert. Practices"); *see also* Washington Admin. Code, *supra* note 7, § 434-180-330(5).

[285] *See* Brussels Convention *supra* note 118; *see also* PAG APP 2 (*Jurisdiction and Enforcement of Judgments in Civil and Commercial Matters*, European Commission, 1999 O.J. (L 319), 9 (1999) (European Free Trade Association (EFTA) Convention), *available at* <http://www.curia.eu.int/common/recdoc/convention/en/c-textes/lug-idx.htm>, hereinafter "Lugano Convention"). EU Rome Convention, *available at* <http://www.jus.uio.no/lm/ec.applicable.law.contracts.1980> (addresses applicable law in consumer transactions). EU's Brussels Regulation (clarifying the Brussels Convention) *available at* <http://europa.eu.int/eur-lex/en/lif/dat/2001/en_301R0044.html>, which will enter into force on 1 March 2002, permits a consumer to sue an online supplier domiciled in an EU Member State in the courts of the Member State of the consumer's domicile, even though the contract between the consumer and the supplier may choose the supplier's jurisdiction. Also, the proposed Rome Regulation suggests that in non-contractual B2C disputes, the law of the consumer's country would apply. *See generally* PAG APP 2 (*Jurisdiction and Applicable Law in Cross-border Consumer Complaints*, ECLG/157/98 (29 Apr. 1998) *available at* <http://europa.eu.int/comm/consumers/policy/eclg/rep01_en.html>, hereinafter ("Rome II Green Paper").

[286] See, e.g., PAG APP 2 (Of New Wind and Old bottles: Personal Jurisdiction, the Internet, and the Nature of Constitutional Evolution, Redish, M.H., 38 JURIMETRICS J. 575-610 (1998), herinafter "Redish"); see also PAG APP 2 (Law of E-Commerce, Winn, J., & Wright, B. (4th ed. 2001) Chap. 3, hereinafter "Winn").

Assessors should analyze the applicable law relating to dispute resolution. Some mechanisms may be required and some prohibited. At a minimum, applicable law may require certain disclosures relating to dispute resolution. Statutes and rules governing licensed certification authorities may require the CP, CPS, or other documentation to include and prominently display a mandatory dispute resolution process, especially when some of the PKI's participants are consumers.[287]

Appropriate Requirements and Practices. PKIs should adhere to any limitations placed on them by applicable law with respect to dispute resolution. Subject to such laws, PKIs will want to establish dispute resolution mechanisms that constrain risks and liability, but provide an environment that is sufficiently fair so as not to deter customers from using their services. Moreover, they may have an incentive to require certain alternative dispute resolution mechanisms to reduce the cost of claims and possibly find more hospitable triers of fact. Subscriber and Relying Party communities may have an incentive to scrutinize alternative dispute resolution mechanisms, under the view that it favors members of the PKI industry. CAs and other service providers, however, may want to look for such mechanisms because they may be necessary to avoid the biases of the court systems that may favor hometown Subscribers and Relying Parties over foreign corporate CAs or other service providers.

D.2.5 FEES

Issue Summary. This section addresses the amount and the manner in which PKI entities, most commonly CAs, charges for their services.[288] The subsections of this section list the various possible services for which fees may be assessed and state whether, in fact fees are charged for these services within the PKI.

Relevant Considerations. Assessors should review the PKI's documentation to determine whether the PKI (e.g., a CA or RA) charges fees for various services. The different kinds of fees possible are described in the various subsections of this PAG § D.2.5. Assessors will want to determine whether the fees charged or required by a PKI make sense in light of the PKI's business model so that they provide adequate revenue for the PKI to operate its services, but are not so high as to deter people from using its services or to cause the PKI to lose business to competing PKIs.

Assessors should determine whether a CA's or RA's fee structure is consistent with requirements or limitations imposed by contract or applicable law. For example, a CP might permit CAs to charge fees for Certificates, but prohibit charging a fee for Certificate status information, in order not to discourage the dissemination of Certificate status information. Assessors should determine if the PKI's documentation is consistent with these requirements. Finally, assessors should determine whether the fees charged within the PKI are, in fact, consistent with the requirements and disclosures set forth in its documentation.

Appropriate Requirements and Practices. The decision to charge a fee or not for various services will depend on the PKI's business model. If the certification services were the means by which the CA or RA obtains revenue, it would be natural to charge a fee, at least for issuing and renewing or rekeying the Certificates themselves. If, however, the certification services are an ancillary one to the marketing of other services, the CA or RA may want to absorb the cost of the Certificate and other services and fold such expenses into the cost of the principal business.

---

[287] *See* Minnesota Cert. Practices *supra* note 284; *see also* Washington Admin. Code *supra* note 7.

[288] In documents that follow the RFC 2527 framework, it is rare for this section to contain much detail about the fee structure or the various amounts charged as fees by PKI service providers. While a fee schedule might populate this section in a corresponding CP or CPS, such detail is usually reserved for an easily-amended fee schedule. However, because this document will serve as a reference for performing PKI assessments, a more detailed discussion of PKI fee structure is provided than would normally be found in an RFC 2527-compliant document.

If the PKI does charge for various services, the relevant considerations in deciding what a CA or RA should charge for its services are how much to charge and whether to make the fee structure confidential. In setting fees and publicizing a fee structure, important considerations include whether a PKI's business model is open or closed, whether the fee structure accounts for the relationships among the various parties within the PKI, and whether the fee structure is appropriate in light of the attendant risks involved.

Fees charged by a CA for services should generally be commensurate with the type of service being provided and should be consistent with applicable law and requirements imposed by contract. A CA or RA may have a publicly available price list and/or may have confidentially negotiated fee structures for specific customers. Whether the fee structure is public or confidential, the PKI's documentation should clearly set forth those fees before and after the fact to those who generate the charge(s) and to those who are responsible for paying them. Hence, clear information regarding the specific charges for any and all CA or RA services should be available to a Subscriber, Relying Party, or customer obtaining Certificates in bulk for a Subscriber community before and after those services are rendered. A CP might also state that the fees charged must be in accordance with a fee schedule approved by the policy management authority.

Moreover, as a general matter, a PKI's fee structure should not inadvertently inhibit the development of the PKI by creating a disincentive to the use of its services. For example, assessors may want to ensure that the PKI's fee structure apportions costs among the various parties in a manner that is appropriate for the deployment of the PKI

D.2.5.1 Certificate issuance or renewal fees

Issue Summary. This section addresses fees a CA or RA charges for the processing of a Certificate Application and/or for the issuance and renewal of Certificates. Specifically, this section discusses how a CA or RA might structure these fees.

Relevant Considerations. PKIs have four options with respect to charging certificate issuance or renewal fees. First, a PKI may charge subscribers on a retail basis for certificates issued to them. Under this model, each subscriber obtains certificates one at a time or as packages of relatively small numbers. Such a retail price would likely be the highest price a PKI would charge for certificates. Second, a PKI may provide certificates to organizations in bulk for further distribution to the organization's members. The purpose of such bulk purchases is for use of the certificates within the organization's business applications. The organization may or may not charge the end-user subscribers a fee for distributing certificates to them. This method of providing certificates would likely result in a lower per-certificate cost than providing certificates on a retail basis. Third, a PKI may provide certificates to a business partner in the role of a distributor who, in turn, resells the certificates on a retail or wholesale basis. Unlike the second model, such certificates are not for the business partner's own applications, but rather are intended for applications of the distributor's end customers. Fourth, a PKI may choose to provide certificates to end-user subscribers without charging a fee. The PKI may be able to build the price of the certificate into other fees charged to subscribers or may be able to recoup the costs of the certificates by charging a third party for them. For instance, a brokerage may be able to provide certificates to its customers without charge and try to recoup the costs through commissions or an annual maintenance fee.

If a PKI does charge certificate issuance or renewal fees, the PKI can provide in its contracts with subscribers that they agree to pay the applicable certificate issuance fee if they are issued a certificate, or as a condition of accepting a certificate application. The assessor should review the subscriber agreement and determine whether the certificate issuance fee is an application fee as opposed to a service provider fee. Payment may be made by credit card, direct debit, purchase order, invoice or some other payment method made available through the service provider, or through other previously-made payment arrangements, e.g., vouchers, bulk purchase contract, etc.

Assessors should be aware of the PKI's business model and determine how certificate pricing factors into it. They should also be aware of any externally-imposed requirements or constraints on the price that PKI

participants may charge. Such requirements may arise under contract or applicable law. Assessors should review the PKI's documentation to determine if it sets requirements and discloses practices relating to charging for certificates and their renewal. Finally, assessors should determine whether the fees charged by PKI participants match the parameters set by the PKI's documentation.

Appropriate Requirements and Practices. The nature of the PKI's business model is perhaps the most relevant consideration when assessing a CA's or RA's given fee structure for the issuance and renewal of certificates. The choice of which of the four pricing models above is best will depend on factors such as:

- Whether the CA or RA is in the business of providing certification services or whether the PKI is merely a value-added service that is secondary to some other, more important service,
- Whether the PKI participant is a CA or RA that has the infrastructure and desire to provide services to the general public or whether the participant is instead a CMA that wishes to provide back-end services for other PKI participants,
- Whether the PKI participant has available connections and business partners to support different distribution channels for certificates,
- Whether a third party is available and willing to pay for certificates issued to subscribers,
- Whether the PKI faces competition from competing PKIs that may limit its ability to set high prices,
- The extent of transaction costs that impact the economic feasibility of charging a fee.

Where a PKI does charge for certificates, circumstances specific to the PKI will determine whether the fee is a non-refundable application processing fee or whether the fee is refundable if a certificate is not issued.

In any case, the pricing model chosen by the PKI should be appropriate for its business model. Certificate issuance fees can be broken down into at least three different cost components: I&A/LRA services, certificate manufacture and token issuance. The cost to manufacture certificates also might be separated from other certificate issuance costs. From the example above, where the I&A portion of cost is assumed by the RA, the fee charged for certificate issuance might consist primarily of the costs related to securely manufacturing the certificate – costs for staffing and securely housing the CA server. If the software used to create the certificates is licensed from a third party, then the certificate issuance fee might also cover the cost of maintaining the software license. The storage mechanism required for the private key may be another component of certificate issuance. For example, where the CP specifies that the private key must be stored on a token rated at FIPS 140-1 Level 2 or better, the PKI service provider might bundle the price for the purchase of the token and certificate issuance together.

The pricing requirements and practices should be reflected in the PKI's documentation. The documentation should account for any externally-imposed requirements for or limitations on pricing imposed, for example by contract or applicable law. Finally, the prices actually charged by PKI participants should be consistent with requirements, disclosures, or limitations appearing in the PKI's documentation.

D.2.5.2 Certificate access fees

Issue Summary. This section addresses fees a CA or repository may charge for allowing potential Relying Parties to have access to Certificates so that they can use such Certificates for applications within the PKI. In specific, this section discusses whether the CA or repository should charge such fees and, if so, how it might structure them.

Relevant Considerations. The possibilities for CAs or repositories charging certificate access fees are:

- Charging a relying party to obtain a certificate for the relying party to use for the relying party's applications,
- Charging a third party for permitting relying parties to obtain certificates, or
- Providing certificates to relying parties without charge, by building the price of providing certificates and associated directory services into the price of providing certificates to subscribers.

The PKI business model may involve a fee in the form of a subscription or a transactional charge, to obtain access to certificates published and accessible in a repository or directory using Lightweight Directory Access Protocol (LDAP). The certificates for which a fee is charged can also be bundled within an LDAP directory additional valuable information about subscriber attributes, authorizations, etc.

Assessors should determine whether charging for access to certificates fits within a PKI's business model and, if so, which pricing model is most appropriate for the PKI. Assessors should also ascertain whether any external requirements for or limitations on certificate access fees apply, for example under a contract or by operation of applicable law. They should also review the requirements and disclosed practices relating to charging for certificates in the PKI's documentation. Lastly, assessors should check whether PKI participants are, in fact, charging (or not charging) for access to certificates in accordance with the PKI's documentation.

Appropriate Requirements and Practices. Whether a PKI charges relying parties, directly or indirectly, for access to certificates will depend on the nature of the PKI's business model. The factors relating to certificate issuance or renewal fees in PAG § D.2.5.1 will also apply in the context of certificate access fees as well.

It is relatively uncommon for PKIs to charge a fee for providing certificates per se. PKIs instead build the cost of providing certificates to relying parties into the price of certificates that they charge to subscribers or their sponsors. This latter model is most appropriate for open PKIs, where the PKIs typically want to encourage relying parties to obtain easy access to certificates. Charging a fee to obtain certificates would place an obstacle to that goal and thereby tend to defeat the open PKI's objective of permitting anyone to rely on certificates. By contrast, certificate distribution within a closed PKI tends to be easier, and relying parties may have stronger incentives to obtain certificates with a commensurately stronger willingness to pay for certificate access.

In any case, the choice of charging a fee for certificate access and, if so, the pricing model for charging such a fee should make sense in light of the PKI's business model. Whatever fees are charged or prohibited should be reflected in the PKI's documentation and should be consistent with any requirements or limitations imposed by contract, applicable law, or other external source. Finally, PKI participants should only charge fees to the extent permitted or required by the PKI's documentation.

D.2.5.3 Revocation or status information access fees

Issue Summary. This section is related to the discussion in PAG § D.4.9.7 (Notification of Certificate Revocation to Others) and addresses the fees a CA or repository may charge for allowing potential relying parties to have access to certificate status information in connection with the relying parties' use of certificates for applications within the PKI. More particularly, this section discusses whether such fees are appropriate within the PKI and, if so, how a CA or repository might structure these fees.

Relevant Considerations. As mentioned in PAG § D.4.9.7, much has been written about the different mechanisms available to check for certificate revocation. To determine certificate status, a relying party may want to implement a process of CRL checking, OCSP, or a combination of both. The fee structure for revocation checking will depend on the mechanisms selected to check for certificate status, which may in turn

depend on the legal or policy requirements of the PKI. For instance, some PKIs may require that all transactions be validated with a signed OCSP response.

The possibilities for CAs or repositories charging fees for certificate status information are similar to those for certificate access fees. A CA or repository can:

- Charge a relying party to provide him, her, or it with certificate status information on a transactional basis when a relying party wishes to rely on a given certificate or on a subscription basis for the relying party to obtain access to some or all status information that the relying party could potentially need,
- Charge a third party for permitting relying parties to obtain certificate status information, or
- Provide certificate status information to relying parties without charge by building the price of providing such information into the price of providing certificates to subscribers.

In addition, however, a CA or repository could create multiple tiers of service, permitting all relying parties with a certain basic level of information, such as information in CRLs, for no cost or a nominal charge, and charging a fee or a higher fee for a higher level of service. Such a higher level service could involve providing more up-to-date information, for example OCSP services, or could involve coordinating and arranging revocation information in a way that makes it easier to use or more useful to analyze.

The fees charged for the service might be similar to the credit card processing model, with a PKI service provider charging a minimal transaction fee for providing certificate status. Alternatively, the PKI service provider might charge a single subscription fee on a monthly or yearly basis. The examples given above are often characteristic of an OCSP service.

A per transaction fee may be less suitable for a service that allows certificate checking via CRLs because multiple transactions can be validated using a single CRL. CRLs have other advantages, and they have disadvantages as well. In addition to the short response time that a local CRL provides, a CRL may be a cost-effective means to validate certificates in low-value transactions where the infrequent revocation of a certificate keeps the CRL relatively small. In such situations, the relying party's system can be designed to check for and pull down updated CRLs as often as convenience and risk management dictates. However, a CRL may only be considered valid at the time it is published. As the size of the CRL and the value of the underlying transaction grow, the CRL becomes a less cost-effective solution.

The solution chosen in some situations might include a combination of both CRL and OCSP checking. For example, a relying party using certificates for both low-value access control and high-value financial transactions might want to use CRLs for access control with OCSP for its financial transactions. The fee structure might be a hybrid of subscription and per transaction charges.

Assessors should examine the PKI's business model to see what kind of policy towards charging for certificate status information is appropriate. They should also determine whether any external requirements, imposed via contract, applicable law, or otherwise, bear on whether and to what extent the PKI can charge for certificates status information. Assessors should also examine the PKI's documentation to see what it says about charging for such fees and whether it is consistent with any external requirements. Finally, assessors should check whether PKI participants are complying with the PKI's documentation.

Appropriate Requirements and Practices. As with charging for access to certificates themselves, the policies relating to charging for certificate status information depend on the PKI's business model. Again, the factors relating to PAG § D.2.5.1 (Certificate Issuance or Renewal Fees) will also bear on the policies relating to charges for certificate status information.

Similar to certificate access fees, charging for certificate status information is not the most common model, although it is more common than charging for certificate access, at least with regard to charging for higher-value certificate status information, such as OCSP. In fact, open PKIs may want to preclude the practice of charging for certificate status information. To the extent they want to impose a requirement on a large, distributed population of relying parties to check certificate status, they will want to make it easy for relying parties to obtain certificate status information. Charging a fee for that information will discourage relying parties from checking certificate status, and therefore work against the PKI's objective to make sure relying parties check certificate status in all cases. On the other hand, relying parties in closed PKIs may have a stronger incentive to check certificate status and therefore a greater willingness to pay a fee for certificate status information.

If a PKI does decide to charge a fee for certificate status information, a number of different models could apply. Similar to the credit card processing model, a PKI service provider may want to charge a minimal transaction fee for providing certificate status. This service might consist of digital time-stamping, transaction signing, and an insurance- or collateral-backed warranty program to help establish nonrepudiation. For example, relying parties could be required to pay certificate validation fees based on the actual number of validations performed on a monthly basis. Validation fees under this model could vary between $5.00 and .01 depending on transaction volume, transaction warranty coverage, and transaction type.

Whatever the choices made by the PKI concerning charges for certificate status information, the PKI's policy relating to such charges should make sense in light of its business model. Such policies should be consistent with any external requirements and should be documented in the PKI's documentation. Finally, the PKI's participants should, in fact, charge or not charge fees in accordance with the PKI's documentation.

D.2.5.4 Other Fees

Issue Summary. This section specifies any other fees for services not included in the other categories of certificate issuance and renewal, certificate access and certificate status services.

Relevant Considerations. A PKI service provider's fee schedule may also contain charges for root key generation, installation and set-up, collocation services, software licensing, service and maintenance, as well as fees for professional services related to policy development, system integration, training, project management, etc.

Appropriate Requirements and Practices. If an "Other Fees" section is used (for example in a government-issued RFP), an appropriate requirement or practice would be: vendors shall state the fee for the generation and delivery of a self-signed CA Certificate performed according to the key generation ceremony specified herein. Vendors should also bid on the cost to provide secure hosting and collocation of the CA root key and other amounts for annual costs of software licensing, support and maintenance.

D.2.6 PUBLICATION AND REPOSITORIES

Issue Summary. This section addresses obligations of a CA to publish the certificates that it issues, as well as certificate revocation or other status information. It also addresses publication of a CA's documentation, such as the applicable CP, CPS, PKI disclosure statement, subscriber agreements, and relying party agreements. Furthermore, the section addresses when and how often the CA must publish such information. Also, the section covers security mechanisms to control access to the information published to prevent unauthorized access or tampering.

Relevant Considerations. Assessors should review the PKI's documentation, particularly its CP, CPS, and outsourcing agreements with repositories to determine the publication obligations of the various parties. Assessors should focus on agreements with repositories to ensure that all required publication functions are accounted for and responsibilities are clearly divided between the CA and repository. To some extent, there is

overlap between this section and the discussion of repository obligations in PAG § D.2.1.5 (Repository Responsibilities and Liability) *supra*. If the PKI documentation treats these issues comprehensively in section D.2.1.5, there may be nothing more than a cross-reference in section D.2.6 (of the PKI documentation) to the discussion in section D.2.1.5 (of the PKI documentation). If section D.2.1.5, however, has a cross-reference to section 2.6 and other repository discussions, the main discussion of repository functions may appear in this section.

With respect to the frequency of publishing certificate status information, this section may or may not deal with such requirements in detail. The frequency of publishing such information is also covered by sections discussing revocation and suspension. *See, e.g.*, PAG § D.4.9.7.1 (Notification of Certificate Revocation to Others). Therefore, this section of the PKI documentation may cross-reference more detailed treatment of this issue in section 4 of such documentation.

From the perspective of an assessment on behalf of an entire PKI, assessors may want to ensure that the CA and/or its repositories are publishing all of the information required by the PKI, consistent with the PKI's documentation, particularly a CP. Assessors should be aware of any requirements imposed by contract or applicable law either requiring or limiting the publication of certain information. Limitations may arise through the operation of privacy laws and consumer protection laws. These requirements may be as to form, content (plain English) and presentation, duration of storage, and information collection and access policies. *See* PAG §§ C.5 (Consumer Issues and Privacy), D.2.8 (Consumer Issues, Information Practices, Privacy), and D.4 (Certificate Life Cycle Operational Requirements). In addition, assessors should be aware of any security requirements placed on repositories by law or contract.[289]

Appropriate Requirements and Practices. Assessors should ensure that the PKI documentation adequately covers the publication obligations appropriate for the PKI, by provisions in sections D.2.6, D.2.1.5, and the revocation and suspension requirements of section 4. What is appropriate in the context of any given PKI will depend on the nature of the PKI's business model. In lower assurance PKIs where revocation is not offered as a service, there may be no publication of revocation information. In such environments, the PKI may not feel it necessary to write or publish extensive policy documentation.

Generally, however, CAs are be viewed as under an obligation to critical information relating to its services. Such information normally includes:

- The Certificates issued by the CA so that relying parties can use them for their intended application,
- Certificate revocation and other status information, in order to inform relying parties when certificates are unreliable; revocation services are considered a critical part of providing all but the lowest-assurance PKI services,
- Policy and practice information, including any applicable CP, CPS, PKI disclosure statements, and agreements such as subscriber and relying party agreements. To the extent that this information is directed to consumers it should be presented in an easily accessible form both in terms of the actual content and in terms of navigation.

Publication of revocation information can take place by publishing a CRL or making the certificate status available through an on-line database of information accessible via the web or OCSP queries.

A common exception to the foregoing requirements exists where the PKI is closed or information within policy and practice documentation is security sensitive and treated as confidential. When the PKI is closed, a PKI may not want to publish certificates broadly to prevent misuse of the certificates beyond their intended application

[289] *See supra* notes 114 and 266 and PAG § C.5.3.5 (HIPAA) (discussing HIPAA requirements for the security of information systems containing personally identifiable health information).

within the closed environment. For the same reason, certificate status information and policy and practice information may be narrowly disseminated only to the participants within the closed system.

In addition, policy and practice information may contain sensitive security information, which, if published, could compromise the security of the PKI. In these situations, some information is required to be treated as confidential. In these situations, some PKIs have a "public" set of documents and confidential "internal" documents. The public documents contain no sensitive information and can be safely disseminated broadly for marketing and other business purposes. The internal documents can contain the operational guidelines and parameters to assist the PKI's operations, and dissemination of such documents can be limited to personnel having a need to know the information.

In terms of the frequency and promptness of publication, higher assurance PKIs commonly impose an obligation on CAs to publish the foregoing information within a reasonable time, which the PKI may set at a specific period of time. With respect to the publication of certificates and policy information, such a requirement may mean that a CA should publish these items within a reasonable time after creating certificates or writing the policy information. With regard to certificate status information, such a requirement may mean publish such information within a reasonable time of being informed of key compromise or receiving a request for revocation.

In PKIs providing higher assurance certificates, it is likely desirable to have security mechanisms in place to protect the repository of a CA. Such a requirement would dictate the use of access control technology to prevent unauthorized access to the repository and tampering with its systems. Indeed, security mechanisms may be required to protect the privacy of subscribers.

Finally, this section can deal with the division of responsibility between a CA and any repository service that the CA uses to perform publication functions. It is helpful for policy and practice documentation to disclose whether the CA uses a separate repository. If so, the documentation should discuss which functions are performed by the repository and which the CA retains.

In general, assessors should ensure that the publication functions performed by the CA and/or repository meet any requirements imposed on them by applicable law or contract. For instance, CAs may be under an obligation to make their CPSs publicly available under some jurisdictions' laws. Also, assessors should make sure that any privacy or other restrictions imposed by law or contract are implemented properly.

D.2.7 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Issue Summary. This section primarily concerns the periodic assessment of PKI participants (primarily CAs, and RAs, but also repositories, and other entities) to determine whether a PKI or an entity within a PKI complies with certain benchmark control objectives. Most often, such assessments are in the form of audits. Specifically, the issues covered in this section concern who is performing the assessment, how often the entity needs to be assessed, what topics are covered by the assessment, the communication of assessment results, and what happens if deficiencies are shown by the assessment. This section addresses many concerns involved with periodic audits. In addition, where a PKI requires assessments other than periodic compliance audits, this section is a helpful place to describe requirements relating to these other kinds of assessment. One example is a one-time review that a PKI may require a CA to undertake before the CA is allowed to begin operations. The issues of who performs these assessments, what topics are covered, communication of results, and consequences of deficiencies are similar to the audit context.

Relevant Considerations. A compliance assessment (most often, an audit) is designed to determine the degree to which a PKI participant (most likely a CA) operates in accordance with stated security policies and procedures (including the relevant CPs, CPSs, and other relevant documents). In general terms, such an assessment will likely determine whether the entity "keeps its word" with respect to how it operates. In other

words, does the entity do what it promised to do, and does the entity do it in a manner that would appear to be reasonable given applicable standards of care?

Assessors should review the PKI's policies and procedures documentation, inquire of management and operations personnel, observe implemented processes and controls, and perform tests to verify that processes and controls are operating as intended. Applicable assessment criteria covering environmental, key management, and certificate life cycle management controls should be used.

Assessors should also ascertain whether there are specific legal or other assessment requirements that must be met by the audited entity. For example in some jurisdictions, there may be specific audit requirements for licensed CAs that require a specific type of audit report, the use of a certain set of criteria, or a certain audit frequency. Assessors should ensure that the PKI participant's assessment meets such requirements.

Appropriate Practices and Requirements. The stringency of standards for qualifications and conduct of auditors, the thoroughness of the audit, the controls over communicating results, and the severity of consequences in the event of deficiencies will likely be commensurate with the assurance level provided by the certificates issued within the PKI. From the perspective of an entity operating a PKI, the entity has an incentive to ensure that audit practices are robust to prevent trust dilution by accepting into the PKI entities that are untrustworthy. From the perspective of CAs, RAs, and other entities that will be audited, these entities have an interest in making sure that the audit practices are not excessively burdensome or costly.

The PKI should clearly document its assessment requirements and practices. The documentation should also reflect any externally-imposed requirements, such as those arising out of contract or applicable law. Finally, the PKI participants that are subject to an assessment requirement should in fact follow the policies for undergoing compliance assessments as set forth in the PKI's documentation.

D.2.7.1 Frequency

Issue Summary. This section concerns with the frequency with which a compliance audit or other assessment must take place.

Relevant Considerations. Various factors are relevant to determining the frequency of compliance assessments. In jurisdictions where CAs are licensed or regulated, specific audit periods (*e.g.*, annually) may be mandated.[290] In jurisdictions where CAs are not regulated, CAs may have some discretion in determining the frequency of an auditor other assessment. Frequency of the audit of both CAs and RAs could be fixed by the CPs the CA is operating under, or fixed, in some PKI models, by the terms of cross-certification agreements among two or more CAs. Assessment frequency may also be determined by the degree of assurance to be placed upon certificates; higher levels of assurance may call for shorter periods between assessments. For higher assurance levels, it will be important to audit the RAs (at least for identification and authentication, shared secret handling and other assurance requirements) as often as the CA is audited.

Appropriate Requirements and Practices. Assessors should ensure that the PKI's documentation establishes audit frequency consistent with requirements placed on the PKI by law or contract. It is common for CAs to be required to undergo annual audits. In any case, the frequency should reflect the business of the PKI and the

[290] *See, e.g.*, PAG APP 2 ("*Model PKI CA IT Security Guidance Document*, Gov't of Canada (2000) p. 9, *available at* <http://www.cio-dpi.gc.ca/pki-icp/documents/documents_e.asp>, hereinafter "Canadian Security Standards"). Some such jurisdictions also require more frequent auditing upon occurrence of triggering events such as abnormal increases in the system load and important changes to the CPS. *See also* PAG APP 2 (*Certification Authority Guidelines, Electronic Commerce Promotion Council of Japan* (1998) § 3.6.5, *available at* <http://www.ecom.or.jp/qecom/ecom_e/guide/cag.pdf>, hereinafter "Japanese Guidelines").

applications for which the certificates are intended. Moreover, the PKI participants subject to an assessment requirement should undergo assessments at the frequency required or disclosed in the PKI's documentation.

D.2.7.2 Identity and Qualifications of Auditors or Other Assessors

Issue Summary. This section covers the qualifications and training that personnel need in order to be qualified to perform PKI compliance audits or other assessments.

Relevant Considerations. Because public key infrastructures are a combination of complex business, technology and legal elements, the assessment of PKIs requires specialized skill sets. Assessors should:

- Possess adequate technical training with a demonstrated proficiency in public key infrastructure technology; information security tools and techniques, security auditing; and the third-party attestation function;
- Be accredited by a recognized professional organization or association. Membership in the particular organization or association should require the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education; and
- Be organizationally independent of the assessed entity's operation and policy authorities.

The accreditation body of the evaluators serves as a centralized organization to promulgate standards of practice in conducting CA evaluations. It is assumed that among other participants, members of the audit/assessment community will be represented. The accrediting body for assessors should be a professional organization or committee with a reputation among interested parties for high standards of integrity, objectivity, and quality assurance.

Auditors may have various professional credentials that make them qualified to perform information technology audits, such as Certified Information Systems Security Professionals (CISSP) and Certified Information Systems Auditors (CISA). These credentials also qualify persons to perform other kinds of assessments.

Assessors should be aware of any minimum requirements on the qualifications of auditors based on applicable law or contract. For example, a CP may place requirements on CAs to obtain audits performed by auditors having certain qualifications. Assessors should also review the PKI's documentation to determine the PKI's requirements or disclosures relating to assessor qualification. Finally, depending on the kind of assessment, assessors may need to check to determine if the personnel performing compliance audits or other assessments meet the qualification requirements or standards set forth in the PKI's documentation.

Appropriate Requirements and Practices. It is essential that assessors have adequate knowledge of PKI in general, information security principles, the specific vendor products deployed, and the third party attestation function. In some jurisdictions the assessor may be required to possess additional qualifications. The appropriate qualifications should be reflected in the PKI's documentation. In any case, entities subject to an assessment requirement should retain auditors or other assessors that meet the qualifications standards placed on them by contract or applicable law, as well as the PKI's documentation.

D.2.7.3 Assessors' Neutrality

Issue Summary. This section discusses the degree to which auditors or other assessors must be neutral and independent of the entity being audited or otherwise assessed.

Relevant Consideration. The requirement for assessor neutrality will depend on the PKI. Having the personnel performing CA or RA functions assess their own performance is an inherent conflict of interest. In theory, they have an incentive to gloss over or even conceal the deficiencies in their performance.

By contrast, retaining a sophisticated independent auditing firm minimizes such conflicts of interest because under most circumstances, the personnel of the auditing firm will not suffer the consequences of an assessment showing deficiencies in the system. Moreover, these firms have a professional reputation to uphold, and they purport to abide by industry standards for ethics. The difficulty is that hiring such a firm is likely to involve paying the fees of the firm.

For these reasons, the PKI should set independence requirements based on a balancing of cost and trustworthiness. The higher the assurance level of the PKI and its certificates, the greater will be the need for independence of the assessors from the assessed entity and its personnel. In addition to the two extremes of self-assessment and assessment by an independent firm are having assessors within an assessed entity's audit department perform the assessment. Alternatively, some departments or groups may share an audit group with other departments within a larger organization. For example, a state agency having a PKI may want members of the state's office of the auditor general to perform an audit.

Assessors should determine whether any independence requirements pertain to the PKI under applicable law or by contract. They should then ascertain whether PKI participants meet these requirements when they undergo their compliance audit or other assessment.

Appropriate Requirements and Practices. In general, a PKI should require a level of independence of its assessors that is commensurate with the assurance level provided by the PKI and its certificates. An independent party provides greater assurances of trustworthiness than one tied to the assessed entity. The practices of the audited entity should comply with any independence requirements contained within a certificate policy, otherwise required by contract, or imposed by applicable law.

D.2.7.4 Scope of Audit or Other Assessment

Issue Summary. This section describes the topics that an audit or other assessment must cover. It also describes the standards that assessors should consider to establish an appropriate scope of the assessment.

Relevant Consideration. The scope of a compliance audit or other assessment may be defined by the requirements within the CP, and by agreement between the assessor and the authority operating the PKI. Thus, the compliance audit or other assessment may apply to any participant or component in a PKI addressed in the certificate policy. In some cases, the focus may be solely on the CA requirements, and in others it may extend to other participants in the PKI, such as RAs, repositories, subscribers, and relying parties. Frequently, this section lists as a requirement a standard audit methodology, which has associated with it a certain scope of audit or standard control objectives against which the audited entity must be audited. In addition to the requirements of a CP, assessors should ascertain whether applicable law imposes any audit or other assessment scope requirements and whether the PKI's assessment methodology is consistent with these requirements.

Appropriate Requirements and Practices. The scope of the assessment is the review of the design and operational effectiveness of the assessed entity's controls covering a specified period of time. The audit or other assessment should be performed using appropriate criteria covering environmental, key management, and certificate life cycle management controls of the assessed entity. Such an assessment should be intended to assess whether the implemented controls are effective and in accordance with the defined business practices as articulated in one or more Certificate Policies, a Certification Practices Statement, and supported policies and procedures. Refer to PAG APP 4 (PKI Audit Methodology and Guidelines) for a description of the audit process and the specific environmental, key management, and certificate life cycle management controls topic that would typically be audited or otherwise assessed.

The auditor other assessment process typically consists of inquiries of management and operations personnel, observation of processes and controls, testing specific controls procedures, and review of documented policies and procedures including the following:

- A documented certificate policy and the assessor's understanding of the intended CP requirements in the context of the business and operating environment;[291]
- A supporting certification practice statement and a review of the design and operating effectiveness of practices set forth in the CPS to support the certificate policy; and
- Relevant security policy and security procedures.

It may be impractical, however, to list all of the possible topics to include within an audit or other assessment. Accordingly, PKIs often find it useful to refer to an external standard that imports a certain scope of assessment or set of topics to cover. With respect to audits, the two most common standards referred to are:

- The American Institute of Certified Public Accountants' Statement on Auditing Standards (SAS) Number 70, *Reports on the Processing of Transactions by Service Organizations* (SAS 70); and
- The principles and criteria of the American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants *WebTrust Principles and Criteria for Certification Authorities* ("CA Trust").

SAS 70 provides a reporting model where the audited entity is evaluated against control objectives and control procedures, which are specified in the detailed SAS 70 report. SAS 70 provides a flexible reporting framework and does not specify the scope of the audit or the control objectives that should be included. Such control objectives are specified by the audited entity and can be based on industry standards. The SAS 70 report is lengthy, including the auditor's opinion and also describing in detail the overall environment or service, the entity's control objectives and procedures, the test procedures performed by the auditor, and the results of such tests. SAS 70 provides the audited entity with the opportunity to describe its environment and specific control procedures in detail for communication to readers of the report.

CA Trust provides a reporting model where the audited entity is evaluated against the CA Trust Criteria (based on the ANSI X9.79 standard[292]) and its CA business practices (e.g., CPS and CP). With CA Trust, management asserts that it has met the CA Trust criteria during a period of time and the auditor issues a report opining whether management's assertion is fairly stated. The procedures performed by the auditor are the same as would be performed to issue a SAS 70 report; however, the reporting process is streamlined.

In any case, the scope of the assessment should be consistent with requirements set by contract (for example, by a CP) or by applicable law. The PKI should document its requirements and practices relating to the scope of assessment in its documentation. Moreover, the actual practices of entities in seeking and obtaining an assessment should match what

See PAG APP 4 (PKI Audit Methodology and Guidelines) for more detailed guidance on this topic.

D.2.7.5 Actions Taken as a Result of Deficiency

Issue Summary. This section discusses the actions that must be taken if a compliance audit or other assessment shows deficiencies in the performance or the infrastructure of the assessed entity. This section may discuss

[291] If a certificate policy and a certification practice statement are set forth in one combined document, that document will be considered.

[292] *See* PAG APP 9, § 9.1 (Significant Issues Related to PKI and Information Security in Financial Services, § 1.1).

remediation procedures to cure the deficiencies and the penalties that could be imposed on the assessed entity because of the deficiencies or the failure to cure them.

Relevant Considerations. Assessors should review the PKI's documentation to determine what steps are required when a deficiency appears in an audit report or report following another kind of assessment. Assessors should review the documents in light of the incentives of the parties. Entities operating a PKI have an incentive to have aggressive deficiency-curing provisions in their documentation in order to compel entities having deficiencies in their assessments to cure their deficiencies quickly and efficiently. Entities having the deficiencies, however, have an incentive to make sure that the PKI does not impose cure provisions that cause undue burden or expense. Assessors should check to see if there are applicable contractual obligations calling for certain deficiency-curing provisions, such as in a CP. They should also review applicable law to determine if there are any requirement or limitations on deficiency-addressing provisions. Assessors should also determine whether a PKI does, in fact, enforce such provisions in its dealings with subordinate components.

Appropriate Requirements and Practices. The types of appropriate responses to deficiencies will depend on the business model and assurance level of the PKI. The higher the assurance level of the certificates involved and the more sophisticated the PKI, the more likely it is to have a policy concerning the cure of deficiencies and the more likely it is to have provisions permitting the PKI to take swift and firm measures to cause the entity to cure its deficiencies.

Examples listed in RFC 2527 for possible responses to assessment deficiencies include:

- Temporary suspension of operations until the deficiencies are cured;
- Revocation of the certificates issued to the audited entity;
- Changes in personnel;
- Invocation of a "liability policy," which is presumably a reference to the pursuit of remedies through litigation or another dispute resolution mechanism; and
- More frequent compliance audits.

In addition, a PKI may find it helpful to require cooperation with deficiency-curing provisions. Furthermore, the remedy of termination of the audited entity may be helpful for deficiencies that pose an immediate threat to the security of the PKI or where the assessed entity does not cooperate with deficiency-curing measures.

In any case, assessors should ensure that the PKI meets any requirements for deficiency provisions under applicable contracts or laws. Such provisions should be clearly communicated in the PKI's documentation. Moreover, the PKI will want to enforce documented deficiency requirements and practices against subordinate entities within the PKI in accordance with its documentation.

D.2.7.6 Communication of Results

Issue Summary. This section covers issues relating to the communication of the results of an audit or other assessment. It discusses who is to receive a report of the assessment, whether any other parties have the right to view the report, which is responsible for communicating the report, and how the report must be communicated.

Relevant Considerations. Assessors should review the PKI's documentation to determine the PKI's policies relating to the communication of audit results. PKIs have an interest in reviewing the assessment reports of their participants because they will want to ensure the uniformity of trustworthiness throughout the PKI, and the assessment provides perhaps the most important measure of trustworthiness. Where the assessed entity provides services to various entities or customer organizations, it is often necessary to share the results of an assessment

with such entities. In some cases, the assessed entity may wish to broadly share the results of an assessment with subscribers, relying parties, and potential customers. Contracts or applicable laws may also require disclosing the report to other entities.

Appropriate Requirements and Practices. In more sophisticated PKIs and especially those offering higher assurance certificates, an entity operating a PKI may find it useful to require entities undergoing assessments to provide it a copy of the assessment report promptly after completion of the assessment. This will enable the PKI to review the report and determine whether any curative measures are necessary to address the deficiencies and whether any immediate issues pose a threat to the integrity of the PKI. A PKI may also have a marketing incentive to publish certain portions of an assessment report to publicize the trustworthiness of its infrastructure. It may, however, wish to keep some portions of the report confidential, since some discussions of the assessment may compromise its security.

Assessors should ensure that the PKI's documentation and the audit or other assessment results communications provisions comply with requirements set by contract or applicable law. Where licensed or otherwise regulated, for example, a CA may be obliged to indicate to its licensing or accreditation authority the results of any compliance inspection.

The PKI's assessment-reporting requirements and practices should be reflected in clear terms in the PKI's documentation. Lastly, the PKI should ensure that PKI participants undergoing assessments do, in fact, provide assessment reports in accordance with the PKI's documentation.

D.2.8 CONSUMER ISSUES, INFORMATION PRACTICES, PRIVACY

D.2.8.1 Consumer Issues

Issue Summary. This section covers legally mandated consumer protections that may apply to a PKI under a variety of national and local jurisdictions.

Relevant Considerations. As discussed more fully in PAG § C.5, (Consumer Issues and Privacy), consumer protections under foreign or international law, and in various sectors within the U.S., may range from compulsory disclosure requirements, to mandated privacy practices, to outright prohibitions on certain types of contract provisions that would be entirely legal (if not appropriate) in a business-to-business transaction. These protections may either preempt normal PKI contractual provisions or otherwise survive contrary choices of law. Moreover, consumer protection laws of jurisdictions other than the headquarters of the CA or RA may apply to PKI participants, depending on the extent and geographical reach of the services provided by these entities. For instance, the legal requirements of the jurisdiction in which consumer subscribers, relying parties, or other participants may apply to CAs and RAs.

Assessors should review these factors and determine which consumer protection laws apply to the participants within the PKI. They should also review the PKI's documentation to determine if it satisfies the requirements of applicable consumer protection laws, or at least does not contravene applicable limitations on PKI documentation. Finally, assessors should determine whether the PKI's participants do, in fact, comply with requirements established by consumer protection laws consistent with the PKI's documentation.

Appropriate Requirements and Practices. CAs, RAs, and other organizational PKI participants should be aware of, and make adequate provisions for, applicable consumer protections, whether legal and governmental, private-sector based, or media driven, in the potentially large number of jurisdictions in which users may request and use certificates. After becoming aware of the relevant consumer protections under which it may be subject, a CA, RA, or other participant should decide what steps it will take in response to such protections. It may choose to modify some of its business practices so as to comply with a significant number of known consumer protection requirements; it may choose to increase the amount and quality of consumer disclosure offered to

maximize consumer awareness and comprehension of the participant's business practices and PKI in general; it may choose to undergo certification, accreditation, or achieve other publicly know attestations of its sound practices; or it may limit the amount of business that it chooses to do with consumers.

Regardless of the exact steps taken, the services of CAs, RAs, and other PKI participants should comply with applicable consumer protection laws. PKI documentation should reflect these requirements and should not exceed limits placed on contractual provisions or other limits by consumer protection laws. Finally, the practices of CAs, RAs, and other participants should be consistent with their own documentation.

D.2.8.2 Business and Corporate Information Practices

Issue Summary. This section addresses the internal and external information practices of a CA, RA, or other PKI participant holding information concerning subscribers, customers, and business partners. Specifically, this section concerns the information oversight and compliance policies placed on the handling of such information, such as security, procedural, and contractual controls. The information referred to in this section is broader than just the personally identifiable information, which is the basis of the following section on privacy, and may include transaction and other information.

Relevant Considerations. The concept of "business and corporate information practices" refers to the policies and procedures that a business may implement when dealing with customer information. Businesses handle business information internally and may also share information with other business divisions of the same company, or with partners and other companies. The handling of business information may be subject to certain legal requirements and sectoral practices. Unlike the use of personal and sensitive information from consumers, the use of business information by PKI participants will be governed almost exclusively by contractual limitations. PKI participants and their customers and business partners must negotiate and mutually determine how business information may be used. Controls over the handling of business information may include security policies, access controls, and policies on how corporate information may be shared and/or sold with entities outside of the corporation. Also relevant are principles of data relevance and duration of storage.

Assessors should determine whether a PKI operates within an environment where business or legal constraints require policies or procedures for the handling of business information. These constraints may exist by virtue of applicable law, such as laws relating to the confidentiality of banking transactions, or by virtue of contractual limitations, such as those imposed by nondisclosure agreements. Assessors should review the PKI's documentation to determine how it responds to the applicable business and legal constraints. Lastly, assessors should determine whether PKI participants do, in fact, abide by requirements for business information handling and control imposed by applicable law or contract in a way that is consistent with the PKI's documentation.

Appropriate Requirements and Practices. PKI participants should adopt business information policies and practices that meet any requirements established by contract or applicable law. They also have an incentive to establish procedures that have the appearance of being fair in the context of the specific sector in which they do business. To establish fair and best practice information practices, PKI participants may wish to look to underlying principles described in the Electronic Commerce and Consumer Protection Group's *Guidelines for Merchant-to-Consumer Transactions* and the Better Business Bureau's *Code of Online Business Practices*.[293] The PKI's documentation should reflect the business information policies and practices appropriate for the sector and consistent with external constraints. Finally, the business information handling practices of participants in the PKI should match the PKI's documentation.

[293] *See supra* note 134.

D.2.8.3 Privacy

Issue Summary. This section relates to the handling and treatment of personally identifiable information ("PII")[294] obtained from individuals in connection with the services of a PKI's participants. This section may also establish a requirement for PKI participants to have a privacy policy, set a requirement to post the privacy policy on a web site or otherwise, and cover the general areas to be addressed in a privacy policy, and place an obligation on PKI participants to follow the terms of a posted privacy statement.

Relevant Considerations. The most common example of individuals providing PII to other PKI participants is the process in which certificate applicants submit PII to a CA or RA as part of the certificate application process. It is possible, however, for other certification services to involve the transfer of PII. Moreover, PKI participants may use or disclose PII to third parties in order to provide services associated with issuing a certificate. In addition, the certificate itself may contain, and thus disclose, PII.

A variety of legal obligations may be imposed on a PKI participant that collects, uses, and/or discloses PII. These obligations are discussed in more detail in PAG § C.5 (Consumer Issues and Privacy). At the current time, if general or industry-specific legislative provisions do not apply (e.g., the Gramm-Leach-Bliley Act as to financial institutions, the Privacy Act of 1974 as to federal governmental entities, the EU Data Privacy Directive, or COPPA as to the collection of personal data from children), then there is no express statutory requirement for an organization or its website, including any domestic PKI participant or web site, to have, publish, or follow a privacy policy.

Nonetheless, there are a variety of non-legal considerations, such as reasonable public expectations and standards of independent accrediting and certifying bodies that affect the collection, use, and disclosure of PII. Disregarding these expectations and standards may substantially harm the "trust" reposed in a PKI participant. The failure of an interactive website to post any privacy policy may begin to attract negative attention. The practice of posting a privacy notice has recently become more customary on many consumer-oriented sites. In fact, some organizations provide and license trustmarks related to privacy practices, and PKI participants may wish to consider whether such services provide value for consumers and others evaluating their services. Companies that decide to post an online privacy policy, whether legally mandated or for non-legal considerations, should be aware that within the U.S. the terms of the policy can be legally held against the company if the company deviates from its stated terms. [295]

In light of the attention that the privacy issue has garnered from the FTC and other regulatory agencies, assessors will likely want to review the use of consumer PII by PKI participants, especially if they make use of the PII for any purpose other than providing certification services. Assessors considering the sufficiency of the privacy practices of PKI participants should first determine which privacy laws apply to the PKI and what the laws require. They should also account for any contractual covenants requiring certain privacy practices. In addition, assessors should determine whether PKI participants have privacy policies and other documentation of their privacy practices and whether the documentation adequately embodies the requirements imposed by law or contract. Finally, assessors should determine whether or not PKI participants abide by the privacy policies and other obligations that they purport to follow.

Appropriate Requirements and Practices. In drafting a privacy policy, companies subject to general or industry-specific legislative provisions (e.g., the Gramm-Leach-Bliley Act as to financial institutions, the Privacy Act of 1974 as to federal governmental entities, HIPAA as to health care information, the EU Data Privacy Directive, or COPPA as to the collection of personal data from children) will need to comply with the requirements under the applicable laws. Companies not subject to general or industry-specific privacy

[294] *See* discussion *supra* PAG § C.5.2 (Consumer Issues and Privacy); *see also* PAG § APP 1.1 (Glossary) definition of "personally identifiable information".

[295] The FTC will acquire jurisdiction over any false advertising or deceptive trade practices that result from the failure of a company to follow its published privacy policy.

legislation should consider the fair information practice principles that have been promulgated by the FTC, as discussed in PAG § C.5 (Consumer Issues and Privacy), as well as self-regulatory privacy principles, such as those of the Online Privacy Alliance. In any case, companies posting privacy policies must be aware of the enforcement authority of the FTC or other appropriate regulatory body against misleading, deceptive or unfair trade practices, which may result in civil fines and potentially harmful negative publicity. A company will be considered to have committed an unfair or deceptive act or practice if it posts a privacy notice or privacy policy on its website, and has actual practices that materially vary from its privacy notice or privacy policy. In addition, websites doing business with EU citizens will need to satisfy the requirements of the EU Data Privacy Directive, as discussed in PAG § C.5. One way to satisfy those requirements would be to self-certify to the Safe Harbor.[296]

In addition to applicable law, PKI participants should follow any applicable contractual requirements to establish privacy policies, include within such policies any required content, respect the privacy policies of business partners, customers and vendors, and follow certain information-handling practices. The privacy policies and other PKI documentation should reflect applicable privacy laws and contractual constraints. Finally, PKI participants should follow their own privacy policies and other PKI documentation when performing their services.

D.2.9 INTELLECTUAL PROPERTY RIGHTS

Issue Summary. This section covers the assertion by PKI participants of intellectual property (IP) rights over various aspects of the PKI, such as Certificates, CPs, CPSs, names, public and private keys, and databases. Protection can potentially be asserted under patent, copyright, trademark, trade secret, and unfair competition laws.

Relevant Considerations.

Basic Intellectual Property Concepts

Patent law protects new, unobvious, and useful inventions. Recent court decisions have broadened the scope of patent protection to methods of doing business as well as processes that develop certain end products, where the end product is protected as a result of use of the patented process. Copyright law protects original works of authorship embodied in a tangible medium of expression. To be copyrightable, however, the work cannot be purely functional. A relevant consideration in the protection of copyright is copyright misuse. For example, anti-competitive clauses in licenses such as restrictions on the development of competing products or software may be instances of copyright misuse[297]. To obtain patent protection, one needs to file a patent application with the Patent and Trademark Office and obtain a patent from it. Copyright, however, arises automatically when an author creates a work.

Trademark law establishes exclusive rights to use marks that distinguish one manufacturer, merchant, or service provider's goods from those of others. A trademark is usually a word or group of words but may consist of any device that serves to distinguish good or services, such as designs and patterns.

The Uniform Trade Secrets Act, which has now been adopted in 40 states, defines a trade secret as:
"Information, including a formula, pattern, compilation, program, device, method, technique or process, that:
"(i) derives independent economic value, actual or potential, from not being generally known to, in not readily ascertainable by proper means by other persons who can obtain economic value from its disclosure and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

[296] The Safe Harbor is the accommodation reached between the U.S. and the EU to provide a finding of adequacy of data practices under the EU Data Protection Directive, *available at* <http://www.ita.doc.gov/ecom>.

[297] See Lasercomb America, Inc. v. Reynolds, 911 F.2d 970 (4th Cir. 1990).

Possible IP Concerns Relating to PKI

The establishment of a PKI raises many possible IP concerns, the full extent of which are beyond the scope of the PAG. If the reader requires more detailed information concerning IP issues, the reader may want to consult the various primary and secondary sources of law in the IP field. This section of the PAG will, however, raise the most important PKI-related IP considerations at a general level in order to raise issues, of which the reader may not be aware, and facilitate further inquiry.

The use of PKI may raise IP issues relating to both the infringement of a PKI on the intellectual property rights of others and the infringement by others on the intellectual property rights of PKI participants. In the area of patent, for instance, a PKI or a PKI vendor may produce hardware or software products to perform PKI functions that are covered by patents. Moreover, the services of a PKI may involve the use of methods or procedures that are patented. On the other hand, PKI participants and PKI vendors may have obtained patent protection over their own products and methods. If others use these products and methods without license, they may be liable to these PKI participants or vendors for patent infringement.

The copyright area also raises issues. Copyright laws protect the expression of ideas within PKI documentation, such as CPs and CPSs. These documents are potentially copyrightable works of authorship, just like any other document, and PKI documentation may assert copyright protection, including through a copyright notice. Therefore, PKI participants commonly watch to make sure that they do not infringe upon the copyright rights of others when they create PKI documentation, and determine whether or not others are infringing upon the copyrights on their documents.

Copyright law is also relevant if a PKI wants to prevent unauthorized copying of certificates, the public keys within certificates, and information in repositories, directories, and other PKI-related databases. The copying of certificates and public keys within them are relevant because organizations copying certificates or repository information can potentially compete against the CA or repository providing such information by copying the information without cost using "data mining" techniques and reselling it to others. If the data miner sets up his own repository as an alternate site for distributing a CA's signed Certificates, then the CA might want to assert an infringement claim to prevent the copying and distribution of Certificates by such a third party.[298]

The copyrightability of certificates has not yet been determined in a decided case and is an open issue.[299] Nonetheless, it may be possible for a CA or repository service provider to obtain copyright protection for its

[298] Note, however, that the ordinary copying and distribution of certificates by relying parties may be permitted under either the fair use or implied license doctrines.

[299] Copyright protection for individual certificates is a difficult question and requires further analysis. In *Feist Publications, Inc. v. Rural Telephone Svc. Co.*, 499 U.S. 340 (1991), the court stated that the original sequencing of unprotectable data itself may be protectable under the compilation doctrine. *Feist* holds that only the original efforts relating to selection, coordination, or arrangement in factual compilations are protectable. To obtain protection, the selection, coordination and arrangement of compilations of factual data must possess at least some minimal degree of creativity. However, to the extent that such sequencing is obvious (e.g., alphabetical telephone listings as in *Feist*), or purely functional (i.e., not copyrightable under Section 102 of the US Copyright Act), or dictated by "externalities" such as industry standard specification (e.g., the X.509 specification), such sequencing would not be protectable under copyright law.

Even though the issue of originality is a low threshold requirement, as formatted documents that contain factual data organized into predefined formatted fields, it is not clear whether certificates are protected by copyright. In *MITEL, Inc. v. IQTEL, Inc.*, 124 F.3d 1366, 1373, (10th Cir. 1997), the plaintiff's random selection of numbers to represent command codes did not have the required originality and was denied copyright protection. Nonetheless, if the CA uses a creative or proprietary technique for generating certain certificate information, it is arguable that this technique creates a basis for claiming originality and copyright protectability. Another relevant question is whether the CA uses a sequencing of fields in the certificate that is not dictated by external standards (e.g., the sequencing defined by the X.509 specification). Even if the CA does use a sequencing of fields that is not dictated by external standards, however, copyrightability may be sustained if there is a sufficient number of

compilation of certificates or other repository information. As with the copyrightability of certificates, however, the courts have not yet decided whether repository information is protectable.[300] Public and private keys likely are simply factual data, and as such, are less likely to qualify for copyright protection, although here again, there are no decided cases on point.

Nonetheless, at least private keys may be protectable under trade secret laws. A trade secret is any information that (1) is secret, and (2) has economic value by virtue of the fact that it is kept secret. Furthermore, there may be a basis for claiming trade secret protection for the methods and techniques used to generate the key pair. In any event a private key should be treated as the sole property of the legitimate holder of the corresponding public key, as identified in the certificate.[301]

Trademark law becomes relevant in connection with naming. Names used by various entities within the distinguished names in issuer and subject fields within certificates may be the subject of protection under trademark law. Assessors should determine whether PKI documentation sets policies relating to disputes over subject names that arise between a subscriber that obtained a certificate issued with a certain subject name and a third party claiming to have exclusive rights to use the name in commerce. Documentation may also include or

---

alternative ways to accomplish the same result. A third way that a CA can claim copyright protection is if the CA employs extensions per the X.509 specification that includes the original information and/or sequencing of information.

[300] In *Feist*, the U.S. Supreme Court discredited the "sweat of the brow" doctrine, which protected databases based on the effort expended by the data compiler. Under *Feist*, databases of facts are not protectable unless the databases contain originality in the selection, coordination, or arrangement of the facts. Consequently, there is a current debate whether Congress should grant a "sui generis" protection to databases in order to provide investment incentives for database developers. In this regard, the U.S. House of Representatives passed the Antipiracy Act, *see* PAG § APP 2 (*Collections of Information Antipiracy Act*, H.R. 2652, 105th Cong. (19 May 1998), hereinafter "U.S. Antipiracy Act"). This bill creates a property right in databases of information, even if including only public domain information. The bill was referred to the Senate Judiciary Committee, but was not enacted by the Senate. The European Union adopted a directive, effective January 1, 1998, that grants a *sui generis* property right in the contents of databases. The directive protects against unauthorized extraction or reutilization of all or a substantial part of the contents of a database for a period of 15 years.

The *Feist* ruling in the US is not inconsistent with database compilation protection for the CA's entire database of Certificates, but the CA would need to show original structure, sequence, and organization factors. Certainly that protection will expand if the US and other countries follow the lead of the European Data Protection Directive and the protection it grants for collections of factual data.

Hence, any analysis of a CA's rights in any database of Certificates it maintains should take into consideration the following elements:

Does the CA database of Certificates include original selection, coordination, or arrangement of data so as to qualify for U.S. copyright protection?

Can the CA invoke the protections of foreign jurisdictions (e.g., the European Union) to prevent improper exploitation of its database?

Assessors should also consider whether the misappropriation doctrine allows the CA to protect against the taking of its database contents by competitors.

[301] Private keys may also be protectable under state law on other theories. *See, e.g.*, PAG APP 2 (*Electronic Commerce Security Act*, 5 ILL. COMP. STAT. 175/1-101, § 10-140 (enacted Aug. 1998) hereinafter "Illinois Security Act"), (discussing "unauthorized use of signature device," which makes it a criminal offense to "knowingly or intentionally access, copy, or otherwise obtain possession of or recreate the signature device of another person without authorization").

No person shall knowingly or intentionally:

access, copy, or otherwise obtain possession of (or recreate) the private key of another person; or

alter, disclose, or use the private key of another person;

without authorization, or in excess of lawful authorization for the purpose of creating, or allowing or causing another person to create, an unauthorized digital signature using such private key.

disclaim any transfer or intellectual property rights or licenses in names deemed to arise out of the process of applying for a certificate.

Considerations in Assessments

Assessors should review the PKI's documentation and its coverage of intellectual property issues. In assessing the intellectual property provisions of the documentation, assessors should determine whether the assertions of protection are supportable under applicable IP law and consistent with any requirements or limitations imposed by contract. Assessors representing CAs or RAs may want to ensure that they assert and confirm all available protections under the applicable IP laws. By contrast, other assessors may have an interest in ensuring that CAs and RAs are not overreaching in terms of the assertions in the PKI documentation. Likewise, an assessment should include an analysis of the scope of indemnities for infringement by the PKI technology used of the IP rights of others. The provider of the technology has an incentive to minimize and constrain such indemnities, while the party procuring and using such technology has an incentive to broaden such indemnities.

A review of the documentation should also focus on whether the IP-related rights and obligations are clearly disclosed and stated. Moreover, the PKI agreements may be in the form of a license or contain discrete IP licenses. If so, assessors should determine what rights, restrictions, and liabilities are addressed in such licenses. The rights in such agreements may include an entitlement to use, copy, and distribute certificates.

Appropriate Requirements and Practices. The need or desirability for provisions relating to intellectual property protections over certificates and keys will depend on the business model of the PKI. CAs may want to analyze whether asserting such rights are helpful accomplishing other purposes, such as having a claim to assert against people who use certificates and keys for unauthorized purposes like involuntary certification. Moreover, CAs may wish to employ agreements addressing data mining and involuntary certification concerns. To underscore any claim of ownership over certificates or certificate content, CAs may want to populate their certificates with notices of copyright or other ownership protections.

Aside from certificates and keys, it is common to assert intellectual property ownership over a CP or CPS. To the extent that these are original works of authorship, copyright law protects them. It is probably worth emphasizing this ownership via copyright notices and statements within these documents that IP rights in them are preserved.

With respect to names, it may be helpful for PKI documentation to set policy relating to the use of names. For instance, a PKI may wish to avoid disputes among Subscribers and third parties by stating that names appearing in the subject fields of end-user subscriber certificates are the property of their respective owners and that the CA is not responsible for adjudicating disputes among rival claimants to IP rights over such names. A CA may also wish to assert trademark rights over names that appear in issuer fields within the certificates it issues.

Users of the services of CAs, RAs, and repositories may want to seek an indemnity for losses caused by service providers' infringement upon the intellectual property rights of others. The providers of such services, by contrast, have an interest in limiting the scope of such indemnities to a reasonable and appropriate scope.

With all of the matters possibly covered by IP rights, PKIs should utilize agreements that clearly allocate IP rights and ensure that the relevant PKI participants are bound by such agreements. Policies clearly delineate circumstances in which the use, copying, modification, and distribution of various aspects of the PKI are permitted. These agreements and other documentation should be consistent with applicable law, and assessors should ensure that PKI documentation is not overreaching in its assertion of IP protection.

D.3 Initial Validation of Identity, Authority, and/or Other Attributes

In most instances[302], the ultimate purpose of certificates is to bind a public key to one or more attributes of a person (natural or legal). Most often, the relevant attribute being bound to a public key is a person's identity. In some PKIs, however, a public key is bound to the authority to act in certain circumstances, in addition to or instead of identity. Other attributes may be bound as well (such as role). This section describes the names included within certificates and the methods by which identity, authority, or other attributes are validated as a precondition of issuing a certificate binding a public key to such attributes. Note that, unless otherwise specified, certificates in this section refer to identity certificates.

D.3.1 NAME FORMS

Issue Summary. This section states the requirements and disclosures concerning the names of certificate subjects that appear in their certificates. The section specifies what kinds of subject names are acceptable, whether pseudonyms are permitted, how specific naming conventions should be understood, and whether names must be unique within a given domain.

Relevant Considerations. Name form requirements and disclosures relate to the names that appear in the subject field and (if used) the alternative subject name field (subjectAltName).[303] The subject field contains the name of the subject of the certificate (i.e., the subscriber). The alternative subject name is sometimes used to contain a name that can be used to identify the subject other than the subject name, which appears in the subject field. For example, if the subject name contains an individual's first name and last name, a CA may wish to place an identifying number within the subjectAltName field that may be a more effective way for a server to look up and confirm the identity of the subject of the certificate. In most cases, however, this section focuses on acceptable name forms for the subject field.

Assessors should consider the naming provisions of the CP, CPS, or document they are reviewing in the context of the technical limitations and requirements facing the PKI. If software conventions require certain naming structures, assessors should ensure that the naming conventions used by the PKI meet these requirements and fall within the limitations. Naming requirements may be reflected in a CP, and assessors should determine if the PKI's naming practices meet these CP requirements. In various contexts, these requirements may promote uniformity and enable interoperation, as well as automated processing.

Appropriate Requirements and Practices. Certificates convey information about the persons they identify. Therefore, a common convention for identifying those entities should be selected. RFC 3039, Qualified Certificates Profile, provides a useful guideline for this purpose.[304] A PKI should have clearly stated requirements concerning how names should be constructed and placed within the subject field of certificates. If a PKI uses the subjectAltName field, the PKI should identify the information that populates that field and the rules relating to its use.

It is important to remember that the concept of identity may involve more than just the name contained in the certificate. In an X.509 certificate, moreover, a certificate may provide assurances about a suite of attributes about a person bound to a specific public key. Accordingly, the requirements of the PKI related to other attributes about a subscriber must be considered.

[302] The obvious exception is anonymous and pseudononymous certificates, discussed in PAG § D.3.1.2 (Pseudonyms and Anonymity), *infra*.

[303] For example, a subject name might be John Smith, and the subjectAltname might be "5FMwAOMzgJJ0ACQ."

[304] *Available at* <http://www.ietf.org/rfc/rfc3039.txt>.

D.3.1.1 Types of names

Issue Summary. This section specifies how subject names are expressed within certificates to be issued by a CA.

Relevant Considerations. Certificates can contain a variety of name forms for different applications and purposes. Some examples of possible name types include X.500 distinguished names, e-mail addresses, IP addresses,[305] GUIDs or UUIDs,[306] and URLs.[307] X.500 names are intended to identify a particular person or device within a domain unambiguously. *See* PAG § D.3.1.4, (Uniqueness of Names), *infra*. Since there are many people who share the same name, distinguished names attempt to add additional information to distinguish one person possessing a given name from another with the same name.

If a PKI uses X.500 distinguished names, it may state requirements or disclose the different components that must be or are used to compose distinguished names. Common examples of distinguished name components include fields for the "common name" of the subject (such as first name and last name of a natural person), the "organization" to which the subject belongs (like a corporation), and the "organizational unit" (such as a department within a corporation). A PKI may also have more detailed rules for use of these fields. For example, a PKI may require that a common name field include first name, middle initial, and last name. Or it may require only first name and last name.

Requirements for constructing distinguished names may also include requirements to place information within naming fields that are not, under a common sense or technical view, part of a name itself. For example, some PKIs may place disclaimers and other legal text in organizational unit fields within a distinguished name. Although the naming fields were not designed for the expression of legal text, a PKI may find it helpful to use a naming field for that purpose. One reason for such usage is that commonly used client software able to display certificate content does not always permit users to view the fields that could be used for legal text, especially older applications. The naming fields may be some of only a small number of fields that a user could see within a certificate. To the extent placing information in naming fields may be the only way to communicate information in certificate content to the users of certain software, a PKI's choice might be to use naming fields for this non-naming purpose. If not, a possible risk to the CA exists where the terms and conditions the CA may wish to place on relying parties are found to be unenforceable as a result of the failure to provide adequate notice. Other mechanisms, however, such as the PKI Disclosure Statement discussed in PAG APP 6, can minimize the risk.

Assessors should review this section to determine what types of names are required or used by the PKI. Assessors should also determine whether such names are appropriate for the applications for which certificates will be used. Finally, assessors should determine if the types of names used by a PKI are consistent with obligations placed on the PKI by contract, policy, or applicable law.

Appropriate Requirements and Practices. A PKI should have clearly stated requirements or disclosures relating to the types of names required or used. Clear guidelines will enable CAs wishing to comply with requirements to populate name fields with the proper information.

[305] An Internet Protocol address (IP address) is a method of identifying devices connected to a network (i.e., the Internet and proxied sub-networks connected to the Internet). IP addresses are 32-bit numbers expressed as four 8-bit sequences in dotted-decimal notation (32 ones and zeros, divided into four eight-number sequences and separated by periods, and then converted to decimal notation, i.e., numbers 0-9, which when converted result in a number from 0 to 255). For example, 00010101.00001101.10000000.10111111 becomes 21.13.128.191.

[306] Globally Unique Identifiers (GUIDs), also known as Universally Unique Identifiers (UUIDs), are 128-bit unique numbers calculated using an algorithm, Coordinated Universal Time (UTC) and the originator's IP address to ensure uniqueness.

[307] *See* RFC 2527, *supra* note 193 at 41 n. 7.

In choosing which name forms are appropriate for certain applications, a PKI should consider the limitations placed on naming by the applications processing the certificates and the need for interoperability. The choice of one type of name versus another will generally depend on intended purpose and applications for the certificates. For widely-deployed PKIs, an X.500 distinguished name in most instances provides the most effective name form. Its ability to identify a person or device unambiguously within a name space is useful when the purpose of a certificate is to provide assurances that the public key within the certificate is tied to a particular person's identity. If a PKI requires that certain legal information should be placed within naming fields, the PKI's documentation should clearly state what kind of information a CA must place in certificates.

D.3.1.2 Pseudonyms and Anonymity

Issue Summary. This section addresses the question of whether pseudonyms or aliases[308] can be used within the subject name fields within a certificate or whether a certificate may be issued for the purpose of providing total anonymity. The underlying issue is whether certificates within the PKI are intended to support anonymous, pseudonymous, or attributable transactions.

Relevant Considerations. In most PKIs, the names within certificates are intended to be real names corresponding to real-world people. For privacy purposes, however, some people may wish to conduct business or other transactions anonymously or pseudonymously or the PKI may require this mode of operation. To protect privacy, the PKI or individual subscribers may not wish the actual names of the subscribers to appear in certificates that are used for conducting transactions. Rather, a pseudonym or alias may be used as the name within a certificate. Such a desire to use a pseudonym or alias by an individual subscriber may or may not be approved by the CA.

In the European Directive on Electronic Signatures[309] the concept of a pseudonym is introduced. This Directive enables digital signatures signed under a pseudonym to be given legal effect even though the relying party may not be able to identify the signatory without recourse to the CA.

Assessors should review a PKI's documentation to determine whether or not pseudonyms and aliases are permitted. If individuals are permitted to select a pseudonym (in contrast to having the CA assign it), assessors should check the PKI's requirements for, or limits on, the way a certificate applicant can choose a pseudonym or alias. An assessor should check to see if the PKI's requirements or disclosures are consistent with the requirements placed on the PKI by contract or applicable law.

Appropriate Requirements and Practices. PKIs should follow any requirements imposed by contract or applicable law to accept pseudonyms or aliases for the purpose of facilitating anonymous transactions. PKIs specially designed to facilitate anonymous or pseudonymous transactions will likely find it helpful to permit pseudonyms and aliases, subject to clear limitations.

Other than in these contexts and depending on the assurance levels of the certificates, most PKIs will probably find it appropriate to prohibit the use of pseudonyms and aliases. Certificates issued within these PKIs will likely be intended to provide assurances that a public key is bound to a real person having a real name. In the transactional context, a relying party will want to know the real-world identity of the subscriber in order to know whom the relying party should provide the goods or services and, if necessary, to bring a lawsuit against the subscriber. Permitting pseudonyms would prevent people from obtaining the binding between a public key and a real-world identity, possibly permit the subscriber to avoid identification for the purpose of bringing suit, and thereby frustrate the purposes of a typical identity certificate. If pseudonyms and aliases are prohibited by contract or applicable law for these reasons, the PKI's documentation should reflects this prohibition.

[308] Deep Throat was the alias for Washington Post reporter Bob Woodward's super source during the paper's coverage of the Watergate scandal in 1974 and is one of the best-kept secrets in the history of American journalism and politics.

[309] *See* EU Signature Directive, *supra* note 5.

D.3.1.3 Rules for interpreting various name forms

Issue Summary. This section addresses possible semantics that a PKI may require or use for understanding what certain name forms mean. A name may not be meaningful at first glance without knowing what the name means or how it was constructed. This section addresses special rules to make facially meaningless names understandable.

Relevant Considerations. A PKI may decide to use names that are immediately meaningful and understandable to persons viewing the certificate at first glance. For example, a PKI requiring the use of X.500 distinguished names may require that the common name field of the distinguished name contain the first and last name of the individual subscriber. Anyone looking at that name within the certificate could immediately understand what the name signifies.

Other PKIs, however, may use name forms that do not have such an apparent meaning. For example, if a name field contains a code such as "HA-11359," the field does not provide a person unfamiliar with the coding system with any meaningful information about the certificate's subject's name. Rules for interpreting this name might be, for instance, that the first letter of the code signifies the location of the subscriber, where "H" might mean "headquarters." Another rule might be that the second letter indicates the department of the subscriber, and in this example "A" might mean "accounting." Another rule might be that the number following the hyphen indicates the employee number of the subscriber. Knowing these three rules, the name above becomes clear; the subject of the certificate is located at headquarters, works within the accounting department, and is employee number 11359.

Assessors should determine whether any special name forms requiring interpretive rules are necessary. If so, assessors should check the PKI's documentation to determine if rules for interpreting these name forms are disclosed. Finally, assessors should ascertain whether contractual requirements or requirements imposed by law necessitate the use of special name forms or the disclosure of the rules to understand those name forms.

Appropriate Requirements and Practices. If a PKI uses special name forms not understandable on their face for the purpose of a specific application, the rules for interpretation should be provided in the CP, CPS, or other PKI documents. Also, if special name forms are required by contract or applicable law, this section should state how these names are to be understood. In many instances, however, special name forms are unnecessary, since the PKI may require the use of names that are understandable on their face. In that case, it may not be necessary for a PKI to state anything in this section.

D.3.1.4 Uniqueness of names

Issue Summary. This section concerns whether or not the names of certificate subjects must be unique within a PKI's domain. In other words, does the PKI address the possibility that there may be two persons with the same name applying for certificates?

Relevant Considerations. Many PKIs intend to provide services to enable subscribers and relying party to conduct transactions where a communication can be bound to a specific person. This is likely to be true in all but the most rudimentary PKIs. Uniqueness is necessary for proper system and relying party identification of users upon certificate presentation. Relying parties want to avoid the possibility of a subscriber attempting to repudiate the communication by claiming the certificate and the communication are actually those of another subscriber within the PKI's domain having the identical name. Some examples of domain-wide unique identifiers are e-mail addresses (the user name jsmith cannot be used to identify more than one user; there can only be one jsmith@company.com) and GUIDs/UUIDs (introduced above in PAG § D.3.1.1 (Types of Names)).[310] Assessors should review the PKI's CP, CPS, or other documents to ascertain whether the PKI

[310] GUIDs/UUIDs may be used instead of user names and e-mail addresses where a PKI requires temporal uniqueness of names. For example, the Distinguished Name concept makes is relatively easy to ensure that a PKI does not duplicate names

requires unique names or not. They should also determine whether the PKI's statements about uniqueness are appropriate in light of the applications for which the certificates will be used. Finally, they should find out whether obligations imposed by contract or applicable law bear on whether or not names must be unique.

Appropriate Requirements and Practices. If a PKI is intended to provide assurances that transactions and communications are bound to particular individuals, user names within a PKI should generally be unique. Rules for uniqueness and valid exceptions should be specified in the CP, CPS, or other appropriate documents. For example, a CP may state "a GUID shall be associated with the Subscriber's Common Name and Subscriber Account when an applicant registers his or her information with the CA and obtains a certificate. A GUID shall remain associated with the Subscriber as long as he or she renews the certificate prior to expiration or revocation."

D.3.2 PROCESSING OF A CERTIFICATE REQUEST

D.3.2.1 Recognition, authentication, and Role of Trademarks

Issue Summary. This section covers rules relating to a certificate applicant's use of a name in a certificate application that may infringe upon the rights of the holder of a trademark or service mark (i.e., whether the CA will issue a certificate with the name requested by an applicant in the subject field of a certificate). Also, this section addresses whether or not a CA or RA will resolve any conflicts among actual or potential subscribers or certificate applicants relating to the use of names, and in particular, names that also constitute trademarks and service marks. If a CA or RA will resolve such conflicts, this section addresses how those conflicts are resolved.

Relevant Considerations. Organizational certificates may contain names, trade names, or other words that serve as trademarks or service marks. These names or other words appear in the name fields of a certificate, either the subject name field or the alternative subject name field. In some instances, there may be conflicts as to whether or not names or other words to be placed in a subject field of a certificate infringe upon the trademark rights of third parties.

A party whose rights may be infringed in this way may come to have actual knowledge of a certificate application, but more likely, such a party will discover that the disputed words appear in a certificate issued to another party. Such a discovery may be part of a larger dispute relating to the use of such names or other words on the subscriber's web site, packaging, or other collateral. When a dispute about the name within a certificate occurs, an aggrieved party may assert a claim and contend that its alleged mark is infringed by the words within the certificate's subject field. The aggrieved party may seek to enjoin the certificate applicant or enjoin the subscriber from using certificates containing the alleged mark. The aggrieved party may even seek relief from the CA, such as the rejection of a certificate application or revocation of the certificate containing the alleged mark.

To address this latter concern, a PKI may have specific restrictions relating to the use of names in a certificate application to prevent trademark infringement. A PKI may also have a policy concerning what procedures should be followed in the event that the right of a subscriber to use a name or words within a certificate is challenged by the holder of a mark who claims that the certificate content infringes upon its mark.[311]

Assessors should review the PKI's documentation to determine whether it addresses the selection of names that may infringe upon the rights of a trademark or service mark holder. Assessors should also determine whether or

at any given time, but a C=US, O=US Government, OU=DoD, CN=JSmith might come and go, then another JSmith enter into the PKI, and there could be confusion as to which JSmith is associated with the certificate.

[311] *Available at* <http://www.icann.org/udrp/udrp.htm>.

not the PKI has a dispute resolution policy in case there is a conflict. Assessors should further determine whether any such policy is appropriate under the PKI's circumstances.

Appropriate Requirements and Practices. In constructing a policy to deal with conflicts over the names appearing in certificates, PKIs will generally want to follow the path that minimizes their own liability toward mark holders and minimizes their chances of becoming embroiled in a litigation as a party to the dispute over a mark in which they have no real interest. At the same time, PKIs will not want to be liable to their customers for rejecting a certificate application or revoking a certificate based on an actual or perceived conflict over a mark.

In trying to balance these interests, a PKI may find it helpful to minimize risk by, at a minimum, imposing terms in its documentation prohibiting certificate applicants from infringing the rights of others under the trademark laws. If the responsibility is placed on certificate applicants (possibly coupled with an indemnity for liability of the CA caused by any infringement), the CA or RA may be able to shift liability to the certificate applicant. At the same time, resting the responsibility to avoid infringement with the certificate applicant or subscriber may be a defense against a contract claim by the certificate applicant or subscriber based on a rejection of a certificate application or revocation of the certificate. To avoid such a claim, the PKI may also want to add an acknowledgement that a CA or RA, within its sole discretion, is entitled to reject a certificate application or revoke a certificate to avoid infringement liability.

PKIs may or may not want to go further and have a policy concerning resolving conflicting claims to the right to use a name. A CA or RA invoking such a policy may find itself embroiled in an expensive dispute over the name, when it has no real interest one way or the other in who ends up with the right to use the name. On the other hand, the PKI may be able to adopt a suspension mechanism to place a certificate application or certificate in abeyance until the rights are sorted out. Before adopting such a policy, a PKI should have intellectual property counsel provide a careful review of it, so as to strike a balance that will minimize the burden, expense, and liability placed on the CA or RA. Also, any such policies should be consistent with external requirements placed on the PKI, for example by restrictions within a CP on the ability of a CA or RA to resolve trademark disputes.

D.3.2.2 Method to prove possession of private key

Issue Summary. The purpose of this section is to specify how certificate applicants must demonstrate that they have possession and control of the private key corresponding to the public key to be placed in a certificate issued to the certificate applicant.

Relevant Considerations. Some commercial software includes a mechanism by which a certificate applicant can prove to a CA that the certificate applicant possesses the private key that corresponds to the public key to be listed in a certificate issued to the certificate applicant. Requiring such proof diminishes the likelihood that a subscriber will repudiate transactions signed with the private key corresponding to the public key in the certificate, and the likelihood of disputes arising from situations such as:

- the inability to verify the party's signature,
- the inability to properly encrypt/decrypt information, or
- a party obtaining a certificate for someone else's public key.

PKCS #10 and the Internet's Certificate Request Message Format (PKIX –CRMF)[312] are examples of commonly used protocols that support proof of possession of a private key. Some software uses proprietary

[312] *See* PAG APP 2 (*Internet X.509 Public Key Infrastructure, Certificate Request Message Format*, RFC 2511, Internet Engineering Task Force (IETF) (Mar. 1999), *available at* <http://www.ietf.org/rfc/rfc2511.txt>, hereinafter "RFC 2511").

methods of proving possession of a private key. Other PKIs, depending on the business model, may not require a technical means of proving possession of a private key, or may require no such proof at all.

Assessors should determine from the PKI's documentation whether there is an express requirement that a certificate applicant use a specific method of proving possession of a private key as a condition of issuing a certificate containing the public key corresponding to the private key. If so, they should determine whether or not the method required or used is appropriate in light of the risk of issuing a certificate in error and the assurance level provided by the certificates and whether any applicable requirements compel the use of certain methods.

Appropriate Requirements and Practices. It is generally appropriate for a PKI to require that certificate applicants prove that they possess the private key corresponding to the public key to be placed in the certificate by performing a cryptographic operation with the private key, which the CA can verify using the public key to be certified. PKCS #10 is a common protocol by which a certificate applicant can provide such proof. Most PKIs will want to require proof of private key possession by requiring the use of PKCS #10 or a cryptographically equivalent demonstration, depending on which protocols are supported by the software used.

In any case, the method that the PKI chooses for proving possession of a private key should be appropriate in light of the assurance level of the certificates and the risks posed by issuing a certificate to the wrong person. In addition, the method chosen should be consistent with requirements placed on the PKI by contract or applicable law.

D.3.2.3 Validation of organization identity

Issue Summary. This section covers the methods by which a CA or RA validates the identity of organizations. Such validation may be part of the process by which a CA or RA processes a certificate application for an organizational certificate. This process may also apply to validation procedures for an individual certificate where one of the attributes of the individual validated is the individual's affiliation with a real organization; in that event, the procedures in this section would cover the process of confirming that the organization listed in the certificate application does in fact exist. To the extent the public key of a device or application is certified, procedures in this section would also include validation of the identity of the organization controlling the device or application. Finally, this section could cover the processes by which a PKI validates the identity of organizations taking on the role of another PKI participant, such as a relying party,[313] or a new CA or RA that wish to operate within or interoperate with the PKI.

Relevant Considerations. The validation of organization identity generally has two purposes. First, the CA or RA performing the validation must be sure that the name in the certificate application or other application corresponds to an organization in the real world. In other words, does the organization really exist? Validation procedures seek to prevent fraudulent applications submitted on behalf of non-existent organizations. Second, assuming that the application refers to a real organization, a CA's or RA's validation procedures must ensure that the people presenting a public key for certification, controlling a device that does so, or applying on behalf of an organization wishing to become a CA or RA actually represent the organization and are authorized to submit the certificate or other kind of application. In other words, is the application in fact originating from and authorized by the organization named in the application? Validation procedures, in this case, attempt to prevent fraud based on the impersonation of another organization.

Assessors should determine, based on the assurances provided by the certificates issued within a PKI, whether both of these purposes must be met by the PKI's validation procedures. For lower assurance certificates, the expenditures involved with accomplishing both of these purposes may not be cost effective, in light of a

[313] Where a relying party is not necessarily a subscriber (e.g., a relying party might hold an administrative certificate used solely for access control to a database containing certificate-related information), PKI service providers should perform identification and authentication to ensure that only authorized applicants are able to obtain relying party status.

relatively modest risk of fraud. With respect to higher assurance certificates, however, assessors will want to determine whether validation procedures meet both purposes. Assessors should then determine whether the PKI's actual validation practices accomplish the purposes it sets out to meet in its documentation.

PKIs may utilize a number of ways to identify an organization listed in a certificate application, an organization controlling a device or application, an organization applying to become a CA, RA, or another kind of PKI participant. The methods for validation of the identity of organization are necessarily different from those used to validate the identity of individuals. Examples of validation methods include, but are not limited to:

- Comparing information in a certificate application or other application to documentation and/or certifications evidencing valid formation and/or recognition (as a corporation, partnership, non-profit organization, etc.) in a particular jurisdiction.

- Comparing information in a certificate application or other application with information available from third party sources to confirm that the organization named in the application does in fact exist.

- CA or RA personnel initiating an investigation of the organization, for example through face-to-face discussions with organizational representatives or visits to the organization's site.

- Communications with personnel at the organization who are able to corroborate the organization's identity and the fact that the organization or one of its representatives has in fact submitted a certificate application or application to become a CA or RA.

Assessors should review a PKI's documentation to determine how the PKI purports to validate the identity of organizations. Where external requirements apply to a PKI's validation procedures, assessors should check to see if the PKI's documented procedures meet these requirements. Also, assessors should ascertain whether the validation procedures are sufficiently rigorous in light of the assurances that the PKI intends for the certificates to provide. Finally, assessors may be tasked to determine whether the PKI does in fact follow the procedures that it has documented.

Appropriate Requirements and Practices. The need for rigor in validation procedures will vary from PKI to PKI. A PKI should use validation procedures commensurate with the level of assurances purportedly offered by the certificates. Determining which procedures are appropriate will depend on the risk, sensitivity, and consequence of the transactions, communications, or other applications supported by the certificate. Validation procedures should be sufficiently robust to match the level of assurances provided by the certificates and the business needs underlying the PKI.

Where relying parties or customers of a CA or RA need to decide which certificates are appropriate to trust, CAs will likely want to disclose the practices used by them or their RAs to validate the identity of certificate applicants or potential CAs or RAs. Moreover, CAs and RAs should perform the validation checks that they are required to perform (by policy or other external requirements) as well as checks that they claim to perform in their documentation.

D.3.2.4 Validation of individual identity

Issue Summary. This section covers the methods by which a CA or RA validates the identity of individuals, most likely in connection with a certificate application for an individual certificate.

Relevant Considerations. The validation of individual identity generally has two purposes corresponding to the two purposes for validating organization identity in PAG § D.3.2.3 (Validation of Organization Identity). First, as with the validation of organization identity, the CA or RA performing the validation must be sure that

the name in the certificate application corresponds to a person in the real world.[314] Stated another way, does the individual really exist? Validation procedures prevent the submission of fraudulent applications submitted on behalf of non-existent persons. Second, assuming that there is a real person named in the certificate application, a CA's or RA's validation procedures must ensure that the certificate applicant is in fact the person named in the certificate application. In other words, is the certificate application really from the person named in the certificate application? Validation procedures, therefore, are intended to prevent impersonation.

Assessors should review the PKI's validation procedures in light of the assurances provided by the certificates issued within a PKI, whether the validation procedures meet both of these purposes. For lower assurance certificates, there may not need to be any validation procedures at all, or validation procedures that provide only modest assurances of identity. Assessors should then determine whether the PKI accomplishes the purposes it sets out to meet.

PKIs may utilize a number of ways to identify an individual listed in a certificate application. Examples of validation methods include but are not limited to:

- Requiring a certificate applicant to appear in person before an agent or employee of a CA or RA and to present one or more forms of identity credentials to the agent or employee, who determines whether the credentials confirm the identity of the certificate applicant;[315]
- Comparing information in a certificate application with reliable information in the records or databases of the CA or RA, which may include employment, customer, membership, voting, professional licensing affiliation, email address, and other records;
- Comparing information in a certificate application with reliable information in the records or databases of organizations that specialize in compiling identification data, such as credit bureaus; and
- Requiring the certificate applicant to provide in the certificate application a piece of secret information that has previously been provided to the certificate applicant by the CA or RA (such as a PIN) or that the certificate applicant already possesses (such as information appearing on a pay stub).[316]

The following are examples of credentials that a CA or RA could use to identify a certificate applicant based on personal presence:

- birth certificates,
- driver's licenses,
- employee badges,
- passports, and
- voter registration cards.

[314] *Cf.*, PAG § D.3.1.2 (Pseudonyms and Anonymity).

[315] The PKI may utilize notaries public to check the credentials of certificate applicants.

[316] This last bullet also describes a process that is similar to the method a CA can ensure that the subscriber applying to the CA is the same one whose identity was confirmed by the RA. In such cases, a shared secret is issued to the subscriber after identity confirmation by the RA, then used by the CA to ensure that the subscriber applying to the CA is the same person whose identity was confirmed by the RA. Assessors should keep in mind that there may be numerous, equally-valid variations of this approach, which are used to handle identification, authentication, certificate retrieval and other certificate management processes.

This list is not intended to be exhaustive. Additional features, such as physical identifiers (e.g., biometric measurements, DNA, etc.), may be required for higher assurance levels. Assessors should review a PKI's documentation to determine how the PKI purports to validate the identity of individuals. A PKI may have external requirements that apply to its validation procedures, which assessors should determine.[317] If so, assessors should check to see if the PKI's documented procedures meet these requirements. Also, assessors should ascertain whether the validation procedures are sufficiently rigorous in light of the assurances that the PKI intends for the certificates to provide. Finally, an assessment may involve the determination of whether the PKI does in fact follow the procedures that it has documented.[318]

Appropriate Requirements and Practices. As with the validation of organization identity, the need for rigor in the validation process for individuals will depend on the assurance levels of the certificate and the business model of the PKI.[319] Similarly, the choice of which procedures are appropriate will depend on the risk, sensitivity, and consequence of the transactions, communications, or other applications supported by the certificate. Procedures for validating individual identity should be sufficiently robust to match the level of assurances provided by the certificates and the business needs underlying the PKI.

Validation procedures are generally disclosed by the PKI in cases where relying parties or customers of a CA or RA need to decide which certificates are appropriate to trust. Moreover, CAs and RAs should perform the validation checks that they are required to perform (by policy or other external requirements) and as indicated within their documentation.

D.3.2.5 Validation of authority and other attributes

Issue Summary. This section covers the methods by which a CA or RA validates the authority of persons to act on behalf of others, normally the organizations such persons represent. Such authority may be in the context of a person having a specific role with an organization. Validation may be part of the process by which a CA or RA processes a certificate application for an organizational certificate, or a certificate issued to a device or application, where the certificate provides assurances that the person operating the private key (or the device or application that uses the private key) has the authority to do so on behalf of the organization. Finally, this section could cover the processes by which a PKI validates the authority of persons purporting to act on behalf of an organization applying to become a new CA or RA that operates within or interoperates with the PKI.

Relevant Considerations. PKIs may utilize a number of ways to validate the authority of a person to act on behalf of an organization listed in a certificate application, an organization controlling a device or application, or an organization applying to become a CA or RA. Since organizations have no physical existence, individuals act on behalf of the organization as agents or employees. Depending on the PKI, the validation of authority may, but need not be, coupled with the validation of the identity of the individual exercising that authority under PAG § D.3.2.4.[320] Examples of methods to validate authority include but are not limited to:

---

[317] *See* PAG APP 2 (*Policy requirements for certification authorities issuing qualified certificates*, v.1.1.1, European Telecommunications Standards Institute (ETSI TS 101 456) (Dec. 2000) § 7.4.4(f), *available at* <http://www.etsi.org/sec/el-sign.htm>, hereinafter "ETSI Signature Standard"), "includes requirements for validation of individual identity on registration".

[318] *See* PAG § D.2.7 (Compliance Audit and Other Assessments).

[319] For example, within the healthcare industry there are emerging practices for PKI. *See* PAG APP 2 (*Standard Certificate Policy for Healthcare PKI*, Committee 31.20, American Society for Testing & Materials (ASTM) *available at* <http://www.astm.org>, hereinafter "ASTM Cert. Policy").

[320] Conversely, there may be instances in PKIs offering lower assurance certificates where validation of an individual's identity is not necessary, or where establishing a subscriber's authority without an identity check is sufficient to conduct business, such as an anonymous certificate issued to someone with a $3,000 credit limit that the person uses to purchase items anonymously on the Internet.

- Comparing information in a certificate application with public records or records available from third party sources showing the authority of the individual acting on behalf of the organization.[321]

- Requiring an executive or other manager of the organization to submit a letter, application, or other document stating that the individual named in the certificate application has the authority to act on behalf of the organization. The letter or form could be notarized to strengthen the procedure.

- Communications with personnel at the organization, such as the manager of the person named in the certificate application, which are able to corroborate the person's authority to act on behalf of the organization, the person's possession of a role that entails certain authority.

Assessors should review a PKI's documentation to determine how the PKI purports to validate the authority of organizational representatives. Where external requirements apply to a PKI's validation procedures, assessors should check to see if the PKI's documented procedures meet these requirements. Also, assessors should ascertain whether the validation procedures are sufficiently rigorous in light of the assurances that the PKI intends for the certificates to provide. Finally, some kinds of assessors may be tasked to determine whether the PKI does in fact follow the procedures that it has documented.

Appropriate Requirements and Practices. The degree of diligence that a CA performs in validating the purported authority of a certificate applicant may depend upon the intended use of the certificate. A PKI should use validation procedures to confirm authority that are commensurate with the applicable level of assurance. Determining which procedures are appropriate will depend on the risk, sensitivity, and consequence of the transactions, communications, or other applications supported by the certificate. The PKI should choose procedures to validate authority or other attributes that are sufficiently rigorous to match the applicable level of assurance.

Where relying parties or customers of a CA or RA need to decide which certificates to trust, CAs are expected to disclose the practices used by them or their RAs to validate the authority of organizational representatives. Moreover, CAs and RAs should perform the validation checks that they are required to perform (by policy or other external requirements) as well as the checks that they claim to perform in their documentation.

D.3.2.6 Non-Verified Subscriber Information

Issue Summary. This section relates to the issue of whether a PKI declares or requires that certain information sought in certificate applications will not be validated by the CA or RA and, if so, which information falls within this category.[322]

Relevant Considerations. In the absence of a disclosure in an agreement or policy, a relying party might assume that all information within a certificate has been validated by a CA or RA. Business reality and cost, however, may not make it feasible for a CA or RA to validate all information within a certificate, even though the PKI may find it helpful to include such information within a certificate. For example, a certificate used primarily for client authentication in e-commerce shopping sites may contain demographic information supplied by the certificate application. The CA or RA may not find it feasible or cost effective to confirm all of this information, even though sites may want to use such information for the purpose of providing more personalized services to the subscriber. The sites may know that a certain percentage of subscribers will not

[321] For example, if the certificate applicant purports to be the Sheriff of Palm Beach County, Florida, acting on behalf of the Sheriff's department, one means of validating the certificate application would be to use public records to confirm that a certain person holds the office of Sheriff, coupled with validation procedures to confirm that the certificate applicant is in fact that person.

[322] *See* DSG, *supra* note 2, § 5.6(1).

provide accurate information of this kind on their certificate applications, but the sites may find that it is more useful having this mostly accurate information than not having the opportunity to have this information at all.[323]

Assessors should review the PKI's documentation to determine if certificate information is collected but not validated. They should further determine whether the PKI's practices of not validating certain information is consistent with external requirements that certain information be validated or not validated (such as imposed by law or contract). Finally, assessors should determine whether the information validated by CAs or RAs is sufficient to meet the business needs of the application supported by the PKI. For example, certificates issued to corporate representatives for business conducted on behalf of the corporation may provide insufficient assurances if the corporate affiliation listed in the certificate application is not checked by the CA or RA.

Appropriate Requirements and Practices. In general, a PKI has a strong incentive to provide notice to potential relying parties as to which information has and has not been validated. In the absence of such notice, a CA or RA could be held liable for inaccuracies in information within certificates that it did not validate. Therefore, a PKI will likely find it essential to provide notice as to which information within certificates has not been validated.

With regard to the decision as to which information should be validated and which information need not be validated, a PKI should use validation procedures to confirm the information needed to provide the assurances that the certificates are intended to offer. For example, if certificates purportedly support e-commerce activities by corporate representatives, a certificate is unlikely to provide sufficient assurances if corporate affiliation is non-verified subscriber information. Determining which information should be validated will depend on the risk, sensitivity, and consequence of the transactions, communications, or other applications supported by the certificate. PKIs should ensure that enough information is validated and critical information is not placed within the non-verified category to match the level of assurances provided by the certificates and the business needs underlying the PKI.

Once a PKI decides which information should be validated and which information need not be validated, the PKI's policies relating to non-verified subscriber information should be clearly stated in the PKI's documentation. Further, PKI participants' practices relating to non-verified subscriber information should be consistent with the PKI's documentation.

D.4 Certificate Life Cycle Operational Requirements

This section sets forth the operational procedures followed during the life cycle of a certificate, from application through expiration or revocation.

D.4.1 CERTIFICATE APPLICATION

D.4.1.1 Who can submit a certificate application

Issue Summary. This section describes who can submit a certificate application to a CA or RA, requesting that the CA issue a certificate to a given subscriber.

Relevant Considerations. Based on the CP or other PKI design documents, a PKI service provider will design and create an enrollment process covering the types of certificate applications it expects to receive. Some types of certificates and persons permitted to submit certificate applications are:

[323] *See* EU Signature Directive, *supra* note 5.

- Individual certificates, where an individual applies for her own certificate;
- Individual certificates where the CA or RA generates a key pair and certificate on a smart card or other hardware token and gives the token to the subject, which may make it unnecessary for the subscriber to submit a certificate application, at least until the token is distributed;
- Individual certificates, where a fiduciary (e.g., executor, trustee, attorney-in-fact) requests a certificate on behalf of and in the name of the fiduciary's individual beneficiary, or an agent requests a certificate on behalf of and in the name of his individual principal;
- Organizational certificates used in client applications, where the agent or employee of an organization (e.g., corporation, trust, partnership, LLC, LLP) requests a certificate on behalf of the organization;
- Organizational certificates for client applications issued with the subject being the organization, but the private key is operated by an organization representative with authority to use that key; and
- Certificates issued to a device (e.g., a server) or application that is operated by an agent or employee of an organization authorized to operate the device or application.

Assessors should determine whether a PKI has established the proper enrollment procedures appropriate for the applicable types of certificates issued that ensures only authorized persons are permitted to apply for certificates. They should account for any external requirements, such as those arising from contract or applicable law. Assessors should review the PKI's documentation to determine whether it discloses, at least at a general level, the nature of the enrollment process and the persons applying for certificates. Finally, they should determine whether PKI participants have, in fact, implemented such enrollment procedures.

Appropriate Requirements and Practices. Typically, a certificate is requested by the subject of the certificate. If the PKI's documentation allows submission of an application by an intermediary acting on behalf of a certificate applicant, then the documentation should indicate how the person acting on behalf of the applicant must prove to a CA or RA that she is authorized to request the certificate on behalf of the individual or organization named in the certificate application.[324] A PKI will likely want to define constraints on the delegation of such authority in its CP. The CPS (or another publicly accessible document) can then define how those constraints are implemented.[325] The relationship between the certificate applicant and authorized agents should be defined in the PKI's doumentation to properly identify who can request a certificate.

For a certificate that is intended to be used and relied on with adequate assurances, the certificate applicant (or agent) may digitally sign its certificate request, submit it to the CA (e.g., using a PKCS #10 request) and, in the case of agents, request the certificate on behalf of the certificate applicant. For higher assurance certificates, the agent should be required to provide actual proof of his/her authority to act on behalf of the prospective subscriber. Alternatively, a certificate applicant may use another secure means to request a certificate.

The PKI may also place limitations on the kinds of individuals and organizations that can apply for certificates. For example, if certificates are intended to support a university PKI, the PKI may limit the range of who may apply for certificates to the faculty, staff, and students of the university.

In any case, the enrollment procedures of the PKI should facilitate the submission of certificate applications by persons authorized to apply for certificates. The persons permitted to apply for certificates should be disclosed in the PKI's documentation, taking into account any external requirements, and PKI participants should

[324] The relationship between the certificate applicant and the subscriber may impact the Subscriber responsibilities in PAG § D.2.1.3 (Subscriber Responsibility and Liability).

[325] *See* PAG APP 2 (*Certificate Issuing and Management System, Level 3, Protection Profile*, v. 0.3, NIST (12 July 1999) § 3.2.1.6), hereinafter "CIMS Level 3"), which describes threats from numerous subscribers.

implement their enrollment procedures for authorized certificate applicants in accordance with the PKI's documentation.

D.4.1.2 Certificate application process

Issue Summary. This section discusses how a CA or RA has established an enrollment procedure to allow the submission of certificate applications.[326]

Relevant Considerations. A CA or RA can establish enrollment procedures by which it obtains certificate applications either individually or in bulk. The enrollment process will require some sort of interface, whether online or offline, to permit the submission of certificate applications. Some examples of certificate application processes that a CA or RA can set up include the following:

- A web site that explains the enrollment process and permits certificate applicants to fill out and submit an online application form; the CA or RA can then compare the information in the certificate application against validating information in either a manual fashion by looking up the appropriate records and approving certificate applications one by one, or the process can be automated so that the CA or RA systems compare the information in the certificate application with information in a database and if the information matches, the CA or RA systems approve the certificate application.

- A procedure by which the CA or RA requires the certificate applicant to appear in person and sign paper-based application forms; this procedure may also involve the generation of a PIN or password that the certificate applicant can later use to input into a web site for downloading the applicant's certificate.

- A procedure by which the certificate applicant submits a paper-based certificate application through the mail and receives by return mail or e-mail a PIN or password for downloading the certificate online.

- A procedure by which the CA and/or RA manages the process of the distribution of smart cards or other hardware tokens that authorize certificate applicants; such a procedure may involve the pregeneration of keys on behalf of the certificate applicants and pre-issuance of the certificate prior to the on-line or paper-based application.

- A procedure by which an RA gathers certificate applications using one of the mechanisms above, the RA gathers the certificate applications into a bulk certificate issuance request, and passes the bulk request to the CA; such requests would be signed by the RA's private key.

Assessors should check to determine whether a PKI's enrollment procedures make sense in light of the number of certificates the CA and/or RA will need process. They should also consider whether the procedures make sense in light of validation procedures used for the certificates. Assessors should determine whether external requirements, including technical constraints and requirements originating from contract or law, require the use of certain enrollment procedures. Assessors should then determine whether the PKI's documentation encompasses enrollment procedures appropriate to the PKI. Finally, they should determine whether CAs and RAs within the PKI are, in fact, accepting enrollments using procedures appropriate for the PKI.

[326] Assessors may find that there is some overlap in the discussions related to this section and other portions of PAG § D.4.1 (Certificate Request) and § D.4.2 (Certificate Application). However, this section attempts to focus on the "how" rather than the "who" (PAG § D.4.1.1) of the request. Section D.4.2 focuses on the "what" of the application, which discusses the collection of information for Identification and Authentication performed under the provisions of PAG § D.3 (Initial Validation of Identity, Authority and/or Other Attributes).

Appropriate Requirements and Practices. The certificate request process should provide security safeguards against deliberate attacks and errors, including unauthorized access. The safeguards need to provide assurances commensurate with the intended uses of the certificate as defined in the CP.[327] CAs and RAs, when establishing enrollment procedures, should consider security at every step, from completion of an application form, its transmittal, and its reception and logging by the PKI service provider to the validation and approval of the request.

The security safeguards implemented must ensure the integrity of the completed request in transit, afterwards and generally the confidentiality of the information contained therein.[328] To establish a higher assurance level, a certificate request should be submitted on a signed request form in order to provide additional evidence that the request was properly made. The PKI participant hosting the enrollment process may find it helpful to reference its privacy statement of the enrollment pages or documents. *See* PAG § D.2.8 (Consumer Issues, Information Practices, and Privacy). In addition, completion of a Subscriber Agreement and a point of contact to verify any roles or authorizations requested may be required.[329]

Aside from security concerns, PKIs will want to institute an enrollment process that permits efficient handling of certificate applications. In large PKIs, for instance, it may not feasible to process certificate applications manually. Such PKIs may therefore wish to institute procedures to allow the bulk processing of certificate applications. In addition, the handling of certificate applications should mesh with any requirements that end-user subscribers use smart cards or other hardware tokens. Where there are doubts about the enforceability of online subscriber agreements, and the assurance level provided by the certificates warrants it, the PKI may wish subscribers to submit paper-based certificate applications.

In any event, the enrollment procedures for certificates should correspond to the business needs of the PKI and adhere to any external requirements, such as those imposed by law or contract. The PKI's documentation should accurately reflect the enrollment procedures shown. Finally, the enrollment procedures established by the PKI should match those described in the PKI's documentation.

D.4.2 CERTIFICATE APPLICATION PROCESSING

Issue Summary. This section outlines the responsibilities of PKI service providers, such as CAs and RAs, relating to processing certificate applications in accordance with the relevant CP or other document.[330]

Relevant Considerations. Once a CA or RA has received a certificate application, it must then process the certificate application in some way. Processing a certificate application ultimately culminates in either the approval or the rejection of the certificate application. The processing can either be done by the CA itself, or the CA may delegate this task, as part of its delegation of front-end functions to an RA (*see* PAG § 1.3.1). The CA or RA may also be under some obligation to process a certificate application within a given amount of time.

[327] *See* CIMS Level 3, *supra* note 325, § 3.2.2.1, (which describes threats from the CA); §3.2.2.2 (which describes threats from the RA).

[328] For example, the Canadian PKI allows optional authentication (via a key delivered by out-of-band means) for an applicant's on-line communications with the CA. However, it is unclear whether an application may be submitted electronically. *See* PAG APP 2 (*PKI Certificate and Key Management Interface Specification*, v. 1, Gov't of Canada (Mar. 2000) § 2.1.2.2, *available at* <http://www.cio-dpi.gc.ca/pki-icp/documents/documents_e.asp>, hereinafter "Canadian Interface Specs").

[329] *See* Gatekeeper Criteria, supra note 33 at p. 17. Australian Gatekeeper accreditation mandates the use of a "Customer (Subscriber) Agreement" that "defines the undertakings that subscribers will make in order to obtain and use certificates confirming their digital identities." *See* ASTM Cert. Policy, *supra* note 319. A subscriber agreement is required.

[330] *See* CIMS Level 3, *supra* note 325, § 2.3, ¶ 2, which generally describes CA responsibilities in the area of validation.

Some or all of the RA functions can be delegated to a notary public. A notary may act as or in support of an RA by confirming the identity of the signer. Notaries, especially those in the civil law tradition, are personally responsible for their actions, and most carry liability insurance and/or bonds to cover claims against them.

- A notary assumes responsibility for the contents of a notarial certificate.
- Civil law notarial rules require an established audit trail and retention of documents for specified periods.
- Notaries are appointed by the state, and additionally there is an element of delegated state function in the office of a notary, so that the concept of trust is already built in.
- Compliance audit is ensured through the notarial disciplinary rules.

Assessors should determine which certificate application processing tasks make sense for a given PKI, based on the kind of certificates being issued. Assessors should determine whether any external requirements apply here, such as those imposed by law or contract. They should determine whether specific time periods are required for CA or RA performance levels, and whether the PKI could benefit from having notaries public performing some or all of the RA functions. Assessors should review the PKI's documentation to determine whether it sets forth the kinds of certificate application processing tasks that are appropriate for the PKI and whether these tasks mesh with the validation procedures described elsewhere within the PKI's documentation. Finally, assessors should determine whether PKI participants are, in fact, processing certificate applications in the fashion described in the PKI's documentation.

Appropriate Requirements and Practices. Perhaps the most important task involved with processing a certificate application is the process by which a CA or RA confirms the identity and/or other attributes of the certificate applicant. Successful confirmation of identity or other attributes is commonly the criterion by which the CA or RA either approves or rejects the certificate application. It is common for PKI documentation to refer to the validation procedures in other portions of the documentation, *see* PAG §§ D.3.2.3 (Validation of organization identity), D.3.2.4 (Validation of individual identity), D.3.2.5 (Validation of authority and other attributes).

In addition to confirming identity or other attributes, a CA or RA providing medium or higher assurance certificates will likely want to ensure that its systems confirm that the certificate applicant has possession of a functioning key pair. Specifically, its systems should confirm that the certificate applicant possesses the private key corresponding to the public key in the certificate request. (*See* PAG § D.3.2.2 Method to prove possession of private key.)

Within certain PKIs, there may be a need or desire to ensure that a CA or RA processes certificate applications within a certain amount of time. Such time periods are often set forth in a service level agreement between a PKI participant and its customer or entity delegating tasks to it. There are no standard amounts of time it should take to process certificate applications of different types. For that reason, some PKIs may choose to set forth a standard of conduct rather than a certain amount of time, for example requiring that CAs process certificate applications within a "reasonable" amount of time. Manual validation processes will, of course, take longer than automated validation processes.

It may be helpful, however, to measure processing time periods from the time that the CA or RA receives a completed certificate application until the time a the CA or RA takes action upon it. Measuring time periods in this way includes only the time in which the certificate application is solely within the CA's or RA's control. If the relevant time periods being measured include tasks that may be performed by others, including the certificate applicant, then the CA or RA may be penalized for the delays caused by others.

Some PKIs may find it helpful to make use of notaries for the identity validation portion of certificate application processing. Given typical requirements that notaries confirm identities only when in the personal

presence of a person whose act is being notarized, notaries are particularly helpful in performing some or all RA functions where the PKI's validation requirements call for the personal presence of a certificate applicant before an RA. Moreover, the widespread availability of notaries to confirm identities may make it convenient for certificate applicants to find and make use of a notary's services.

In general, a PKI's documentation concerning certificate application processing should take into account the kind of validation procedures described in other portions of the documentation so that CAs and RAs undertake steps that are appropriate in light of the kinds of procedures undertaken to confirm identity and/or other attributes. The documentation should also account for any statutory, regulatory, or contractual requirements concerning certificate application processing. Furthermore, a PKI's documentation should include compliance with any applicable service level agreements or other documents imposing time limits on certificate application processing. Finally, PKI participants should adhere to documented procedures concerning the processing of certificate applications.

D.4.3 CERTIFICATE ISSUANCE

Issue Summary. This section relates to the process by which a CA issues a certificate in response to a certificate application. It can cover the circumstances under which a CA issues certificate and/or the significance of certificate issuance. Moreover, this section can describe ways in which the CA makes the certificate available for the subscriber to use. Finally, this section can reference methods by which the CA notifies the community of potential relying parties or others of the issuance of a certificate.

Relevant Considerations. The certificate issuance process takes place following the approval of a certificate application, in which the information in the certificate application was confirmed. Certificate issuance involves the CA constructing and populating the fields of the certificate and digitally signing this structure to create the certificate.[331] The contents of the certificate are frequently defined in the PKI's documentation. See PAG § D.7.1 (Certificate Profile). The certificate issuance process may culminate in making the certificate available to the subscriber, and otherwise notifying the certificate applicant of its issuance, and the publication of the certificate in a repository.[332]

A CA can make use of a variety of mechanisms to make the certificate available to the subscriber. First, a CA may explicitly notify the subscriber of certificate issuance by e-mail or other communications.

Frequently, such a notice serves the purpose of giving the subscriber an opportunity and instructions to download the certificate and load it into the subscriber's software. Alternatively, a CA can send the certificate to the subscriber with instructions on how to load the certificate into the subscriber's software. Such notification mechanisms may require confidentiality and integrity protection.[333] In yet other cases, issuance of a certificate precedes delivery of a smart card or other token containing the subscriber's key pair and/or associated certificate. In such cases, the process of making the token available corresponds to the process of making the certificate available to the subscriber.

---

[331] *See* DSG, *supra* note 2, § 1.16.1, ("[t]he creation of a certificate by a certification authority includes both generation of the certificate and the digital signature of the certificate. The certification authority must generate the certificate before it can be digitally signed. How and by whom it is generated depends on the specific practices of the certification authority for issuing the certificate").

[332] *See* CIMS Level 3, *supra* note 325, § 3.2.1.1.2 (CA), § 3.2.1.2.8 (Admin) and § 3.2.1.4.1 (Incidental Bystander), for threats related to integrity of the transmitted private key. *Id.*, § 5.1.2.1, ¶ 2 and § 5.1.3.1, ¶ 3 for related requirements.

[333] "The certification authority may give notice of the creation and contents of the certificate by giving the subscriber a printed representation of the certificate, by allowing the subscriber to view the contents of the certificate on-line or on subscriber's computer, or by communicating the contents of the certificate to the subscriber in any other reasonable way. The notification requirement may be accomplished by providing the subscriber with an electronic copy of the certificate, which has the further advantage of enabling the subscriber to further distribute the certificate to third parties in the position of relying on it to verify the subscriber's digital signature." *Id*.

In some cases, a CA's specific notice to a subscriber that a certificate has been issued may be unnecessary. Publication in a repository may constitute sufficient notification of issuance to a subscriber.

Publication of the certificate serves as notification to potential relying parties that a CA has issued a certificate to a relying party. "Publication" is the act of recording or filing "in one or more repositories." DSG § 1.26. A CA may have its own designated repository for the purposes of publication. In addition or alternatively, the CA may also publish certificates in other recognized third party repositories. The community of potential relying parties may be limited in closed communities.[334] In other PKIs, however, there may be no limitation on who may become a relying party, and in such communications, a PKI may decide to allow the general public access to its repository.

Assessors should review the PKI's documentation to determine the circumstances under which certificate issuance takes place, its significance to the PKI, and the process by which the CA notifies PKI participants and others of the issuance. They should determine whether such procedures make sense in light of the kinds of certificates issued and the business needs of the PKI. Assessors should also determine whether such procedures are consistent with any external requirements for issuance procedures placed on a PKI by law or contract. Finally, assessors should determine whether, in fact, CAs within the PKI are following the issuance procedures described in the PKI's documentation.

Appropriate Requirements and Practices. PKI documentation typically states that a CA will issue a certificate after the certificate applicant has successfully completed all enrollment procedures, the CA or RA has completed all validation procedures, and the CA or RA has approved the certificate application. In other words, certificate issuance is typically appropriate once all of the certificate application processing tasks identified in PAG § D.4.2 have been completed. Where there is no formal approval of the certificate application recorded or logged, a PKI may wish to state in its documentation that issuance of a certificate indicates final approval of the certificate application leading to the certificate's issuance. That is, the significance of the fact that a certificate was issued may be its role as an acknowledgement that the CA has made a final acceptance of the certificate application.

The process of creating and populating the certificate is generally mentioned in PKI documentation, although PKIs typically do not detail specific certificate content in the sections of their documentation corresponding to this PAG § D.4.3. Rather, PKIs may simply cross-reference other portions of their documentation that cover certificate content. *See* PAG § D.7.1 (Certificate Profile).

The method by which the CA makes the certificate available to the subscriber will largely depend on the types of systems used by the subscriber, the relative sophistication of the subscriber's software for installing the certificate, and the urgency of the business' needs for the subscriber to use the certificate as soon as possible. Where individuals are using client certificates, there may be a business need to create an application as part of the enrollment process that automatically loads the certificate into the client software. This kind of software may be especially helpful where subscribers do not have a lot of experience in installing certificates. In such cases, the CA may notify the subscriber of a website that the subscriber can use to invoke the application that installs the certificate. If the PKI does not have a business need to ensure that subscribers make use of their certificates as soon as possible, the PKI may simply make the certificate available for downloading or receipt and place the onus on the subscriber to initiate the process to retrieve the certificate. Where subscribers are relatively more sophisticated, a CA may also make a certificate available by e-mailing it to the subscriber with instructions on how to install it.

In some cases, it may be appropriate to notify the subscriber of certificate issuance where the person submitting the certificate application is not himself or herself the subscriber. For instance, where the certificate is issued to a device through the actions of an agent submitting a certificate application, the CA may wish to inform other people within the subscriber organization of the issuance of the certificate. If the certificate application were

[334] *See* CARAT Guidelines, *supra* note 200, § C.2.3.1.

mistaken or unauthorized, such a notice could trigger a response by the subscriber and the CA would be able to catch the mistake or fraud.

CAs normally make certificates available to others by publishing the certificate in a repository. Since publication functions are normally covered in sections of a PKI's documentation other than the one corresponding to this PAG § D.4.3, a PKI may find it convenient simply to cross-reference the section in which it discusses publication of certificates. *See* PAG § D.2.6 (Publication and Repositories).[335]

In some cases, the CA may wish to inform people other than the subscriber and potential relying parties of the issuance of a certificate. For instance, the CA may want to tell the RA that approved the certificate application that the CA has, in fact, issued a certificate to the certificate applicant. Also, in the case of a sponsor that has arranged for the issuance of certificates in bulk to a certain community of interest, the CA may wish to inform the sponsor of the issuance of certificates to members of the community.

In general, a PKI should establish procedures in its documentation that provide an efficient mechanism to provide certificates to subscribers after a CA or RA processes a certificate application in light of the types of subscribers using certificates and the systems they use. The PKI should notify parties that have a need to know of the certificate issuance and should make the certificate available for use by potential relying parties. The PKI's documentation should reflect these procedures, which should be consistent with any statutory, regulatory, or contractual requirements. Finally, CAs should follow the documented procedures.

D.4.4 CERTIFICATE ACCEPTANCE

Issue Summary. This section specifies the means by which a subscriber manifests acceptance of the certificate that the CA has issued.

Relevant Considerations. Acceptance of a certificate may be expressed or impled. Acceptance of a certificate is always the act of a subscriber, but in the case of implied acceptance, the conduct need not be an explicit agreement to the content of the certificate.[336] The act of acceptance triggers duties, rights, and obligations as described in PAG § D.2 (General, Legal and Business Provisions).

The subscriber may be given the opportunity to examine the issued certificate before issuance. Such systems present the certificate applicant with the proposed content of the certificate, require the certificate applicant to review the content, and either accept or reject the proposed certificate. Where this occurs the CA may provide the appropriate tools to intelligibly read, or "parse," the certificate fields.[337] Most CAs, however, utilize software and systems that do not afford subscribers the opportunity to inspect the actual certificate prior to the issuance. These CAs may issue the certificate, make it available to the subscriber for use, and require the subscriber to review the certificate. The PKI documentation may place an obligation on the subscriber to notify the CA or RA of any mistakes in the certificate within a reasonable time.

---

[335] *See* DSG, *supra* note 2, § 3.8(2), (a CA should not publish a certificate until after a subscriber had accepted it). *But see id*., § 1.1.4 (contemplating a scenario in which publication precedes implied acceptance). Some software is capable of showing proposed certificate content to a subscriber and requiring the subscriber to manifest assent to such certificate content before the CA publishes the certificate. Most CAs, however, do not use such software, but rather rely on subscribers to revoke their certificates in case they do not accept the content of the certificates, for example in cases of errors in certificate content. Therefore, most PKIs would find it unrealistic under today's technological environment to require acceptance to precede publication.

[336] *See* DSG, *supra* note 2, § 1.1, ("[t]o demonstrate approval of a certificate while knowing or having notice of its contents"). *See also* ASTM Cert. Policy, *supra* note 319, (for healthcare requiring express subscriber acceptance of certificate).

[337] Measures designed to prove receipt of the certificate by the subscriber may be useful in establishing notification. *See* Japanese Guidelines, *supra* note 290. Alternatively, a CA may request a secure message confirming successful receipt of the certificate.

Where the CA's systems cannot require express acceptance as a condition of issuance, acceptance of an already issued certificate has to be implied by the subscriber's conduct. One example of implied acceptance is use of the private key corresponding to the public key in the certificate following downloading of the certificate. In that case, the subscriber has had an opportunity to review the certificate content and, despite an opportunity to request the revocation of the certificate as being unauthorized or inappropriate, the subscriber has nonetheless began to make use of the certificate. Another example of implied acceptance is the passage of a certain period of time following the subscriber's access to the certificate in which the subscriber has not requested revocation of the certificate.

Assessors should determine whether law applicable to the PKI requires or likely requires express assent to a certificate's content in order to constitute acceptance of the certificate, or whether implied conduct can constitute acceptance of a certificate. They should also review the PKI's documentation to determine which kind of acceptance is deemed to be effective within the PKI. The PKI's documentation should implement any requirements for certain kinds of acceptance imposed by law or contract. Finally, assessors should determine whether CAs and RAs have implemented procedures to allow subscriber acceptance of certificates consistent with the PKI's documentation.

Appropriate Requirements and Practices. The issue of whether a PKI should establish systems to require express acceptance of a certificate's content will depend on whether applicable law requires express assent to a certificate content to be deemed acceptance. It is an open question whether contract terms are enforceable if they assume the implied acceptance of a certificate, as opposed to agreements requiring conduct expressly manifesting asset to a certificate. It seems likely that express conduct indicating assent to a certificate will more likely be binding upon a subscriber than an implied acceptance based on related conduct, such as beginning to create digital signatures verifiable with reference to the certificate. On the other hand, procedures to parse the certificate, present proposed content to a certificate applicant, and require express agreement to the content of a certificate may be more costly to establish and more burdensome to users. In the end, the PKI will want to balance the need for enforceability against the cost and burden associated with requiring express acceptance of a certificate.

Whichever type of acceptance is most consistent with the PKI's business needs should be reflected in the PKI's documentation. The documentation should specify whether express, implied, or both types of acceptance are permissible, consistent with any external requirements such as those appearing in applicable law or contracts. Appropriate acceptance procedures may depend on the required level of assurance levels of the certificates. Finally, CAs should implement mechanisms to permit or require acceptance procedures that are consistent with the PKI's documentation.

D.4.5 CERTIFICATE USAGE

Issue Summary. This section addresses the responsibilities, terms, and conditions placed on relying parties relating to the proper usage and reliance upon certificates or any restrictions on usage of or reliance on a certificate.

Relevant Considerations. A PKI will frequently define the intended uses of certificates by both subscribers and relying parties. See PAG § D.1.3.4 (Applicability). The organization may further restrict intended uses of the certificate by such parties. For example, an organization may issue certificates to its employees. The organization may restrict certificate use to business purposes, or it may also permit personal use. Similarly, a trading community may restrict reliance by community members that is outside of the intended certificate usage. In any event, the CP, CPS and other policy documents may set forth the intended uses for the certificates, which may include technical, procedural, and/or legal controls.

Assessors should assess factors that may influence the number and type of restrictions, which may include: the extent to which the CA validates the certificate applicant's identity; the certificate's intended use; applicable laws and regulations; existence of insurance; and specific business needs.

Some relying party systems are able to enforce such certificate usage restrictions. This can be accomplished through programming by allowing software or hardware devices to recognize and rely upon only those with certificates containing the OID of the appropriate CP. *See* PAG §§ D.2.1.4 (Relying Party Responsibilities), B.4 (PKI Documentation) and APP 5 (Proposed Guidance for Development of Compatible End-User Product).

Assessors should review a PKI's documentation to determine what requirements a PKI places on certificate usage and limitations on usage. They should determine whether any externally-imposed requirements apply to the PKI, including those imposed by operation of law or contract. Finally, they should determine whether relying parties participants are, in fact, adhering to any usage requirements.

Appropriate Requirements and Practices. In general, a PKI will want to set forth relying party responsibilities relating to proper certificate usage in its documentation, such as provisions in a CP or CPS, or a subscriber agreement, relying party agreement or certificate (where space allows). It may be helpful to cross reference other sections of PKI documentation relating to the appropriate usage and restrictions on usage of certificates, *see* PAG § D.1.3.4 (Applicability), and sections relating to relying party obligations, *see* PAG § D.2.1.4 (Relying Party Responsibilities and Liability). Such responsibilities should be consistent with external regulatory and contractual requirements. Finally, relying parties should use certificates within the limitations and requirements imposed by the PKI's documentation.

D.4.6 ROUTINE CERTIFICATE RENEWAL

Issue Summary. This section concerns the process by which certificates are renewed on a routine basis. It covers the process by which a CA establishes procedures for renewal, describes the validation of renewal requests, and the actions taken by the RA or CA in response to a renewal request.

Relevant Considerations. Certificates have lifetimes, or operational periods, which may be specified in a CP or CPS.[338] Renewal is the process by which a new certificate is issued in order to replace a certificate that is expiring. Technically speaking, renewal involves recertification of an existing key pair and "rekeying" involves the generation of a new key pair and issuing a certificate certifying the new public key. Detailed information about the procedures for routine certificate renewal may often be found in documentation about the system's renewal operations (i.e., process flow documents). Issues surrounding routine renewal that need attention include:

- whether automatic renewal is permitted (it may depend on level of assurance of certificate), or whether some new validation procedures are required. In the case of automatic renewal, the subscriber should be notified of such renewal on or before the renewal date. There may be reasons to prohibit automatic renewal in favor of a manual certificate issuance process;

- in the case of renewal where revalidation is used, what kinds of validation procedures are sufficient to approve a renewal request;

- whether a new key pair is generated or the CA re-signs the old public key. The creation of a new key pair increases the cryptanalysis efforts needed to identify private keys. Certifying a new key pair burdens key management requirements, including the decryption of archived documents, in the case of encryption certificates;

- whether someone other than the subscriber can request renewal;

[338] The operational period may be linked to the suitability of various technical components. For example, the German PKI places a five-year ceiling on a certificate's validity period subject to the continued suitability of the relevant key generation, hashing, and verification algorithms. *See* PAG APP 2 (*Federal Act Establishing the General Conditions for Information and Communications Services* – Information and Communications Services Act, art. 3, 1997 F.R.G. (enacted 8 Jan. 1997), § 7, *available at* <http://www.iid.de/iukdg/gesetz/sigve.html>, hereinafter "German Signature Act").

- whether the procedures should be different if a subscriber wants to renew a certificate that has expired; and

- whether and how a subscriber is notified that a new certificate has been issued in response to a renewal request.

Assessors should determine whether these issues dictate the need for requirements or practices of a PKI. They should also review a PKI's documentation to determine whether it reflects these requirements or practices, consistent with any regulatory or contractual requirements. Finally, they should determine whether renewal procedures match those set forth in the documentation.

Appropriate Requirements and Practices. The certificate renewal process will depend on a number of factors including key pair validity periods, contractual renewal requirements, software capabilities, etc. Generally, a PKI will want to document its procedure for notifying subscribers of the need for renewal prior to the expiration of their certificate. Where a certificate has a validity of one year, the renewal process may be initiated by attempting to contact the subscriber, for example, three months prior to certificate expiration.

Automatic renewal may occur based upon an on-line connection with the CA some time before certificate validity expiration. The policy for making a renewal request can be modeled on the policies identified in PAG § D.4.1.1, (Who Can Request a Certificate). Generally, only subscribers themselves should have the authority to make a renewal request.

A routine request for certificate renewal is usually made using the private key associated with an unexpired certificate. However, there may be instances where an automatic renewal request may be authenticated based upon a request signed by a private key that corresponds to a certificate that has been revoked for a reason other than key compromise. If a certificate is revoked because the subject changes name or affiliation thereby requiring a change in the distinguished name in the certificate, there is no degradation in the trustworthiness of the certificate and associated signing private key. For efficiency purposes, the corresponding private key could be used as a means of authenticating the subject exclusively for initiation of the automatic renewal.

Unless otherwise specified by a CP or CPS, the renewal request should be treated as valid and authenticated if signed by the private key corresponding to the public key in the certificate renewal request.

The processing of a routine certificate renewal request ensure that the trustworthiness of the procedural and technical requirements required for certificate issuance is maintained for the renewal process. Upon receipt of a routine certificate renewal request, the CA shall ensure that the request is coming from the subscriber or other authorized party, construct/reconstruct the certificate fields, modify the valid from and valid to dates, and sign the certificate.

Notification of certificate renewal can be provided via email or other reliable means. The notice provided to the subscriber by the PKI service provider can describe how and where to retrieve the certificate.[339] If delivery of the certificate requires that the subscriber be authenticated, the subscriber may use its unexpired certificate / key pair for authentication for online retrieval. The notification procedures used by a CA or RA should be equivalent to the procedures used to notify a new subscriber of certificate issuance. *See* PAG § D.4.3 (Certificate Issuance).

In general, renewal practices providing assurances commensurate with the assurance levels of the certificates should appear in the PKI's documentation. The documentation should account for external requirements. CAs and RAs, in turn, should establish renewal procedures that adhere to the documentation.

[339] A CA may also wish to notify others of the renewal of a certificate, such as the RA approving the renewal application or the sponsor of the certificate. *See* PAG § D.4.3 (Certificate Issuance).

D.4.7 PROCESSING A REQUEST FOR A NEW KEY PAIR

Issue Summary. This section identifies the procedures by which an existing subscriber might ask for the certification of a new key pair. This section describes the information and process used to validate such a request. Finally, this section also covers the way in which a CA or RA would process such a request and whether and how a CA would notify the subscriber of the availability of the new certificate.

Relevant Considerations. The process of generating a new key pair and requesting the certification of a new public key may be routine as part of the process to place a new certificate in the hands of the subscriber around the time the subscriber's existing certificate expires. In the case of routine rekeying in response to impending certificate expiration, some of the relevant considerations described in PAG § D.4.6 (Routine Certificate Renewal) apply here. Alternatively, a request for certifying a new key may arise in the case of a key compromise. It may be possible for an existing subscriber to request a new or additional certificate by proving possession of a private key corresponding to the public key of a currently valid certificate or a certificate revoked for a reason other than key compromise as discussed in PAG § D.4.7 (Processing a Request for a New Key Pair) and by undergoing reauthentication procedures to ensure that it is, in fact, the subscriber who is requesting certification of a new key pair.

Assessors should determine which procedures for authenticating and processing requests for certifying a new public key are appropriate for the PKI. They should review the PKI's documentation to determine which procedures are described there, and whether they are consistent with any external requirements. Finally, they should determine if the CA or RA is implementing rekeying procedures consistent with the PKI's documentation.

Appropriate Requirements and Practices. The processes for validating a request to certify a new key pair will vary depending on the mechanisms used to authenticate the requester for key certification. As a default, some PKIs may wish to treat a request for the certification of a new public key to replace an existing certificate in the same manner as a new certificate application, requiring full validation procedures. Such procedures would ensure that the trustworthiness of the validation of initial certificate applications would be the same as the trustworthiness of the process of rekeying. Generally, the same person who is allowed to request a certificate (PAG § D.4.1.1 (Who Can Submit a Certificate Application)) or perform routine certificate renewal (PAG § D.4.6 (Routine Certificate Renewal)) is allowed to request certification of a new key. Unless there is a business need as documented in a CP or CPS, the subscriber should be the only one permitted to request certification of a new key.

Although, a complete re-certification of the subscriber ensures continued trustworthiness of the validation process, it imposes a burden on the CA or RA performing the validation and perhaps the subscriber as well. Therefore, PKIs may want to consider whether processes used to authenticate the existing subscriber in order to avoid a complete re-certification are satifactory in light of the assurances provided by the certificate. These processes may be combined and may include shared secret and biometric verification.

Using such mechanisms for authenticating the existing subscriber may provide accelerated return to operational status for the subscriber and decreased operational burden on the CA, RA, and subscriber.

The processes for certification of a new key may vary depending on the reason for such a request and the methods used to authenticate the certification request. Some of the appropriate requirements and practices involved with certificate renewal apply here if rekeying is simply a mechanism to provide new certificates upon expiration of existing certificates. *See* PAG § D.4.6 (Routine Certificate Renewal). A request for the certification of a new public key of a key pair following a key compromise may call for procedures different from routine rekeying requests.

Once the new key pair has been certified, the CA often notifies the subscriber of certificate issuance. The PKI should document the process to be used to notify subscribers of certificate issuance. Notification to the subscriber that his new key pair has been certified can also contain information about how and where to retrieve

the certificate. If the new key pair certification is the result of key compromise, notification and delivery of the new certificate may need to follow procedures used for new subscribers. It is often possible to use the same notification procedures that a CA or RA uses to notify new subscribers of certificate issuance. *See* PAG § D.4.3 (Certificate Issuance).

A PKI should document rekeying procedures that are commensurate with the level of assurances provided by the certificates. It should consider whether key compromise requires special rekeying procedures. The PKI's documentation should adhere to any external regulatory or contractual requirements. Finally, CAs and RAs should establish rekeying procedures consistent with the PKI's documentation.

D.4.8 CERTIFICATE CONTENT MODIFICATIONS

Issue Summary. This section relates to circumstances under which it is appropriate for a CA to issue a subscriber a new certificate in order to reflect new certificate content. Changes in circumstance that are allowed by the PKI as grounds for issuing a new certificate to reflect content modifications are listed in this section. This section also specifies the information that must be processed by the CA or RA to validate new or changed information. In addition, this section outlines the process for the PKI service provider to follow in issuing a new certificate to reflect content modification. Finally, this section specifies the process, if any, for notifying the subscriber that a new certificate reflecting modifications has been issued and is ready for retrieval.

Relevant Considerations. Several changes in circumstances may arise that will lead to a request for modification of the contents of a certificate. There may be a need to modify the contents of a certificate during the validity period of a certificate. Normally, such requests are made via a signed request using the existing certificate. Those situations are listed below in Appropriate Requirements and Practices.

All of the reasons for requesting or processing a certificate modification may not be known by the parties when policy documents are drafted. Assessors reviewing the implementation of this section should allow a degree of flexibility. For a group of certificates being modified to accommodate a new application or extension, variables associated with that new application or extension may drive the modification process.

Assessors should determine which procedures to validate modifications to certificate content ensure a level of trustworthiness commensurate with the assurances provided by the certificates. They should also review the PKI's documentation to see if such procedures are reflected there, consistent with any requirements imposed by law or contract. Finally, they should determine whether CAs and RAs have, in fact, followed the content modification procedures set forth in the PKI's documentation.

Appropriate Requirements and Practices. Some common situations in which a PKI may want to permit certificate modification are:

- Legal name changes due to marriage, divorce or court petition
- Change in organizational affiliation, including corporate merger or acquisition
- Change in location information
- Change in e-mail address
- Change in any attribute/extension of a certificate
- Addition of a new OID

The subscriber is normally the only person permitted to request modification of a certificate. In the case of a change of affiliation of the subscriber, however, an authorized member of the new organization, working in conjunction with an authorized member of the former organization, may request modification of a certificate.

This may be done as a blanket request in the case of organizational name change, corporate or departmental restructuring, merger or acquisition. The subscriber may also, when permitted by the PKI, delegate to a designated representative the right to request a modification of the content in the subscriber's certificate.

PKI service providers will want to validate the source of a certificate modification request and the information to be contained in the modified certificate. There may be instances where a certificate modification request may be authenticated based upon a request signed by a private key that corresponds to a certificate that has been revoked for a reason other than key compromise. If a certificate is revoked because the subject changes name or affiliation thereby requiring a change in the distinguished name in the certificate, there is no degradation in the trustworthiness of the certificate and associated signing private key. For efficiency purposes, the corresponding private key could be used as a means of authenticating the subject exclusively for initiation of the certificate modification process. Alternatively, because the certificate is a public means of certifying the public key, a bulk revocation and re-issuance process might take place without use of the subscribers' private keys.

After proper validation of the request, processing of a certificate modification will typically follow the same procedures as with a new certificate request. The CA may not revoke the old certificate prior to issuance of the new certificate. To ensure continuity for the subscriber, the new certificate shall be issued and accepted by the subscriber prior to revocation of the old certificate.

Subscriber notification of certificate reissuance based on modified content should be designed and implemented so that the subscriber has adequate notice and instruction about how to retrieve, review, install and use the modified certificate.[340] Designers of procedures for providing subscriber notice of certificate modification may want to consider the timing of providing notice to the subscriber and third parties. In some technological environments, the subscriber may have an opportunity to review the modified certificate for accuracy before it is published and provided to others. With systems used by most CAs and RAs, however, the subscriber may not have such an opportunity, and the PKI may place the onus on the subscriber to notify the CA or RA in the event that further modifications of certificate content are necessary.

Generally speaking, a PKI should adopt certificate content modification and reissuance procedures that are commensurate with the assurance levels of the certificates. The PKI should document these procedures, which should be consistent with any applicable external requirements. Finally, CAs and RAs should implement certificate content modification procedures that adhere to the PKI's documentation.

D.4.9 CERTIFICATE REVOCATION AND SUSPENSION

Issue Summary. This section D.4.9 provides the procedures for revoking and suspending certificates.

Relevant Considerations. Revocation and suspension procedures are usually more critical to the design of a PKI than other procedures. Similar to identification and authentication procedures, which are also PKI-specific and customized, revocation and suspension procedures will depend heavily on the intended goals of the PKI. The design of the revocation and suspension procedures may also depend on external legal requirements, such as statutory suspension and revocation requirements.

Appropriate Requirements and Practices. The subsections within this section contain appropriate requirements and practices relating to more specific topics concerning revocation and suspension.

[340] As with certificate renewal, a CA may also wish to notify others of a rekeying operation, such as the RA approving the rekeying application or the sponsor of the certificate. *See* PAG § D.4.3 (Certificate Issuance).

D.4.9.1 Circumstances for revocation

Issue Summary. This section contains a list of circumstances where certificate revocation is appropriate or required.

Relevant Considerations. The purpose of a digital certificate is for a CA to make an assertion that a public key is bound to a specific identity and/or other attributes of an individual or organization. Although making such an assertion is useful, relying parties are most likely to be interested in knowing whether that binding continues to be true at the time the relying party wishes to rely on that binding. Moreover, a CA may wish to cut off the effectiveness of the assertion if the binding is no longer reliable, or the CA no longer wishes to provide services to the subscriber. The mechanism by which the CA can terminate the assurance of binding is through revocation of the certificate.

Circumstances under which revocation is appropriate roughly fall into four categories:

- The certificate's binding of a public key to a specific identity and/or other attributes is no longer reliable.
- The CA wishes to terminate services to the subscriber for reasons not directly related to the reliability of the certificate.
- Rights underlying the subscriber's access to and use of applications secured with a certificate have terminated.
- The subscriber wishes to terminate the CA's and/or RA's services for some reason.

Assessors should determine, based on the applications secured by the certificates and their assurance levels, which circumstances can or should lead to revocation, and for each set of circumstances, whether revocation should be required or optional. They should consider the effect of any regulatory or statutory requirements or constraints on revocation. Assessors should then review the PKI's documentation to determine if it contains appropriate triggers for revocation. Finally, they should ascertain whether, in fact, a PKI's participants are initiating revocation under the circumstances set forth in the PKI's documentation.

Appropriate Requirements and Practices. Certificate revocation services are, in almost all cases, a critical component of a PKI. Therefore, documenting circumstances under which revocation takes place is important in all but the most rudimentary PKIs, perhaps where certificates provide no assurances of the identity of subscribers or the certificates are being used in a testing environment. Specific reasons for revocation typically include some or all of the following circumstances:

- Loss of control of private key (key compromise)
- Death or disability of the subscriber
- Theft, loss or destruction of the private key or private key container (i.e. smart card, computer)
- Authenticated request of the subscriber for any reason
- Use of the certificate in violation of applicable agreement
- Change of any material certificate data
- Termination of employment or affiliation
- Breach of contract (e.g., nonpayment for service)

- Loss of license or right to access protected information

- To the extent the certificate is used as an access control mechanism to gain access to protected information, the loss of the subscriber's license or right to access such information

Whether revocation is optional or mandatory in each of these cases will likely depend on the circumstances and the assurance levels provided by the certificates. As a general matter, however, revocation circumstances involving the lack of reliability of a certificate involve a higher priority for revocation than other circumstances.

PKIs should document when revocation is mandatory and when it is optional. These circumstances should ensure the continued trustworthiness of the bindings of public keys to identity and/or other attributes in certificates, and should be consistent with regulatory and contractual requirements. Finally, CAs and RAs should ensure that their revocation services conform to a PKI's documentation.

D.4.9.2 Who can request revocation

Issue Summary. This section sets forth who can request certificate revocation, whether that is the subscriber, a representative of the subscriber, or the CA or RA that approved the certificate application.

Relevant Considerations. In addition to the subscriber (or authorized representative), the CP or CPS may specify other parties who are permitted to request revocations. These often include RAs and employers, or parties who attest to the validity of or otherwise supply information stated in certificates. For example, the CP or CPS may permit an RA or an employer to request a revocation where the key is compromised, the employee is terminated, or where the subscriber no longer has access to the key. A CA or RA may initiate a revocation when it has knowledge of facts that constitute grounds for revocation. Additionally, the CA or RA may be required to revoke a certificate in response to court order or other legal process.

Assessors should consider who has a need to request or initiate certificate revocations based on the circumstances under which certificates must or can be revoked. They should then review a PKI's documentation to determine whether it reflects the needs for certain PKI participants to request or initiate revocation under certain circumstances, consistent with any external regulatory or contractual requirements. Finally, assessors should determine whether access to revocation services is limited to appropriate persons in accordance with the PKI's documentation.

Appropriate Requirements and Practices. The identity of participants that can request or initiate revocation will depend on the circumstances leading to the revocation. *See* PAG § D.4.9.1 (Circumstances for revocation). Specifically:

- Where revocation occurs because the certificate's binding of a public key to a specific identity and/or other attributes is no longer reliable, the subscriber is typically required to request revocation and, where the subscriber fails to do so, the CA or RA generally has a requirement to initiate revocation.

- Where revocation takes place because the CA wishes to terminate services to the subscriber for reasons not directly related to the reliability of the certificate, it is typical the CA or RA that has the onus to initiate revocation.

- Where revocation is based on the termination of rights underlying the subscriber's access to and use of applications secured with a certificate, the CA or RA normally bears the burden of ensuring that revocation takes place, although a PKI may refer to a requirement that subscribers request revocation upon resigning from positions meriting a certificate or relinquishing rights to use an application secured by a certificate.

- Where the subscriber wishes to terminate the CA's and/or RA's services for some reason, the subscriber necessarily must be the participant that requests revocation.

In sum, PKIs will want to implement requirements and practices concerning who can request or initiate revocation that are consistent with the circumstances for revocation. The participants permitted to request or initiate revocation should appear in the PKI's documentation. Finally, the revocation procedures established by CAs and RAs should ensure that parties permitted or required to request or initiate revocation can, in fact, do so.

D.4.9.3 Validation of a Revocation Request

Issue Summary. This section specifies the kinds of evidence that a PKI service provider should request and review prior to its decision to revoke a certificate.

Relevant Considerations. Validation of a revocation request is the process by which a CA or RA ensures that a request or initiation of revocation has, in fact, originated from a person authorized to submit the request or to initiate the revocation. Some possible validation mechanisms include:

- Requiring the subscriber submitting a revocation request to digitally sign the request using the private key corresponding to the public key in the certificate to be revoked,
- Requiring the subscriber to submit a shared secret or use a biometric identifier to authenticate the request,
- In the case of an RA instructing a CA to revoke a certificate, a digitally signed revocation instruction,
- In the case of an RA instructing a CA to revoke a certificate or a CA administrator initiating revocation on internal systems, using certificate-based access control to a revocation interface, and
- Out-of-band communications using mechanisms that provide assurances that the revocation request is originating from an authorized participant that meet the PKI's standards.[341]

Note that a revocation request signed with the corresponding private key is presumed valid, even if signed by the person who stole the key. If the subscriber is the one who sent the request, then the CA will want to honor the request because it did, in fact, originate from the subscriber. If a thief is the one who sent the request, the CA will still want to revoke the certificate anyway because the private key is compromised. In either case, whether the subscriber really sent a revocation request or not, a CA will want to revoke the certificate.

Assessors should determine which procedures are appropriate for validating revocation requests in light of the circumstances under which revocation takes place and the identity of the participants requesting or initiating revocation. They should also review the PKI's documentation to determine whether revocation requests are validating in these ways and whether the PKI's practices are consistent with statutory or contractual requirements imposed on the PKI. Finally, assessors should ascertain whether CAs and RAs are, in fact, following the validation procedures appearing in the PKI's documentation.

Appropriate Requirements and Practices. As a general matter, a CA or RA should have sufficient evidence that a revocation request is originating from an authorized party before acting the request. In the event that such evidence is not immediately available, the CA or RA may decide to suspend the certificate pending availability of such evidence to the extent permitted by the applicable rules. Once sufficient evidence has been produced, the revocation request can be processed.

[341] *See, e.g.*, German Signature Act, *supra* note 338, § 9(1) (requiring CAs to provide a 24-hour revocation hotline)

The fashion in which requests are validated will depend on the participant requesting or initiating the revocation and the circumstances of revocation. If the subscriber is the one appearing to request the revocation, a signed message from the subscriber, a shared secret, or use of biometrics would provide the greatest security. The subscriber, however, may not be able to send a signed message if the reason for revocation involves the loss of the computer or token on which the private key resides. Moreover, subscribers may forget or be unable to access the shared secret needed to authenticate themselves. In such cases, a CA or RA may want to allow for "back-stop" measures of out-of-band communications to permit revocation where a subscriber is otherwise unable to perform the authentication procedures. A PKI, however, will have to weigh the need for flexibility against the possible unreliability of such communications.

The way in which CAs and RAs initiate revocations on their own initiative will largely be a function of the CA or RA systems being used to perform revocation functions. Revocation functionality will likely be built into the CA or RA software being used.

PKIs should consider these factors in documenting their procedures to validate revocation requests. The PKI's documentation should account for regulatory or contractual requirements placed on the PKI. CAs and RAs, then, should adhere to the PKI's documentation when validating revocation requests.

D.4.9.4 Procedure for Revocation Request

Issue Summary. This section concerns the procedure that a CA or RA would follow to process a revocation request and the outcome of that process.

Relevant Considerations. A CA or RA can establish an interface and procedures by which it gathers revocation requests from subscribers or other authorized participants, and can establish procedures to initiate revocation upon its own initiative. Once a CA or RA receives a revocation request or initiates a revocation procedure, the processing of the revocation may either be automated or manual. For instance, a revocation may be automatic when a CA system receives a properly signed revocation request, or a subscriber inputs a shared secret or biometric data to an interface designed to gather revocation requests. By contrast, where a subscriber communicates using out-of-band methods with a CA or RA, or a CA or RA must decide whether to initiate revocation, human judgment is involved and revocation processing necessarily must be manual.

Processing revocation requests may also include notifying a subscriber of the revocation. Such a procedure would provide confirmation to a subscriber trying to make sure that the revocation procedure succeeds. Moreover, when a CA or RA initiates revocation on its own initiative, notice to a subscriber may be the only indication that a subscriber has that the certificate has been revoked.

The CA may perform the act of revocation itself by publishing notice that a certificate has been revoked. Providing such notice through certificate revocation lists and other mechanisms may be the basis of a PKI's certificate status services. *See* PAG § D.4.10 (Certificate Status Services).

Assessors should determine which procedures for processing revocation requests are appropriate in light of the circumstances for revocation and the manner in which a CA or RA obtains revocation requests or initiates revocation upon its own initiative. They should also review the PKI's revocation processing procedures to determine their fit to the revocation practices of the PKI and account for any external requirements. Finally, assessors should determine whether or not CAs and RAs adhere to the revocation processing requirements and practices in the PKI's documentation.

Appropriate Requirements and Practices. Upon receipt of a subscriber's revocation request or request of another participant authorized to request revocation, a CA or RA will typically want to conduct validation procedures first to ensure that the request did in fact originate from the subscriber or other authorized person. In some cases, the RA initiates revocation upon its own initiative and instructs a CA to perform the revocation. In response to such instructions, a CA will want to validate that the instructions did, in fact, originate from the RA.

It may be helpful for a PKI simply to cross-reference the section of its documentation concerning validation of revocation requests when mentioning this step. *See* PAG § D.4.9.3 (Validation of a Revocation Request).

Following validation procedures, a CA will generally want to provide notice of the revocation to the subscriber for the reasons described under Relevant Considerations. The revocation process typically culminates in the CA (or service provider performing services on behalf of the CA) providing certificate status services to notify potential relying parties of the revocation.[342] Here again, it may not be necessary to detail certificate status services in the PKI documentation section corresponding to this PAG § D.4.9.4. Rather, the PKI may find it more efficient to cross-reference the section of its documentation relating to publication of certificate status information. *See* PAG § D.4.10 (Certificate Status Services).

In sum, the PKI should include within its documentation requirements or practices relating to the processing of revocation requests. These procedures should make sense in light of the way in which PKI participants request or initiate revocation and should account for any external regulatory or contractual requirements. Finally, the procedures established by CAs and RAs should adhere to the PKI's documentation.

D.4.9.5 Revocation timing

Issue Summary. This section specifies the time in which a subscriber, CA, or RA must or can submit a revocation request or revocation instruction to initiate a revocation following certain events. This section also can specify the time in which a, CA and/or RA would be required to process a certificate revocation request.

Relevant Considerations. Because the degree of trust that is accorded a certificate is based, in part on the degree of confidence of its continued reliability, prompt revocation of a certificate is usually important to a PKI. PKI rules that provide for prompt notification of compromise and prompt processing of revocation requests minimize losses that may arise from private key compromises and enhance the credibility of the entire PKI.

Assessors should review a PKI's documentation to determine its requirements relating to when a subscriber, CA, or RA must submit a revocation request and how much time a CA or RA has to process a revocation request or instruction. They should determine whether these time limits are appropriate within the PKI's business environment and are consistent with any regulatory or contractual requirements. Finally, they should determine whether or not PKI participants adhere to the timing requirements imposed in the PKI documentation.

Appropriate Requirements and Practices. In general, a PKI will want to require that subscribers request revocation promptly after circumstances requiring revocation arise. CAs should in turn process revocation requests and instructions in a timely fashion. A PKI should establish the time frame for performing revocation functions in a CP, a CPS and/or subscriber agreement. In general, timely revocation should be a function of the level of trust associated with the certificate, i.e., the higher the level of trust, the more rapid the revocation process.[343] The CA may suspend the certificate pending the authentication the revocation request if permitted by the CP/CPS. Some PKIs go a step further and require specific time periods, for instance requiring that subscribers notify an RA of private key compromise within a certain number of hours following discovery of the compromise in order to request revocation. The number of hours permitted the subscriber to report a compromise is generally inversely proportional to the assurance levels provided by the different types of certificates. The difficulty with setting a specific time period is the inherent arbitrariness of such time limits, and rigidity in the face of varying circumstances that may call for revocation. On the other hand, specific time periods avoid the vagueness inherent in imposing a standard of "promptness" or some similar expression.

[342] The CA may also want to provide specific notice to an RA or certificate sponsor that a revocation request has occurred or was successful. *See* PAG § D.4.3 (Certificate Issuance).

[343] PKI documentation could also specify the time at which the certificate is no longer valid (i.e., the effectiveness of the revocation). Alternative effective times may be immediately upon authentication of a revocation request or the time of actual publication to the CRL (or other accepted publication method).

It may be more realistic to set specific amounts of time in terms of the time in which a CA and/or RA must process a revocation request. As with certificate application processing, *see* PAG § D.4.2 (Certificate Application Processing), such time periods are frequently set forth in a service level agreement between a PKI service provider and a customer or entity delegating tasks to it. There are no standard sets of time associated with revocation processing tasks, although manual processes will take longer than automated ones. For the reasons explained in PAG § D.4.2, the best way to demark such time periods is usually as the time period between when the CA or RA receives a revocation request until the time the CA or RA completes its action in response to the request.

More generally, the PKI should pick time periods or standards that make sense in light of the applications secured by the certificates, the assurance levels provided by the certificates, and the manner in which CAs or RAs accept revocation requests. Whatever time periods or standards are appropriate should be reflected in the PKI's documentation, which should also account for regulatory or contractual requirements imposed on the PKI. Finally, PKI participants should adhere to the revocation time limitations set forth in the PKI's documentation.

D.4.9.6 Special requirements regarding key compromise

Issue Summary. This section provides any special requirements or procedures relating to revocation, in the event that a key compromise necessitated the revocation.

Relevant Considerations. There may be special requirements for a CA to immediately notify potential relying parties of a key compromise. One possibility is posting an interim certificate revocation list immediately upon revocation, as opposed to waiting to issue the next regularly-scheduled CRL. Another possibility is the dissemination of expedited communications to notify affected participants, communications using channels not normally used to provide notice of revocation, or communications of notice to recipients who do not normally receive such notice.

Assessors should determine whether any business or security needs or external requirements call for special revocation procedures following key compromise. They should determine whether any special requirements appear in the PKI's documentation. Finally, they should determine whether or not CAs and RAs actually follow any such special requirements following the compromise of a subscriber's private key.

Appropriate Requirements and Practices. If supported, special revocation procedural requirements applicable following a key compromise would likely be associated with certificates of a higher level of assurance. The choice of whether such procedures are required and which procedures are most appropriate will also depend on the application being secured by certificates, the business' need for rapid dissemination of notice, and the need for greater certainty in the case of compromise that relying parties will have actual notice of the revocation.

PKIs should adopt such special procedures only if they make sense in light of the need for security of the application. If such procedures are appropriate, the PKI should include them in its documentation, consistent with any external requirements in law or contract. Finally, CAs and RAs should in fact follow requirements in the PKI's documentation concerning special revocation procedures following compromise of the subscriber's private key.

D.4.9.7 Circumstances for suspension

Issue Summary. This section states the circumstances in which a certificate would be placed in suspended status.[344]

Relevant Considerations. Suspension of a certificate is the process by which a CA temporarily places the operational period of a certificate in abeyance for a specified time period. Certificate suspension is a mechanism/feature that can mitigate certain PKI risks but may introduce other risks. For example, certificate suspension can be invoked immediately when a revocation request has been received but not yet authenticated. Doing so may expedite notice to relying parties, mitigate a CA's liability for erroneous revocation, and eliminate the need (and associated costs) of certificate reissuance if it is ultimately determined that revocation would have been unnecessary or unwarranted. Suspension, however, may introduce greater uncertainty as to the precise status of a certificate, and also may create additional overhead and complexity in managing a suspension service.[345]

In some implementations, where an unauthenticated revocation request is received (such as an unsigned request or one where a pre-arranged passphrase is not presented), it may be useful to suspend a certificate until the revocation request can be validated. In other implementations, where a period of inactivity of a certificate is greater than 30 days, the certificate might be suspended pending confirmation of its good standing with the certificate's subject. Suspension may also serve the subscriber's needs when the certificate holder is on long term absence status (disability, vacation, temporary assignment, strike, etc.).

Some state statutes may require suspension in certain circumstances. For instance, under the Washington Authentication Act[346], the Secretary of State may order a licensed CA to suspend a certificate if, after notice and opportunity for a hearing, she determines that the certificate was issued without substantial compliance with the Act and the noncompliance poses a significant risk to persons relying on the certificate.

Significantly, certificate suspension is not supported in many technological environments in widescale deployment today. Thus, certificate revocation is much more common than support for suspension services. In such environments, the only way to respond to factors that might call for certificate suspension would either involve revocation of the certificate with the risk of inappropriate revocation, or doing the additional diligence involved with ensuring that revocation is appropriate.

Otherwise, the Relevant Considerations surrounding circumstances calling for suspension are largely the same as those calling for revocation, *see* PAG § D.4.9.1 (Circumstances for Revocation), except suspension may involve additional considerations of uncertainty relating to the factors underlying the suspension and the possible temporary nature of such factors.

Appropriate Requirements and Practices. A certificate may be placed in suspended status following an unsigned request for certificate revocation, pending authentication of the revocation request. Furthermore, the Appropriate Requirements and Practices applicable to circumstances for revocation, *see* PAG § D.4.9.1, apply here as well. Suspension is sometimes preferable to revocation in instances where there is uncertainty concerning the facts surrounding the motivating factors for suspension. In addition, if such factors are merely

[344] A suspended certificate is not placed on a CRL. For those systems that support certificate suspension, an entry is made in the CA's certificate database that the certificate has been suspended. The CA's response to any certificate status queries made while the certificate is suspended would be either "suspended" or "temporarily revoked."

[345] One problem with certificate suspension is that it may send an ambiguous message to the relying party, i.e., the certificate might be valid or it might be invalid. Knowing that a certificate is suspended may cause the relying party to seek and/or obtain the assurance it needs to proceed with the transaction. By relying on a suspended certificate, however, the relying party might be deemed to have waived its rights to rely on the digital signature against the CA or the subscriber. In any case, a PKI may wish to explain the significance of suspension in its documentation and how suspension should be treated in a variety of circumstances.

[346] *See* Washington Authentication Act, *supra* note 82, § 19.34.210(7).

temporary, and the certificate will once again be reliable following the termination of such temporary factors, it may be preferable to suspend the certificate, rather than to revoke it.

D.4.9.8 Who can request suspension

Issue Summary. This section identifies who is allowed to make a suspension request.

Relevant Considerations. The PKI might allow suspension to be made by the subscriber, a representative of the subscriber, the applicable CA, the applicable RA, or any other person authorized within the PKI. In many PKIs, a revocation request from an unauthenticated person might be treated as a suspension request. The considerations involved with identifying who can request suspension are largely the same as those involved with choosing who can request revocation. *See* PAG § D.4.9.2 (Who Can Request Revocation).

Appropriate Requirements and Practices. The Appropriate Requirements and Practices concerning the persons who may request or initiate suspension of a certificate are largely the same as the Appropriate Requirements and Practices relating to those persons authorized to request revocation under PAG § D.4.9.2.

D.4.9.9 Validation of a Suspension Request

Issue Summary. This section describes the information needed, and the process used, to decide whether or not a request or an instruction to suspend a certificate has, in fact, originated from a person authorized to request or initiate suspension.

Relevant Considerations. Validation of a suspension request is the process by which a CA or RA ensures that a request or initiation of suspension has, in fact, originated from a person authorized to submit the request or to initiate the revocation. The possible mechanisms used to validate a suspension request are potentially the same as those that can be used to validate revocation requests, and the Relevant Considerations are largely the same. *See* PAG § D.4.9.3 (Validation of a Revocation Request).

The need for trustworthiness relating to the validation of suspension requests, however, is lower than the need for assurances in validating revocation requests. Suspension of a certificate, unlike revocation, is a reversible process. A CA can end the suspension of a certificate if the CA or RA discovers that the suspension request was unauthorized or unwarranted. By contrast, revocation cannot be reversed.

Appropriate Requirements and Practices. A CA should have some evidence to document a suspension request even though the quantum of evidence necessary to authenticate a suspension will generally be much less than for revocation. Ssuspension occurs where the subscriber has not yet been fully authenticated; otherwise the certificate could simply be revoked. Thus, the validation of a suspension request will not require the rigor involved with procedures or criteria other than those used for revocation, although the types of procedures may overlap. Otherwise, the Appropriate Requirements and Practices of PAG § D.4.9.3 (Validation of a Revocation Request) apply here as well.

D.4.9.10 Procedure for suspension request

Issue Summary. This section describes the procedures by which a CA or RA processes a request to suspend the certificate and the outcome of that process.

Relevant Considerations. As with revocation, a CA or RA capable of providing suspension services can establish an interface and procedures by which it gathers suspension requests from subscribers or other authorized participants, and can establish procedures to initiate suspension upon its own initiative.

In general, the procedures involved with processing a suspension request are the same as processing a revocation request: some effort is made to validate the suspension request or instructions, the CA either suspends or declines to suspend the certificate in an automated or manual fashion, the subscriber may be notified of the suspension, and notice of the suspension is published. *See* PAG § D.4.10 (Certificate Status Services). The Relevant Considerations are largely the same as those involved with processing revocation requests, *see* PAG § D.4.9.4 (Procedure for Revocation Request), except where suspension occurs because the CA intends to revoke the certificate but does not have enough of a basis to do so. In this case, after the CA or RA has suspended a certificate, it proceeds with additional investigation to determine whether or not the certificate should be revoked. Suspension services also involve procedures that terminate the suspension and restart the certificate's operational period.

Appropriate Requirements and Practices. Suspension procedures will depend on how certificates are used within the PKI and the technology that supports suspension. Upon suspending a certificate, the CA or RA will likely want to promptly notify the subscriber of the suspension and provide an opportunity to terminate the suspension, thereby reinstating the operational status of the subscriber's certificate. Otherwise, the Appropriate Requirements and Practices involving revocation procedures apply here as well. *See* PAG § D.4.9.4 (Procedure for Revocation Request).

D.4.9.11 Limits on suspension period

Issue Summary. This section defines the limits to period of time in which a certificate may remain suspended so that the certificate does not remain indefinitely in a suspended state.

Relevant Considerations. There may be a need to limit the duration of the suspension period to some predetermined maximum, not to exceed the remaining validity period of the certificate. The duration of the suspension period and how the certificate is treated at the end of the suspension period will depend on how the certificate is being used within the PKI.

Assessors should determine whether there is a business need or any externally-imposed requirements for a limit on suspension periods. They should also determine whether the PKI's documentation addresses this issue. Finally, assessors should ascertain whether CA systems enforce any limitations on suspension periods, consistent with the PKI's documentation.

Appropriate Requirements and Practices. Where a suspension occurs due to inability to authenticate immediately a revocation request, the suspension period should not generally exceed the time required to complete the authentication, e.g., the suspension period of a certificate shall be no longer than 120 days. The CP or CPS should specify whether the certificate should be revoked or reinstated at the end of the suspension period if the certificate remains suspended at the end of the suspension period.

Otherwise, the suspension period limitations should meet the business and security needs of the application being secured by the certificates. The limits should be consistent with any regulatory or contractual requirements. Finally, these limitations should appear in the PKI's documentation, and CA systems should enforce the documented limits.

D.4.10 CERTIFICATE STATUS SERVICES

Issue Statement. This section states the requirements imposed on CAs to provide certificate status information, or the CA's practices relating to making certificate status information available. In the event the CA has delegated such tasks to another PKI service providers who provide certificate status services, this section addresses the requirements on or practices of such providers.

Relevant Considerations. A core feature of many PKIs is the ability of certificate users to check the validity of certificates. This service could be implemented by several means including: touch-tone telephone response; issuance, publication and distribution of X.509 certificate revocation lists; or on-line response systems such as OCSP, described in more detail in the sections below.

An assessor should review the operational policies and practices of the certificate status service provider and ensure the proper operation and availability of an effectively implemented status response system. Assessors should review the PKI's documentation to determine requirements or practices involving participants' certificate status services. Finally, they should determine whether documented procedures are consistent with external requirements, such as those imposed by applicable law or contract.

Appropriate Requirements and Practices. If implemented, a certificate status service must, at a minimum, provide accessible informaiton to tell a potential relying party whether or not a given certificate is currently operational, subject to possible latency. *See* PAG § D.4.9.7.1.2 (CRL latency). The choice among which types of certificate status services to provide will depend on the business needs of the application being secured by certificates, specifically the extent of the need for up-to-date information, the technological environment used by or available to the PKI, and the assurance levels provided by the certificates.

A PKI should require or use certificate status services that make sense under its business model, consistent with any regulatory or contractual external requirements. The available certificate status services and requirements surrounding their use should be documented in the PKI's documentation. Finally, PKI participants should make certificate status services available and should use such services in accordance with the PKI's documentation.

D.4.10.1 Certificate Revocation Lists

Issue Summary. This section contains information about certificate revocation list issuance frequency, time to publish a new CRL after certificate revocation (CRL latency), and other information relevant to the issuance of CRLs.

Relevant Considerations. A CRL is a digitally signed list of revoked certificates' serial numbers that is generally issued by the CA that issued the (revoked) certificate. The assessor should review the transactional and security risks that the implementation of PKI is attempting to address. In other words, what assets will be exposed to loss if a subscriber's key compromise is not quickly communicated to a relying party who enables the loss? For example, PKI-enabled systems can serve purposes as simple as access control to information of marginal value, or to the movement of millions of dollars. Also, relying party systems are often designed to cache a copy of CRLs and to use those copies until the date that the next CRL is expected to be issued. The design of a CRL caching system used by a relying party should be carefully reviewed to ensure that the relying party does not unwittingly rely on a revoked certificate.

Appropriate Requirements and Practices. A PKI service provider's CRL-publishing duties (i.e., periodicity and latency requirements) should be commensurate with the value of the transactions taking place within the PKI. Issuing CAs should generally publish CRLs on a regular basis to ensure that relying parties are provided timely information regarding certificate revocation. CAs will likely want to remove superseded CRLs from the directory system upon posting of the latest CRL. If a CRL is being issued as a result of a key compromise or revocation, the CA will want to post such a CRL as quickly as feasible. A PKI's documentation should generally include the details of certificate revocation list posting, and an explanation of the consequences of using dated revocation information.

D.4.10.1.1 CRL issuance frequency

Issue Summary. This section states the frequency with which a CA (or CMA or repository service provider, on behalf of a CA) issues CRLs.

Relevant Considerations. CRLs provide information regarding a certificate's status. CRLs are issued periodically and downloaded to relying party systems on a scheduled basis, e.g., every 24 hours. CRLs contain an issue date as well as the date that the next CRL should be issued. The frequency of CRL issuance tends to reflect the risks and assurances associated with the certificates. In some cases, unscheduled "interim" or "delta" CRLs may be issued, particularly in the event of key compromises.

Appropriate Requirements and Practices. A PKI should document the frequency of CRL issuance within its documentation. CRLs may be issued more frequently than required. If there are circumstances under which the Issuing CA will post early updates, these shall be spelled out in a PKI's documentation. It may also be helpful to document practices surrounding the time limits within which interim CRLs are published.

D.4.10.1.2 CRL latency

Issue Summary. This section describes how the PKI handles issues associated with CRL latency.

Relevant Considerations. CRLs have an inherent latency period associated with them. Figure D-2, below, presents the timeline of a CRL revocation scenario.

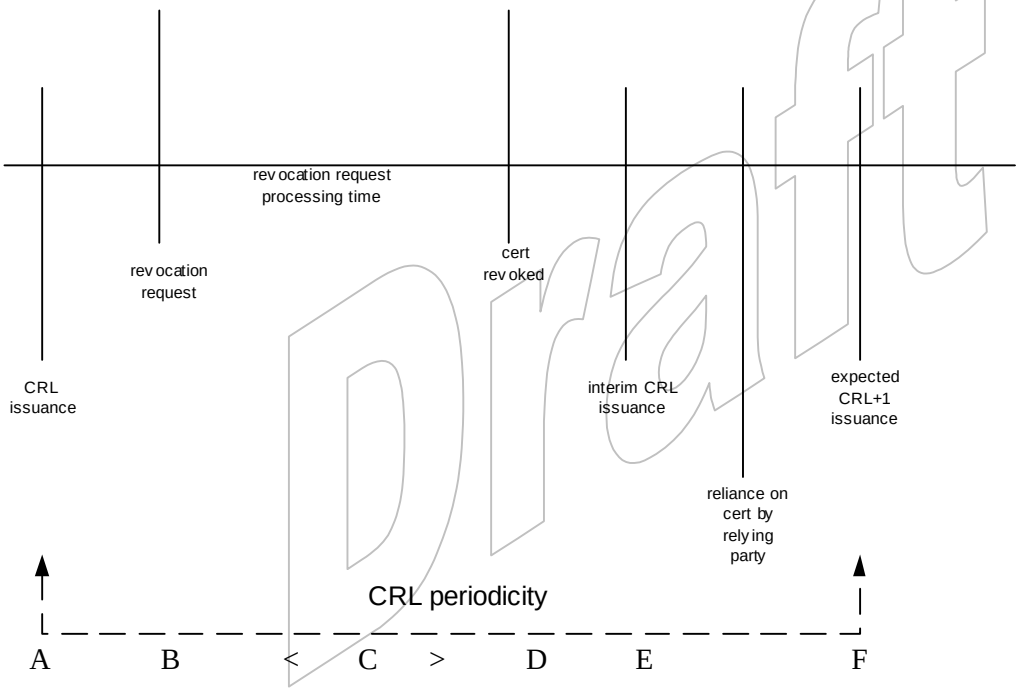


Figure D-2

This scenario, typical of many implemented PKIs, presents a framework to describe many of the latency limitations of CRL systems and responsive approaches to mitigate the risks. A CRL is issued at a point in time (point "A"). At some time after that CRL is issued, a subscriber requests that his certificate be revoked (point "B"). Time is needed to process the revocation request, for example to authenticate the request for revocation, (time period "C"). Later, the CA determines that the certificate should be revoked (point "D"). However, the next regularly scheduled CRL is not scheduled for issuance until much later (at point "F").

Depending upon the applicable PKI documented requirements or practices, the CA may issue an "interim" CRL that includes this newly revoked certificate (at point "E"). CRLs can be partitioned so that separate CRLs are issued for particular reasons; and interim CRLs may be issued that are limited to a single reason, such as key compromise.

Some relying parties that query CRLs from cached copies of the current regular CRL may not necessarily check (or check timely) for a new CRL (particularly where the cached copy is controlled by a third party, such as a

local system administrator), because the next issue date has not yet been reached. Relying parties may be required to check for an interim CRL before relying on a certificate. Interim CRLs may be "pushed" to qualified relying parties. Relying parties may decide, based on the nature (risks/importance) of the transaction or application, whether it is necessary to check for an interim CRL.

Appropriate Requirements and Practices. The extent of the CRL latency period, as well as material aspects of the entire revocation process should be addressed by a PKI's documentation, perhaps especially in a CPS and relying party agreement. CRL latency should reflect the requirements for the secured application (and should not exceed the time period necessary to assure that application's proper operation). Considerations affecting the time period permitted to process a revocation request, the circumstances under which an interim CRLs may be issued, and the obligations of relying parties to check for interim CRLs should also be addressed. *See supra* PAG § D.4.9.5 (Revocation Timing).

On publication of an interim CRL, the CA signing the CRL may want to send or push the interim CRL to all qualified relying parties. Moreover, a PKI may want to place a duty on relying parties to check for an interim CRL prior to relying on a certificate.[347] The CA will typically include a revoked certificate on the next CRL, perhaps even if the certificate has expired prior to the date of that next CRL. (A relying party might check the CRL to see if the certificate was revoked prior to its expiration, and also record of revocation should be maintained on at least one CRL as a record of its revocation for archival purposes.)

D.4.10.2 On-line revocation/status checking

Issue Summary. This section discusses whether a PKI requires or uses online revocation checking mechanisms, such as OCSP or a web site at which relying parties can submit http-based inquiries regarding certificate status.

Relevant Considerations. On-line mechanisms are capable of communicating the current (real-time or near real-time) status of a certificate. These mechanisms eliminate latency issues affecting CRLs, although they may introduce other risks (certificate status responder and Internet connection downtime). The predominant on-line revocation/status checking mechanism is the IETF *On-line Certificate Status Protocol* ("OCSP").[348] OCSP provides a standardized protocol for on-line status requests for specific certificates. Upon request, an OCSP "responder" provides a signed status response message that reflects the current status of the certificate. The responder's signature can be verified by the relying party.

The timeliness of any certificate status information depends on the implementation. Some OCSP responders are merely front-ends for CRL-based revocation systems or base their response on the most current operational records of the CA. In these cases an OCSP response will not contain more current information than the CRLs. In other words, a revocation system that involves updating CRLs immediately upon revocation request validation, with applications pulling a CRL for each certificate validation (i.e., no caching) is equivalent to an OCSP-based system.

Relying parties may need to retain OCSP responses used to verify signatures, since each response is unique to a particular transaction. OCSP is only one of many types of on-line checking mechanisms.

---

[347] *Cf.*, *see* UETA, *supra* note 15, § 10(1), which provides: "[i]f the parties have agreed to use a security procedure to detect changes or errors and one party has conformed to the procedure, but the other party has not, and the nonconforming party would have detected the change or error had that party also conformed, the conforming party may avoid the effect of the changed or erroneous electronic record".

[348] *See* PAG APP 2 (*Internet X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP),* RFC 2560, Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C., IETF, *available at* <http://www.ietf.org/rfc/rfc.2560.txt>, hereinafter "RFC 2560").

Appropriate Requirements and Practices. Whether a PKI requires or uses an on-line certificate status checking mechanism will depend on the business need for up-to-date information, the applications being secured by the certificates, and the assurance levels provided by the certificates. If the certificates are securing applications involving large-value transactions, then there is a relatively great business need for recent status information, and the risks inherent in the latency of CRLs are rather large. On-line status checking mechanisms are appropriate for such environments. By contrast, where the certificates are securing applications involving low-risk transactions, the PKI may not need or want to incur the expense and effort involved with maintaining on-line mechanisms to check certificate status.

D.4.11 TIME-STAMPING SERVICES

Issue Summary. This section states the requirements for PKI service providers who provide time-stamping services.

Relevant Considerations. A time-stamping service generally provides a strong and verifiable cryptographic statement that a specific digital record existed at a specific moment in time. Time-stamping a digital record provides the relevant parties with a verifiable statement of when the digital record was known to exist. Time-stamping a digitally-signed record can further provide the relevant parties with a verifiable statement that the digital record was signed while the signing certificate was valid, e.g., that the signature was formed before the expiration date of the signing certificate. Time-stamping certificate revocation lists and other revocation data corresponding to a signing certificate provides the relevant parties with additional assurances that the signing certificate was not revoked at the time of signing. Time-stamping services thus provide the technical basis for general nonrepudiation services, and for both Common Law- and Latin-derived notarial services.

Assessors should determine whether there is a business need for time-stamping services in relation to a particular application. If so, they should review a PKI's documentation to determine whether it specifies requirements or practices relating to time-stamping and whether they are consistent with applicable regulatory and contractual requirements imposed externally. Finally, assessors should determine whether or not PKI participants are following the time-stamping requirements and practices set forth in the PKI's documentation.

Appropriate Requirements and Practices. The time-stamping service provider will not want to be a party to the time-stamping transaction in question in order to retain its trusted third or fourth party status. The time-stamping service provider only signifies that the digital record existed at a specific moment in time. The time-stamping service will likely want to provide a strong, verifiable cryptographic link between the assigned time value and the digital record. The source and accuracy of the assigned time value should be defined by the operational policy of the time-stamping service. Time-stamping providers may find it helpful to make use of the stable, recognized National Timing Standard as a trusted time source.

A PKI's decision to augment its services with time-stamping services will depend on whether there is a business need for noting the time of transactions in a secure fashion or for confirming the verification of a signature on a transaction at a time certain. Certain applications that are particularly time-sensitive or call for a trail of documentation that includes a time stamp may require such services. If time-stamping services are appropriate for a given environment, the PKI should include time-stamping requirements and practices in its documentation, subject to any requirements imposed by law or contract. Finally, PKI participants should make use of time-stamping services, and time-stamping service providers should meet the time-stamping requirements set forth in the PKI's documentation.

D.4.12 PRIVATE KEY RECOVERY[349]

D.4.12.1 Circumstances for private key recovery

Issue Summary. This section contains circumstances under which recovery of an escrowed or managed private key is appropriate.

Relevant Considerations. Private keys used for confidentiality purposes (encryption) are sometimes escrowed or archived by PKI service providers to respond to requests from subscriber organizations, subscribers, or subscriber designees to obtain the decryption key to gain access to encrypted data. This is called key recovery and this section discusses the circumstances under which the parties may want to or be required to recover escrowed private keys. In order to provide key recovery services, the PKI service provider may store activation data or the decryption key itself. The design and implementation of a storage and retrieval process will usually be specific to the PKI service provider and may involve a combination of chain-of-custody, dual control, split-knowledge (*see e.g.*, PAG § D.5.2.2 (Number of Persons Required Per Task)), encryption and other techniques by the parties involved to provide procedural protections for the private key.

Private key recovery presents the security risks of unauthorized access to the private key, which can be used to decrypt sensitive information. In the case of single key pair schemes, where one key services for both signature creation and decryption purposes, there may be reasons for escrowing or managing the single key. When such systems are used, unauthorized access to a private key also entails the risk that an attacker could create digital signatures using the recovered key and thereby impersonate the subscriber. The technical security controls involved with private key escrow are discussed in PAG § D.6.2.3 (Private key escrow).

Consequently, there is a business need to limit the circumstances under which a private key can be recovered and also control access to the private keys to prevent unauthorized private key recoveries. *See* PAG § D.4.12.3 (Procedure for Private Key Recovery)). Circumstances under which recovery is appropriate or required generally fall into two categories: voluntary requests from the subscriber and requests for a subscriber's private key that originate from another responsible and authorized party, which are likely to be involuntary from the perspective of the subscriber.

When key escrow or management is used within a PKI, assessors should determine, based on the context in which certificates are used, which circumstances warrant key recovery. Assessors will likely need to delve into requirements that may arise from applicable law or judicial or administrative process. Judicial and administrative processes may include search warrants and subpoenas in criminal action, and in the civil context, requests for production propounded to a litigant or subpoenas presented to a non-party. Assessors should review the PKI's documentation to determine what it says about appropriate key recovery circumstances and whether it is consistent with these requirements. Finally, assessors may want to determine whether PKI participants have responded appropriately in the past to key recovery requests, in accordance with the PKI's documentation.

Appropriate Requirements and Practices. The reasons typically supporting a request for key recovery are:

- Loss or corruption of the private key,
- Death or disability of the subscriber,
- Termination of employment or affiliation,
- Suspected fraud or other wrongdoing of the subscriber, where the entity escrowing the key has a right to conduct an investigation of the subscriber's conduct,

[349] *See* CIMS Level 3, *supra* note 325, § 2.1 (describes a separate protection profile effort for key recovery system).

- A request from law enforcement officials or prosecutors,
- A request from a litigant in a civil action, and
- A request from regulators in an administrative action.

In general, the circumstances in which key recovery are appropriate or required should match the purpose of the key escrow systems and should be consistent with any applicable requirements imposed by applicable law or contract to divulge the key. The PKI should place circumstances for key recovery in its documentation and PKI participants should adhere to it.

D.4.12.2 Who can request private key recovery

Issue Summary. This section establishes who can request recovery of a private key.

Relevant Considerations. Assessors should consider who should be entitled to request private key recovery in light of the circumstances that provide the basis for a private key recovery. Assessors should then review a PKI's documentation to determine whether parties permitted to request recovery are appropriate under the business needs of the PKI and under requirements imposed by applicable law and contract. Finally, assessors should determine whether, in fact, the recovery practices of a PKI service provider do permit persons to request recovery of a private key when authorized to do so under a PKI's documentation.

Appropriate Requirements and Practices. A subscriber may allow a PKI service provider to back-up, archive or escrow (i.e., *store*) his or her private decryption key for key recovery purposes. The PKI service provider should give the subscriber notice of who may request, and under what circumstances, a key recovery. The identity of participants that can request recovery of a private key will depend on the circumstances leading to the recovery. *See* PAG § D.4.12.1 (Circumstances for private key recovery). In particular:

- Where recovery is appropriate merely because of loss or corruption of the private key, the subscriber is typically the participant seeking its recovery in order to resume use of the applications making use of the private key.
- Where recovery occurs because of the death or disability of the subscriber, the CA, RA, and/or organization sponsoring the certificate may be entitled to request recovery.
- Where recovery is based on the termination of the subscriber or the subscriber's affiliation, the CA, RA, and/or sponsoring organization may be entitled to request recovery.
- Where the recovery is based on investigation of fraud or other wrongdoing of a subscriber, the CA, RA, and/or sponsoring organization may be entitled to request recovery,
- In the case of search warrants and subpoenas in a criminal action, a law enforcement official or prosecutor may be entitled to request recovery,
- In the case of discovery requests in a civil action, the requesting litigation may be entitled to request recovery under the applicable statutes and rules of civil procedure, and
- In the case of an administrative subpoena originating from a regulatory body, the relevant regulators may be entitled to request private key recovery.

Generally, PKIs will want to ensure that the right persons are able to obtain access to private keys, without unnecessarily affording access where it is not warranted, or provide unauthorized access. The persons permitted to request recovery should be documented within the PKI's documentation, which should adhere to all

applicable laws and contractual requirements relating to search warrants and judicial and administrative process. Finally, CAs and other parties with access to private keys should abide by the requirements and practices set forth in the PKI's documentation relating to providing access to escrowed private keys, subject to the requirements of applicable law.

D.4.12.3 Procedure for Private Key Recovery Request

Issue Summary. This section describes the process for requesting and performing a key recovery.

Relevant Considerations. As with the previous section, the way in which requests for key recovery are processed will depend on the circumstances under which key recovery is appropriate. In general, requests will either be voluntary on the part of the subscriber or will be involuntary from the subscriber's perspective. Voluntary recoveries may be quite routine, and the most common case involves the subscriber's inadvertent loss or corruption of the private key. In theory, a subscriber may request a recovery because judicial or administrative process is served on the subscriber, and the subscriber is attempting to comply. As to the PKI service provider escrowing the key, such a request is voluntary because it is originating from the subscriber, but the law compels such compliance. In any case, the fact that the subscriber is originating such a request means that the PKI service provider likely has no obligation to afford the subscriber an opportunity to seek a protective order or other relief, or assist the subscriber in seeking such relief.

Key recoveries that are involuntary from the subscriber's perspective may entail complicated legal consequences. The conduct of a company investigating the subscriber may implicate the privacy interests of the subscriber. Moreover, when a PKI service provider escrowing private keys receives a recovery based on judicial or administrative process, the provider may desire or have an obligation under contract to resist the disclosure of the private key to the requesting party until the subscriber has had an opportunity to seek a protective order or other relief under the applicable procedural rules.

Assessors should determine which procedures for permitting private key recoveries are suitable under the various scenarios of key recovery. They should review the PKI's documentation to determine whether the PKI has accounted for these scenarios and has established suitable procedures that are consistent with requirements imposed by law or contract. Finally, assessors should determine whether PKI service providers escrowing keys are conforming to the procedures in the PKI's documentation when they recover private keys.

Appropriate Requirements and Practices. The PKI service provider holding private keys will want to implement procedures to ensure that the stored private key is disclosed only under the circumstances authorized. PKIs will likely find it critical to establish a requirement that PKI participants define their key recovery policy after considering the various scenarios for circumstances under which key recovery may occur. The roles and responsibilities of the involved parties should be clearly explained and communicated in advance. Appropriate notice should be given at time of key recovery.

When confronted with a request for key recovery, the service provider escrowing the keys will want to validate the request. In the case of subscriber-generated requests, the provider will want to ensure that it did in fact come from the subscriber. In the case of other requests, the provider will want to establish who originated the request, and whether the requesting party has the authority to obtain the private key.

Following validation, the provider may want to take some time to evaluate the request and take other steps deemed necessary before simply disclosing the key. It is during this time, for instance, where a provider may desire or have an obligation to resist disclosure of a key in order to afford the subscriber an opportunity to seek a protective order from disclosure.

Once a decision has been made to recover the key, the provider will then use its key recovery systems to obtain the key. In the case of subscriber-generated requests, the provider will likely want to provide the private key to the subscriber in a secure fashion. In the case of other requests, the provider will want to secure the key and

provide it to the requesting party. The extent of the security involved with the transfer of the private key will be commensurate with the assurance level of the certificate containing the public key corresponding to the recovered private key and the need for security in the applications secured by the certificate.

The PKI should document its requirements and practices relating to the procedures for requesting and obtaining escrowed or managed private keys. These requirements and practices should be consistent with applicable law and any contractual requirements. Finally, PKI service providers should adhere to these requirements and practices when operating their key escrow or management systems.

D.5 Management, Operational and Physical Security Controls

This section presents the physical security, personnel security, and operational controls used in whole or in part by a PKI to provide trustworthiness in the operations of PKI participants.

D.5.1 PHYSICAL CONTROLS

D.5.1.1 Physical Security controls for CAs and relevant trusted service providers

Issue Summary. This section relates to the physical controls required of or used by CAs. Since CMAs host CA systems on behalf of CAs, this section also applies to CMAs, to the extent CAs utilize them. A PKI may also use this section to discuss physical security controls for other relevant Trusted Service Providers.

Relevant Considerations. The physical controls for a CA or relevant Trusted Service Provider (collectively referred to in this section as "CA") can range dramatically in complexity, cost, and corresponding effectiveness. Physical controls provide a unique and essential set of protections against the risks of cryptographic key loss, theft, and abuse. Furthermore, because logical controls alone are not capable of providing strong protection of cryptographic keys, physical controls of trusted systems demand attention. Other threats include break-ins, natural disasters, fires, failure of supporting telecommunications or power utilities, structural collapse, water intrusion through floods or plumbing leaks.[350] In terms of the planning and the design of the site and location of a PKI participant, the participant can create a secure facility that includes high security zones where sensitive CA and RA lifecycle services can occur; such as CA or subscriber key generation, certificate generation, private key storage, and revocation management.[351] PKI participants can design their facilities to create defined security perimeters, *i.e.* physical barriers,[352] around the areas where these sensitive functions take place. These barriers, sometimes called physical security "tiers" or "layers," can consist of walls, locked doors, cages, cabinets, safes, locked drawers, and the like. A CA can use various types of barriers alone or in combination.

A physical security tier is a combination of barriers that cannot be circumvented and creates a protected area in which sensitive processes can take place. Preventing circumvention means that an intruder should not be able to go around, climb over, or crawl under a barrier. That is, the barrier should provide complete protection from intrusion and should not present any unprotected openings.[353] Physical security tiers can be nested so that one

[350] *See* ETSI Standard, *supra* note 317, § 7.4.4(f).

[351] *Id.*, § 7.4.4(d).

[352] *Id.*, § 7.4.4(e).

[353] For example, a room with a partial wall that does not reach the ceiling, a room with a locked door at one end but an unlocked door at the other end, and a metal cage covering the top of a raised wooden platform with a thin, weak, and exposed bottom cannot comprise effective security tiers. In the first example, an intruder could climb over the partial wall. In the second example, an intruder could go around the locked door by entering into the unlocked back door. In the third example, an intruder could go underneath the platform, saw through its floor, and thus circumvent the cage.

fits completely within the next-most tier. Thus, a safe located within a locked room creates two physical security tiers of protection; the locked room would constitute tier 1 and the safe tier 2. The use of nested tiers means that the facility can be divided into zones, and those zones within higher (inner) tiers of security can be designated as high security zones. A PKI's documentation can then identify which tiers or zones within a facility should house the systems and personnel performing specified CA or RA functions.

Assessors should consider the various physical threats to a CA's facilities and consider which physical security controls make sense in light of the security needs of the PKI and the assurance levels provided by the certificates. They should determine whether any external regulatory or contractual requirements bear on CAs' secure facilities. Finally, they should determine whether CAs facilities meet the standards and practices set forth in the PKI's documentation.

Appropriate Requirements and Practices. The physical controls implemented should be commensurate with the attendant risks of compromise and the assurance levels provided by the certificates. Controls may be documented in the form of lists of construction parameters and security features, such as wall thicknesses, the presence of cameras, the use of fire suppression equipment, and so on. Protection against break-ins may also be expressed in terms of numbers of physical security tiers or the placement of critical functions and assets in high security zones. It may be helpful for a PKI to speak in general terms in published documents, and document detailed lists of construction parameters and security features in internal documents. Such lists tend to be highly sensitive and PKIs will want to avoid publication of information that could assist attackers.

For moderate to higher trust CAs, many of the following physical security controls are typically implemented:

- **Site location and construction.** The CA facility can be constructed with double or triple layer, floor-to-ceiling walls located in an area of the facility without windows or where windows can be secured effectively.

- **Physical access**. Access to the CA facility can be restricted to authorized personnel or escorted visitors who are onsite with reason to have access. Access to the CA server, software, and hardware is limited to those personnel performing duties specific to operating and managing the CA. Maintenance and service personnel are escorted and supervised.[354]

- **Secure Entry Point.** Access to the CA secure facility can be limited so that access is permitted only through a secure entry point using an access control list, and is monitored 24 hours a day, seven days a week by a security staff, or by other procedural or electronic means.

- **Power and air conditioning.** The CA facility can be equipped with an uninterruptible power supply (UPS) or generators to ensure a continuous supply of power and air conditioning for a predetermined period of time.

- **Water exposure.** The CA facility can be located such that the systems within are protected from water exposure. The facility may also be able to install equipment that can sense flooding and trigger an alarm.

- **Fire prevention and protection.** The CA facility can be equipped with heat and smoke detectors, alarms, and a fire suppression system appropriate for computer equipment.

[354] *See, e.g.*, Canadian Security Standards, *supra* note 290, p. 11.

- **Media storage.** The CA can ensure that storage media used by the CA system is protected from environmental threats such as extreme temperatures, humidity, and magnetism. The CA may want to adhere to standards[355] regarding exposure.

- **Waste disposal.** Information on media used for the storage of information such as keys, activation data, or CA files can be deleted securely or destroyed before released for disposal. The CA can establish procedures for waste disposal of sensitive CA operational data to maintain integrity and confidentiality.

- **Automatic Status Monitoring.** The CA facility and systems can be equipped to monitor system operation; to detect abnormal conditions, abnormal processing time, or service interruption; and to alert relevant personnel in the event of an abnormality.

- **Video and other surveillance equipment.** The ability to properly reconstruct what occurred during a breach can be very valuable. If it is necessary to prosecute criminals and/or assert a civil claim for tortious conduct, video records can provide crucial evidence of what occurred. A video surveillance set up, covert or in plain sight, can help also help to deter wrongful activity. Placement and careful operation of a video recording installation can be worth the expense depending on the risk levels involved.

PKIs should document whatever CA physical security requirements and practices are suitable in light of the security needs of the application being secured by certificates and the assurance levels that the certificates provide. These requirements and practices should account for any regulatory or contractual requirements. CAs should, in fact, implement the controls set forth in the PKI's documentation.

D.5.1.2 Physical Security Controls for RAs

Issue Summary. This section concerns physical security controls required for or used by RAs.

Relevant Considerations. The extent of physical security protections will vary greatly depending upon many factors, as noted above. *See generally* PAG § D.5.1.1 (Physical Security controls for CAs and relevant service providers). Some differences exist, however, between CA physical security and RA physical security. For instance, a CA or facility hosting CAs will have the critical CA private keys in online or offline cryptographic modules, databases of certificates and enrollment information, repository systems, and systems that perform RA functions. RAs, however, will only have systems that perform RA functions, which involve the use of less sensitive RA or RA administrators' private keys stored in.

Although the demands for physical security may be lower in RA facilities than CA facilities, assessors should nonetheless determine the extent to which RA facilities should be secured and compare it to requirements and practices in the PKI's documentation. They should determine if any regulatory or contractual requirements bear on RAs' facilities. Lastly, they should determine whether RAs' facilities do, in fact, implement the controls in the PKI's documentation.

Appropriate Requirements and Practices. The following practices may or may not be implemented, depending upon the assurance level of the certificate and the business' need for security:

- Where considerable public and personnel traffic is anticipated, RA services should be provided in an area that includes a reception area accessible to the public, but which restricts to authorized personnel access to the RA workstations and related sensitive data and devices.[356]

[355] *See, e.g.*, PAG APP 2 (*Care and Handling of Computer Magnetic Storage Media*, NBS Special Publ. No. 500-101, pp. 37 – 52, herinafter "NBS Special Publ") or (*Preserving Digital Information*, chap. 4, ISBN 1-55570-353-4 (2000), pp 53-60, hereinafter "ISBN").

- RAs should maintain possession and control of private keys or keep them in locked containers when the RA equipment is not in use.
- RA equipment should be located in a secure area protected from theft by security personnel or electronic monitoring devices.
- Activity in the overall area should be monitored by the authorized personnel or by security staff.
- Access by the public to the overall area may be limited to specific times of day or for specific reasons, as determined by the jurisdiction or CA domain.
- Maintenance and service personnel are escorted and supervised.

In addition, PKIs may find it appropriate to require the use of some or all of the construction specifications described in PAG § D.5.1.1, although the need for security at an RA facility is likely lower than the need for security at a CA facility. The differences in security may manifest themselves in terms of less extensive requirements (*e.g.*, fewer physical security tiers), omitting certain security features (*e.g.*, not requiring backup power generation capabilities), and a difference in focus. CA facilities are potentially the location of all certificate lifecycle services, possibly including validation, while RA facilities are focused on the validation functions. CAs need to be concerned with the theft of CA keying material, while RAs may focus more on prevent unauthorized use of RA systems to perform unauthorized application approvals or revocations and unauthorized disclosure of personally-identifiable certificate application information. For example, the physical security of some RA environments may consist of nothing more than protecting the RA administrator's workstation and preventing passers-by from performing unauthorized functions or seeing private information on or around the administrator's workstation.

Generally, PKIs should require or adopt RA physical security controls that are commensurate with the assurance levels of the certificates and the need for security in the applications being secured by certificates. The PKI should document these controls and ensure that they are consistent with external requirements. Finally, RAs should, in fact, adhere to the control requirements and practices established in the PKI's documentation.

D.5.1.3 Physical Security Controls for Subscribers

Issue Summary. This section discusses the extent of physical security controls required for or used by end-user subscribers.

Relevant Considerations. The primary concerns relating to subscriber physical security controls involve the protection of the subscriber's private key through security of the subscriber's workstation and the security of any token holding the private key. The approach and extent of successfully requiring and enforcing physical security controls on subscribers depends upon various factors, including the relationship between the subscribers and the PKI (such as whether the subscribers are employees, contractors or customers), and the business and regulatory demands/practices associated with the particular applications undertaken by the subscribers. The approach to physical security controls for subscribers can range from the physical isolation of the computing base/cryptomodule from third party access (such as locking it in a cabinet), to the use of a range of physical tokens (including smart cards) to enhance the strength of access control.[357]

[356] *See, e.g.*, Canadian Security Standards, *supra* note 290, at 11, (requiring a locking file cabinet for subscriber information and secure workstations).

[357] Associated logical physical security controls will impact the physical security control requirements. Logical security controls include the use of passwords or PINs to control access to a subscriber's system, third-party computing resource, or to a private key.

Assessors should determine the feasibility and need for physical security in the subscriber's operational environment. They should also determine whether any external requirements dictate physical security controls for subscribers, such as requirements originating from applicable law or contract. Finally, assessors should determine whether subscribers are, in fact, following physical security requirements set forth in the PKI's documentation.

Appropriate Requirements and Practices. PKI participants may want to include in their subscriber agreements requirements that:

- Subscribers to protect their private key should be conspicuously stated in all subscriber agreements.
- Suscribers locate their workstation in an area reasonably secure from tampering by unauthorized personnel.
- Passwords and PINs should be memorized and not be written down; if a password or PIN needs to be written down it should be stored in a locked file cabinet or container accessible only to designated personnel.
- A private key stored on any unsecured medium, such a diskette, it should be stored in a locked file cabinet, secured digital archive, or locked container.
- Subscribers should not leave their workstations unattended when cryptography is in an unlocked state (i.e., when the PIN or password has been entered). A workstation that contains private keys encrypted on a hard drive should be physically and logically secured or protected with an appropriate access control product.
- Cryptographic tokens should be protected by holders to an extent comparable with that of valuable personal items such as credit cards or drivers' licenses.
- Documents, diskettes, or other items containing PINs or passwords should be disposed of in a manner that does not compromise the confidentiality of the sensitive data.

PKIs will want to establish subscriber physical security requirements that are proportional to the assurance levels provided by the certificates and suitable in light of the need for security in the application being secured by certificates. The PKI should document such controls in its documentation, and particularly in its subscriber agreements, while taking into account any external regulatory or contractual requirements. Subscribers should, in fact, abide by physical security requirements set forth in the PKI's documentation.

D.5.2 PERSONNEL SECURITY CONTROLS

D.5.2.1 Trusted roles

Issue Summary. This section sets forth requirements or practices identifying the specific jobs or classes of jobs as security sensitive, requiring assurances of specified levels that the persons filling these jobs are trustworthy. It also allows for separation of certain roles to prevent conflict of interest in fulfilling those roles.

Relevant Considerations. In Federal and DoD CPs, "Trusted Roles" define specific job titles that require special levels of trustworthiness. These might include CAs, CA equipment operators, system security officers, Registration Authorities, and their agents. Defining these roles and their functions makes it very clear what functions must be performed by "trusted roles" that must meet the requirements defined in Section 5.3. It also allows for separation of certain roles. For example, there is a conflict of interest if the audit data evaluator also acts as a CA or RA administrator, since one purpose of evaluating the audit data is to detect suspicious CA operator or RA administrator activity.

Assessors should determine, in light of the PKI's technological environment and the business need for security and separation of roles, whether there is a need for trusted roles. The assessors should compare these findings with the PKI's documentation. They should also consider whether external requirements bear on the designation of trusted roles, such as regulatory and contractual requirements. Finally, they should determine whether or not PKI participants place trustworthiness requirements on persons seeking or occupying the trusted roles identified in the PKI's documentation.

Appropriate Requirements and Practices. Generally, persons serving in roles that are in a position to compromise keys or otherwise approve certificates and participate in any dimension of the certificate life cycle should be demonstrably trustworthy. Consequently, PKIs will want to document specific job roles or classes of job roles that are required to be trusted roles, consistent with any applicable external requirements. Designating specific job titles as trusted roles has the advantage of certainty and clarity as to which persons need to undergo trustworthiness analyses. Nonetheless, such specificity may come at the expense of rigidity in the face of changing business functions and technology environments. Moreover, identifying entire classes of job roles as being trusted roles in a more general fashion will make it less likely that roles will be omitted inadvertently, although such flexibility comes at a cost of possible ambiguity of which new personnel need to be trusted and which do not. The personnel practices finally adopted by PKI participants in terms of treating certain jobs or job classes as trusted should match the requirements or practices appearing in the PKI's documentation.

D.5.2.2 Number of persons required per task ("Dual" or "Multiple" Control)

Issue Summary. This section considers the extent to which two or more persons are required to perform certain functions to assure trustworthy operations. In specific it lists those tasks or operations that require dual or multi-person controls and the number of persons required to perform them.

Relevant Considerations. The PKI can employ numerous techniques to ensure that no single individual may gain access to critical information stored by the PKI (e.g., private keys), including split-knowledge schemes, such as twin password mechanisms and key-splitting techniques. Separating duties for critical PKI functions to prevent one person from accessing CA or subscriber private keys or other information to which they should not have access or which they do not need to know to perform their duties. In the case of subcribers, it is common for PKI services to require that a subscriber have exclusive access and control of its private keys. This can be achieved by implementing separate trusted roles, by assigning more than one individual to accomplish critical tasks, and by implementing authentication mechanisms.

Assessors should consider functions performed by PKI participants and whether multi-person control makes sense in light of the need for security. They should then compare the results of this analysis with the multi-person control requirements and practices in the PKI's documentation and any applicable regulatory or contractual requirements. Finally, they should determine whether or not multi-person control is enforced for the functions identified in the PKI's documentation as requiring such control.

Appropriate Requirements and Practices. Although an individual operating alone may perform many duties in a lower security environment associated with PKI roles, a multi-user control may be required for PKI best practices in the PKI environment.[358] A PKI should generally provide for a minimum of two distinct PKI personnel roles, distinguishing between day-to-day operation of the PKI system and the management and audit of those operations.[359] Some other activities where multi-person control may enhance security include:

- Private key generation, especially with respect to CA keys;

[358] A PKI must ensure that any process it employs provides for the generation of trustworthy corporate records of all activities performed by PKI role holders. *See* PAG APP 2 *(Digital Signature and Confidentiality, Certificate Policies for the Government of Canada Public Key Infrastructure*, v. 3.02, Gov't of Canada (Apr. 1999), *available at* <http://www.cio-dpi.gc.ca/pki-cp/documents/Certificate_Policy/cp-pctb_e.asp>, hereinafter "Canadian Confidentiality Certificates").

[359] *Id*.

- Private key activation and operation, again especially concerning CA keys;
- Approvals of certificate applications; and
- Gaining access to high security zones.

The need for multi-person control is generally proportional to the need for security in the applications, for which the certificates are used and the assurance levels provided by the certificates. The feasibility of multi-person control may depend on the technological environment. PKIs should adopt multi-person control schemes where the cost and burden associated with such schemes are justified by the need for security. They should document their multi-person control requirements, consistent with external requirements. Finally, PKI participants should enforce the multi-person control requirements and practices set forth in the PKI's documentation.

D.5.2.3 Identification and authentication for each role

Issue Summary. This section addresses the controls required to assure proper identification and authentication of persons seeking to take on certain PKI-related roles, where such controls are applied before they are hired or retained. This section may also address continuing identification and authentication procedures that persons filling certain roles may undertake immediately prior to performing certain functions.

Relevant Considerations. To prevent unauthorized access to critical operations within the PKI system, and to provide verification that an authorized individual performed each PKI operation, PKI participants can implement identification and authentication mechanisms. Identification and authentication mechanisms can fall into two categories. First, PKI participants may want to confirm the identity of persons seeking to occupy certain roles before hiring them for such roles. Second, logical controls may enforce requirements that personnel authenticate themselves to the systems and applications performing sensitive PKI functions before being able to perform such functions.

Assessors should analyze whether there is a need for identification and authentication procedures in the hiring process for certain roles and for logical controls enforcing identification and authentication prior to personnel carrying out critical PKI functions. They should also determine whether such procedures and controls appear in the PKI's documentation. Finally, they should determine whether or not PKI participants are enforcing such controls.

Appropriate Requirements and Practices. The kinds of procedures involved with the confirmation of the identity of certificate applicants can be used to identify and authenticate persons seeking designated roles within a PKI participant's organization during the hiring process. *See* PAG § D.3.2.4 (Validation of individual identity). For example, candidates for trusted roles may be required to appear in person before designated HR or security personnel and present credentials confirming their identity.

Likewise, PKI participants will likely want to mesh identification and authentication controls with logical security controls, through cross-references or otherwise, to show that PKI participants are permitting only authorized personnel to perform critical PKI functions. *See* PAG §§ D.6.5 (Computer Security Controls), D.6.7 (Network Security Controls). For instance, each certificate and account (with the exception of CA signing certificates) should be directly attributable to an individual,[360] not be shared, and be restricted to actions authorized for that role through the use of PKI software, operating system, and procedural controls.[361]

The identification and authentication procedures applicable to the personnel of PKI participants should generally be proportional to the assurance levels of the certificates and will depend on the security needs of the

[360] Where the actual signing is a device-driven automated event, the signing operation performed by the device should be attributable to a person.

[361] *See* Canadian Confidentiality Certificates, *supra* note 358.

applications for certificates. The PKI should document such procedures in its documentation and should account for any regulatory or contractual provisions. PKI participants should, in fact, adhere to the requirements and practices set forth in the PKI's documentation.

D.5.3 PERSONNEL CONTROLS

Issue Summary. This section addresses the controls in place to ensure that personnel are qualified, competent, trustworthy, trained, and deployed to maintain trustworthy operations. It may address controls related to personnel filling trusted roles, but may also include controls on other personnel. This section may address controls that apply prior to a person filling a certain role and controls that apply continuously or periodically during a person's employment.

Relevant Considerations. Personnel controls open to PKI participants include the following:

- Background, qualifications, experience, and clearance requirements
- Background check procedures
- Training requirements
- Retraining frequency and requirements
- Job rotation frequency and sequence (if job rotation is appropriate to the environment)
- Sanctions for unauthorized actions
- Contracting personnel requirements
- Documentation supplied to personnel
- Drug testing and ongoing testing programs
- Routine and impromptu testing of employees of rules and procedures
- Adopting employment practices that assist in attracting and hiring qualified personnel.

Assessors should determine which of these controls make sense in the context of a particular PKI, while considering any external requirements stemming from applicable law or contracts. They should determine whether the PKI's documentation reflects these controls. Finally, they should determine whether PKI service providers are, in fact, enforcing such controls.

Appropriate Requirements and Practices. The presence of qualified, competent, and trustworthy personnel is critically important to ensure the availability, efficiency, integrity, and confidentiality of the PKI services; consequently, this should be a primary objective of the PKI. A PKI should take measures to ensure that personnel who undertake sensitive rules are trustworthy (*but see* PAG § D.5.2.1 for a discussion of trustworthy personnel in light of the trust assurances the PKI is offering).[362] In order to accomplish this objective, the PKI should define and implement personnel control mechanisms that are commensurate with the attendant risks.[363]

[362] *See* Gatekeeper Criteria, *supra* note 33 at p. 15. Accreditation under Gatekeeper requires "[a]ll operational [CA] staff will need to be cleared to the Highly Protected level of personnel clearance."

[363] Some systems impose strict measures, such as "continuous personnel monitoring" of "mental health, health control, and treatment," to insure that CA staff maintain the proper "character." *See* Japanese Guidelines, *supra* note 290, § 2.3.4. For governmental PKIs, pre-existing categories of security clearance may be used. *See also* Canadian Security Standards, *supra* note 290, at 9 (requiring "CA privileged users" and RAs to hold Level II security clearance).

For higher assurance environments, because the best attacks against any security system are still those which can most easily be grouped under the categorization of "social engineering," it would be an acceptable practice for the operators of PKIs to restrict all employment to individuals without any public record of untrustworthiness. For lower assurance environments, the PKI may permit PKI operations to be performed by personnel whose trustworthiness is not necessarily confirmed by investigation but where the PKI in good faith has no reason to suspect that the employee is not trustworthy. Higher-security environments would likely want to require affirmative background checks on personnel.

A PKI will generally want to document its personnel controls and ensure that they comply with applicable law and any contractual requirements. The personnel practices they institute should, in turn, match the requirements and practices appearing in the PKI's documentation.

D.5.4 BACKUP POLICY

D.5.4.1 Types of Data Backed-Up

Issue Summary. This section concerns the extent to which a PKI must ensure that its participants back up critical information, such as applications, data, and files necessary to restore a PKI system's data center after failure. More specifically, this section relates to the types of data that should be backed up by which participants.

Relevant Considerations. Assessors should consider the types of information required or helpful to be backed up, the retention period for backed up information, required backup protection, and backup procedures. Backups provide business continuity capabilities in the event of a disaster or the accidental or intentional corruption of backed-up information. Assessors should also determine whether such backups are required in the PKI's documentation, consistent with any external requirements. Finally, they should ascertain whether PKI participants are, in fact, backing up the data in accordance with the PKI's documentation.

Appropriate Requirements and Practices. PKIs will generally want to back up the following applications, data, and files:

- Installation disks for the operating systems;
- Installation disks for the CA application;
- Installation disks for the directory application;
- Online key, certificate and CRL histories;
- Directory data;
- Subscriber, CA personnel and organisational entity representative data; and
- Audit logs.

The extent of backups required will depend on the need for business continuity and for providing continuous service notwithstanding disasters or security compromises or incidents. The PKI should reflect the types of information backed up in its documentation, which should be consistent with applicable law and contract. PKI participants should maintain backups of the kind of information identified in the procedures contained in the PKI's documentation.

D.5.4.2 Retention Period for Backups

Issue Summary. This section covers the time periods during which backups made under the previous section must be retained.

Relevant Considerations. Since an important goal of PKI is to advance the over-all operation of e-commerce, the retention period of backups of relevant online data is of great import. Assessors should focus on considerations including the nature of the application, contractual obligations (such as a service level agreement), the extent of available system audit trail capabilities, audit requirements, corresponding statutes of limitations, and countervailing privacy considerations. Assessors should compare the outcome of the analysis of these considerations to see if it matches the retention periods set forth in the PKI's documentation. Finally, assessors should determine whether PKI participants are holding backups at least for the time periods mentioned in the PKI's documentation.

Appropriate Requirements and Practices. Relevant data as necessary to prove the propriety of each certificate lifecycle process and operation should generally be retained for at least the operational period of the certificate. For nonrepudiation support, relevant data should be retained for a commercially reasonable period of time.[364] Data should be backed-up in accordance with explicit schedules that match the business needs of the PKI for retaining data long enough to allow recovery of information in the event of a security incident, compromise, or disaster. The retention periods should be consistent with applicable regulatory and contractual limits, and should appear in the PKI's documentation. Lastly, PKI participants should maintain backups for the time periods identified in the PKI's documentation.

D.5.4.3 Protection of Backups

Issue Summary. This section states the controls implemented to ensure that backups are protected from physical damage and security compromise.

Relevant Considerations. Various physical and logical controls are available to protect the integrity of backups and to prevent unauthorized access, disclosure, and modification. Assessors should consider the need for rigor in the controls surrounding backups and any regulatory or contractual requirements for backup protection. They should determine whether adequate backup protection methods are established in the PKI documentation. Finally, a PKI should ascertain whether PKI participants are, in fact, protecting their backups in accordance with the documentation.

Appropriate Requirements and Practices. The manner or means by which a backup is protected will depend on the assurance levels of the certificates and the business continuity needs of the PKI participants. Additionally, for business continuity purposes, the proximity of the backup site to the primary site will likely balance the need for a quick recovery time (transit time between backup site to primary site) with the need for a geographically diverse location between the two sites in order to mitigate or avoid simultaneous damage to both locations from the same disaster (e.g., earthquake, flood, line outages, etc.).

The protection of backups should be undertaken using a combination of physical and logical controls. For instance, some PKIs will want to safeguard at least two (2) backup copies in different secure sites adequately separated by geography. One copy may be kept on the premises of the PKI system, and the other at another secure site.

The procedures the PKI finally chooses to protect its backups should be reflected in the PKI's documentation. That documentation should account for applicable regulatory or contractual requirements. The PKI's participants, then, should implement the procedures set forth in the documentation.

[364] This period may be very long indeed. For instance, the German system requires that security data and individual subscriber information be retained in accessible form for 35 years. *See* German Signature Act, *supra* note 338, § 13(2).

D.5.4.4 Backup Procedure

Issue Summary. This section states the procedures implemented to ensure that backups are created and maintained in accordance with the backup policy.

Relevant Considerations. Factors in gathering backup data involve implementing a tape rotation schedule (including periodic testing for disaster recovery), as well as determining who will perform recovery, how a chain of custody will be established, and how sensitive data (e.g., escrowed/archived private decryption keys) will be protected from compromises in security. Other examples of systems for backing up data that have different speed-of-recovery and cost considerations include:

- **Hot Duplicate.** Mirror image site that is synchronized frequently with seamless and instantaneous recovery. This should include automatic failover.
- **Hot Backup.** Separate site with equivalently configured hardware and software, where recovery can be completed typically within a couple of hours by either loading or updating appropriate applications and data.
- **Warm Backup.** Minimum subset of hardware and software where recovery can be accomplished within 24-72 hrs by loading applications and data on the backup system
- **Daily Backup.** Rebuilding of data from daily backup(s) and reloading of applications when the hardware and software facilities have been restored. Recovery may take hours, days or weeks, depending on the nature and extent of the disaster.

Assessors should determine which of these systems or other mechanisms are appropriate in light of the business continuity needs of the PKI, subject to any regulatory or contractual requirements. They should also review the PKI's documentation to determine if it implements such mechanisms. Finally, assessors should ascertain whether or not PKI participants are adhering to the backup procedures in the PKI's documentation.

Appropriate Requirements and Practices. An example of a useful backup procedural scheme could include the following:

- A daily incremental backup should be performed to capture modifications made during the day.
- A complete weekly backup should be performed to capture modifications made during the week.
- A complete monthly backup should be performed to capture the overall state of the PKI.
- Testing for disaster recovery, which may include testing the process of restoring data from a backup copy, should be performed every six months.
- Sensitive material should be stored in an encrypted format on all backups.

In the end, the backup procedures chosen should provide assurances of business continuity that are appropriate in light of the assurance levels provided by the certificate and the need for uninterrupted service. The PKI should include these procedures in its documentation, accounting for any regulatory or contractual requirements. Finally, PKI participants should implement the kind of controls described in the PKI's documentation.

D.5.5 AUDIT LOGGING PROCEDURES

D.5.5.1 Types of event recorded

Issue Summary. This section addresses the types of system level events that PKI participants must or do record for the purpose of maintaining an audit trail.

Relevant Considerations. Audit logging procedures enhance the trustworthiness of a PKI. They permit the operators of a PKI service provider to ensure the continued security of their systems. For instance, audit logging facilitates the investigation of anomalous events and provides evidence needed to support corrective actions. Moreover, audit logging supports nonrepudiation services. A PKI service provider can provide evidence that certain events took place at certain times to explain, in litigation or another dispute resolution proceeding, the integrity of the services underlying the certification services of the PKI service provider securing the transaction at issue.

Assessors should determine what kinds of events it makes sense to log, consistent with any external requirements. They should also review the PKI's documentation to determine whether an appropriate list or categories of events to be logged appears there. Finally, an assessment can include an analysis of whether audit-logging systems are, in fact, in place and log the events listed in the PKI's documentation.

Appropriate Requirements and Practices. Requirements for recording of relevant events (corporate record) will largely depend upon the level of assurance to be provided by the PKI and the technological environment used by a given PKI service provider. Collection and maintenance of audit logs can be resource intensive and must be balanced. However, significant events on the PKI system should *at the very least* be recorded in audit trail files. There are no specific minimum requirements for logging of events in lower assurance PKIs. For lower- through higher-assurance PKIs, significant events on the PKI system should be automatically recorded in audit trail files or as digital records.

Events commonly logged by PKI service providers include:

- successful and failed attempts to initialize end-users, remove, enable, disable, update and recover users, their keys and certificates
- successful and failed attempts to create, remove, login as, set, reset and change passwords of, create, update and recover keys and certificates for the roles within the PKI operating authority.
- failed interactions with the certificate repository, including successful and failed connection attempts, read and write operations of the PKI application
- all events related to certificate revocation, security policy modification and validation, PKI application startup and stop, database backup, cross-certification, certificate and certificate chain validation, attribute certificate management, user upgrade, distinguished name change, database and audit trail management, certificate life-cycle managemen, and
- PKI key generation, storage, retrieval, activation, deactivation, archival and destruction.

The events a PKI deems appropriate for participants to log should appear in the PKI's documentation. That list should include items that participants are required by contract, or perhaps by regulatory scheme, to log. Finally, participants should establish audit-logging systems that meet the requirements or perform in accordance with the practices set forth in the PKI's documentation.

D.5.5.2 Frequency of processing log

Issue Summary. This section concerns how often and/or under which circumstances audit logs compiled under the previous section are reviewed.

Relevant Considerations. Processing of audit logs refers to the review of audit events as identified in Section D.5.5.1. Such review may be a routine check of such events on a periodic basis or a check when an alarm or other mechanism brings the event to the attention of the participant's personnel. Such logs are critical to the monitoring, oversight, and verification of PKI operational integrity.

Assessors should determine, for given PKI service providers, whether it makes sense for audit log processing to be performed by a manual review of the logs on a periodic basis or whether manual processing is infeasible, which will influence a decision in favor of more automated processing. They should determine whether any externally imposed requirements apply to audit logging process, such as those arising by regulatory scheme or contract. Finally, they should determine whether PKI service providers are, in fact, processing their audit logs as required or disclosed in the PKI's documentation.

Appropriate Requirements and Practices. Requirements for the frequency of the review of audit logs depends upon the level of assurance to be provided by the PKI and can also vary by the specific audit log and type of events captured by the audit log. At the very least a risk assessment should be performed to define the relevant audit events and the relevant impact to the security of the environment. This risk assessment consequently influences the determination of appropriate processing frequency.

In some schemes, recorded audit events can be divided into general categories, and processing practices can be designated for each category. For example, a scheme may state that:

Some events that require immediate processing, such as:

- Firewall penetrations
- System logging shutdown
- System reboot
- CA Signing key activation
- Audit log failure

Some events that require daily processing, such as:

- Login failures
- Login successes
- Software installations
- Backup processes

And some events that require periodic processing

- Password renewals
- Activity summaries and renewals

The choice between manual processes to process audit logs and automated process will depend on the scale of the operations of the PKI service provider. There is some assurance and reliability associated with human processing of audit logs on a manual basis. On the other hand, it may or may not be feasible to have an individual take a given portion of time and review logs on a periodic basis if the scale of information stored in the logs is immense. Also, humans can make mistakes and scripts or alarms may provide more reliability under some circumstances, especially when the volume of audit data is large.

Whatever ways of processing logs are chosen by a PKI should be reflected in its documentation. The documentation should account for regulatory or contractual requirements. The actual logging practices of PKI service providers, moreover, should match those set forth in the PKI's documentation.

D.5.5.3 Retention period for audit log

Issue Summary. This section states the retention period(s) during which log(s) of audited events recorded by the PKI must be or are retained.

Relevant Considerations. Audit logs may be stored on site or off site. The retention periods may be different for each. Alternatively, a PKI can require that logs remain on site for a period of time, after which they are transferred off site. It can then set a retention period for off site storage.

Assessors should consider the appropriate time periods to retain logs. They should determine whether the PKI's documentation reflects these periods, consistent with requirements imposed externally. Finally, they should determine whether PKI participants are, in fact, retaining logs in accordance with the documentation.

Appropriate Requirements and Practices. Retention of the audit log should be predicated on an assessment of the PKI's domain requirements, but should be guided by the minimum requirements outlined in these Criteria. In some jurisdictions, and for specific regulated industries, more stringent requirements may apply. Typically, the higher the assurance needed, the longer the audit log should be maintained. Audit logs are maintained for anywhere from several months to several years depending on the specific characteristics the operational environment. Good practice may dictate that PKI service providers retain these logs for as long as a certificate's validity might be called into question.

The PKI should clearly document its retention periods. In addition, it should ensure that these periods are consistent with any requirements imposed by law or contract. PKI service providers, in turn, should ensure that they retain audit logs in accordance with the requirements or practices set forth in the PKI's documentation.

D.5.5.4 Protection of audit log

Issue Summary. This section states the controls implemented to ensure that audit logs maintained by PKI participants are protected from physical damage and security compromise.

Relevant Considerations. The purpose of protecting the audit log is to ensure the integrity of the logs and prevent unauthorized additions, deletions, or modifications to or from the logs. Thus, audit-logging systems may include functionality to control access to audit logs and to permit only authorized administrators to make changes. Assessors should consider the technological environment and the assurance level of the certificates to determine the extent to which PKI service providers should be protecting their audit logs. They should determine whether the PKI documentation reflects these requirements or practices. Finally, assessors should determine whether PKI service providers are implementing the documented controls.

Appropriate Requirements and Practices. The assurance level of certificates and the features or limits of the technological environment will typically dictate the level of protection imposed on audit logs are identical (for lower, moderate and higher assurance levels and for short-term and long-term retention periods). A PKI will

want to weigh the security assurances provided by protective measures against the costs associated with implementing them it is good business practice to protect the integrity of audit logs by individually time-stamping all entries to the audit log. Good practice also having duly authorized PKI services personnel digitally sign logs. Those performing the functions that generate audit records should genrally not be able to modify (including delete) audit records. A well-designed system will also prevent such persons from reading the audit records, as this makes it harder for operators to find ways to bypass audit functions. Extra assurances are provided by having two copies of the log be made and stored in separate physically secured locations.[365]

D.5.5.5 Audit collection system (internal versus external)

Issue Summary. This section addresses where the audit collection system resides in relation to the PKI participant's systems. More specifically, it concerns whether the mechanisms that collect audit log information are, in relation to a particular PKI participant's systems, internal to that participant or are instead hosted by an external entity.

Relevant Considerations. An audit collection system may be internal to the participant being audited or external to it. The location of the audit collection system could affect the reliability and, therefore, the security of the overall system. Internal audit collection include software and systems hosted on machines located locally that can log events, for example at the entity's data canter. These systems have the advantage of being within the immediate proximity and control of the entity trying to monitor its own systems. Hosting the audit collection system internally reduces the risk of compromise of the audit logs by an external attacker, such as an attacker at the company hosting the audit collection team.

On the other hand, as audit log entries may be used for evidentiary purposes, their accuracy and integrity may be questioned. An audit log resident on a CA's compromised internal machine may not be as useful as a separate or a third party audit collection system. Moreover, an external audit collection system may be hosted by an entity having a more secure facility than the entity being monitored. For instance, a CA may want to compile and collect audit trail information about RA activity in its data center under the view that the CA's facility may be more secure than the RA's. Moreover, an external audit collection system may permit the centralized storage and control of audit log information. The external host could act as a trusted fourth party to store audit logs of a CA to prevent compromise from internal attacks.

If the PKI relies on a single audit system, additional security mechanisms may be necessary to guarantee audit entry authenticity. Alternatively, the audit system may be implemented in a distributed or redundant way where multiple independent copies may be correlated.

Assessors should determine which type of audit collection system is appropriate for the PKI being assessed. Assessors should also review the documentation to determine if it designates an appropriate audit collection system in its requirements or disclosures. Finally, they should determine whether or not PKI participants are using the audit collection systems required or disclosed within the PKI's documentation. The practices need to answer the basic question: "Can I prove to other parties that the audit log is trustworthy?"

Appropriate Requirements and Practices. Audit collection systems typically generate vast amounts of data. When a PKI participant considers future use of such data, the participant should give some forethought to its archive, including appropriate collection and storage controls. As mentioned in the Relevant Considerations section, internal and external audit collection systems each have their own advantages and disadvantages. It is also possible to use a combination of internal and external systems.

PKIs will generally want to use audit collection systems that integrate well with their CA or RA applications. Some applications may have built-in audit logging capabilities. Thus, the choice of internal or external audit collection systems will largely depend on the CA and RA systems used. In addition, the expense and effort of

[365] *Accord*, *see* Japanese Guidelines, *supra* note 286, § 3.6.3(2).

implementing an audit collection system should be commensurate with the assurance levels provided by the certificates and appropriate in light of the security needs of the PKI. In any case, the internal or external nature of the audit collection system should be reflected in the PKI's documentation. Moreover, the PKI's participants should obtain and implement the audit collection systems required or described in the documentation.

More generally, a PKI participant needs to take into account the requirements for independence of the entity collecting audit trail information and the technology needed to implement the audit collection process. These requirements may dictate the decision to use an internal or external system, or the decision to use a single or redundant system. Moreover, referring to regulatory and insurance requirements may be helpful since they sometimes mirror current best practices, and PKI participants should adhere to any applicable regulatory or contractual requirements for internal or external systems. A PKI participant may want to consider having an independent test of the audit system to validate its audit collection ability. It will also want to ensure that its audit logging systems match the requirements or practices within the PKI's documentation.

D.5.5.6 Notification to event-causing subject

Issue Summary. This section concerns whether the PKI has a requirement or practice of notifying a person in the event that the person or a device under the person's control has caused an event that resulted in an alarm, created another anomalous audit log entry, or was otherwise detected.

Relevant Considerations. There is no standard practice concerning whether or not a PKI participant informs a person when he or she causes an event resulting in an alarm or other anomalous log entry. On one hand, telling the subject of the problem that he or she caused an event can facilitate the person ceasing the conduct that caused the problem and preventing reoccurrence. On the other hand, if there is a possibility that the event-causing subject is hostile, then having a policy to alert event-causing subjects of an event may make it difficult to flush out the attacker. Moreover, having a blanket policy requiring such notice is harder to administer than having a policy that does not require such notice.[366]

Assessors should consider whether notification of an event-causing subject would be a suitable practice within the PKI, subject to external regulatory or contractual requirements. They should see whether the PKI's documentation addresses this point accordingly. Assessors, then, should determine whether in fact PKI participants are conforming to the PKI's documentation on this issue.

Appropriate Requirements and Practices. A PKI's choice to have a policy to notify event-causing subjects of an event will be driven by the security and business needs of the PKI and the feasibility of providing such notice. Some events may require the entity causing the event to be notified for investigative or corrective actions (e.g., multiple incorrect password entry). Some events may warrant entity notification and acknowledgement from the entity (e.g., private key destruction or system security policy violations). Whatever choice the PKI makes should be reflected in the PKI's documentation. Moreover, PKI participants should actually provide such notices if required to do so by the PKI documentation.

[366] Of course, notifying the event-causing subject is a separate from the question of whether notice should go to persons responsible for handling security incidents and compromises. Notification of PKI personnel responsible for audit verification of any critical security events or discrepancies as they are logged is often part of a PKI's incident and compromise handling procedures. *See* PAG § D.5.8.1 (Computing resources, software, and/or data are compromised or corrupted).

D.5.6 CORPORATE RECORDS MANAGEMENT

D.5.6.1 Types of Corporate Records Maintained

Issue Summary. This section concerns which records must or are preserved by PKI participants as part of their records management policies and practices.

Relevant Considerations. PKI "corporate records" may involve different types of information. Moreover, records management policies may involve the classification of the character of the documents identified (e.g., confidential, private, protected, top secret, etc). Thus, one aspect of an assessment is an analysis of the kinds of records that a PKI participant has a business need to retain. Corporate records as used in these Guidelines refer to more than just articles of incorporation and corporate minutes. They also include records relevant to the operation of PKI service providers such as agreements, correspondence, and customer and certificate application records.

The management of electronic records within a PKI environment has many similarities with the management of digital data in information systems, such as backup and recovery, event log files, access security, and retrieval, and viewing. Nonetheless, there are also certain areas unique to electronic records management: long-term electronic retention of records (in many cases permanently); long-term accessibility (tens of years or more); audit trails and corporate records of events and actions related to a case file; migration of electronic case files and records to new storage media; transfer to new hardware, software, and application systems; and unique electronic case file and record metadata that provide the information needed for long-term accessibility and transferability. In general, corporate records retention systems emphasize functionality to ensure the integrity, authenticity, and availability of records over time, in contrast to backup systems, in which recovery time is critical.

Furthermore, assessors should be aware that although CAs and relying parties maintain records for the same general business reasons, they maintain these records in support of different business models. As such, record management policies should be evaluated based on the business model that they are attempting to support. The parties may have different retention policies as far as what is archived and the time that such information is retained. For example, the FAA may want 50 years based on the life of an aircraft, whereas the IRS may want 10 years. Although this section focuses on assessing a PKI service provider's records management efforts, the general principles contained herein are equally applicable to relying parties and other entities participating in a PKI.[367]

At the time of writing, SEC Rule 17a-3, 17 C.F.R. § 240.17a-3, is one of the best public examples of records retention requirements, and SEC Rule 17a-4, 17 U.S.C. § 240.17a-4 (discussed in PAG § D.5.6.2 below), is one of the most comprehensive outlines of electronic storage preservation requirements. As such, assessors may want to familiarize themselves with those Rules as part of their assessment process.

Generally speaking, assessors should determine which business records it makes sense for PKI service providers to retain in light of the use of certificates and the assurance levels they provide. They should determine whether any records must be retained under applicable law or by contract. Assessors should see if a PKI has a corporate records management program and whether it calls for the retention of appropriate records. Finally, they should

[367] An example of the divergent needs of CAs and relying parties is found in the preservation of records related to the creation of a digital signature. Certain relying party organizations, for example, have decided that they will only retain proof that they checked a CRL at the time they validated the digital signature. They then discard the digital signature and in the future do not rely on re-validating the digital signature. In a legal dispute, they then provide proof that the digital signature was validated at the time the record was received, and following that, the record was maintained according to proscribed records management practices. In this case, the relying party may enter into an agreement with a CA that releases the CA from its requirements to maintain additional information.

determine whether or not PKI service providers are, in fact, retaining the records they are required to maintain under the applicable corporate records management program.

Appropriate Requirements and Practices. PKI service providers are trusted entities that are required to create, transmit, receive, and preserve highly sensitive information as a normal function of their business operations. As such, they should implement and administer a corporate records management program in accordance with current recognized records management practice guidelines, applicable rules and laws, and the requirements of any applicable contractual requirements. A PKI should document which records they retain as an important component of such a program. Moreover, the records retained by PKI service providers should match the records that must or are retained pursuant to the applicable corporate records management program.

D.5.6.2 Retention Period for Corporate Records

Issue Summary. This section establishes a retention schedule or set retention period for corporate records maintained pursuant to the previous section.

Relevant Considerations. Assessors should take into consideration the objectives and intended assurance level of the PKI when determining whether the appropriate corporate records have been identified for preservation. It is common for regulatory schemes and contractual documents to impose retention periods for corporate records. Consequently, assessors should determine whether any external requirements dictate practices concerning retention periods. Finally, assessors should determine whether or not PKI service providers are, in fact, maintaining documents for the required or stated retention periods.

Appropriate Requirements and Practices. The types of corporate records retained will depend on the applications for which certificates are used and their assurance levels. For PKIs that retain records for a period of time, it is common for them to maintain at least their audit records of CA lifecycle services, copies of certificates, and information supporting certificate applications.

Whatever information is deemed important by the PKI for participants to retain, the PKI should require in its documentation that such records be kept. The documentation should be consistent with any externally-imposed requirements. Finally, PKI participants should put into practice the records retention requirements and practices appearing in the PKI's documentation.

D.5.6.3 Protection of Corporate Records

Issue Summary. This section describes how corporate records should be protected. More specifically, it can relate to the access controls that are established and implemented, and may dovetail with applicable security or personal privacy requirements.

Relevant Considerations. It is important to maintain the integrity of corporate records to ensure the trustworthiness of the PKI and support nonrepudiation services, as with audit logs. *See* PAG § D.5.5.4 (Protection of audit log). Assessors should review the PKI service provider's policies, procedures or access controls to ensure that archived records are accessible only in accordance with the policy requirements of the PKI and the classification of the corporate record (e.g., privacy and security classifications). Assessors should also review all privacy considerations, found above in PAG § D.2.8 (Consumer Issues, Information Practices, and Privacy), and any applicable external requirements. Finally, assessors should determine whether PKI service providers are, in fact, protecting their corporate records in accordance with the PKI's documentation.

Appropriate Requirements and Practices. The records maintenance systems and the assurance levels provided by the certificates will be the chief factors in dictating the measures that should be implemented to protect the integrity of corporate records. PKIs will also want to adhere to any external requirements for protective measures required by law or contract. PKIs will want to balance these needs against the costs and

burdens associated with these protective measures. The PKI's documentation should reflect the protective measures required or chosen. Lastly, PKI service providers should ensure that their corporate records management systems do, in fact, implement the requirements or practices set forth in the PKI's documentation.

D.5.6.4 Archival and Storage Procedures for Corporate Records

Issue Summary. This section describes the archival and storage procedures for corporate records.

Relevant Considerations. Assessors examining the records management activities of a PKI service provider should consider the PKI's documentation as the logical starting point for ascertaining the practices to which a PKI is required to adhere. While the overall purpose of records management is the creation of accurate, reliable, and trustworthy records, records storage is also concerned with preserving the integrity of those records over time. Thus, assessors should determine whether the procedures for archival and storage of corporate records must ensure that the corporate record is maintained in the manner called for by its classification. They should also account for any requirements imposed by law or contract. Finally, they should determine whether or not PKI service providers are, in fact, implementing such procedures.

Appropriate Requirements and Practices. SEC Rule 17a-4 provides one example of a corporate record archival and storage system.

The following also provides a non-exhaustive list of records management issues that a CPS should address in order to achieve an integrated and comprehensive approach for managing electronic records:

1) Policies and procedures should be updated or augmented to reflect the legal and best practice requirements for managing and protecting electronic records.

2) Professional records management personnel and practices should be employed to produce and maintain records retention policies and schedules, and to oversee and monitor the preservation of the information for the full life cycle.

3) Reliable transmission and access security are mandatory for meeting the requirements of preserving integrity, protecting confidentiality, as required, and establishing ongoing authenticity. Security levels must be matched to the sensitivity level of the information and the risk of communication, access and storage being compromised, such as differentiating between open and closed communication systems.

4) A single audit trail should be populated for each access or other event or action that could potentially result in modification, loss, misuse or destruction of an electronic record.

5) Quality control and assurance steps should be an integral part of all acquisition or capture processes, including image scanning as well as electronic receipt and creation, to ensure that accurate and complete records and metadata are being stored.

6) File formats must provide for long-term processibility (rendering on a computer screen and printer) and transferability (from one application environment to another). The Extensible Markup Language (XML) may provide certain benefits for this purpose.

7) Training and documentation are particularly important business practices for achieving a successful transition of business practices and personnel from the current paper-based records environment to electronic records management processes that are computer-controlled.

8) Electronic records management systems should provide a facility for accurately binding information related to time and date to a record. *See* PAG § D.4.13 (Time-stamping Services).[368]

The PKI service provider should provide for the transfer and access of all records upon termination in a manner that will cause minimal disruption to subscribers and relying parties.[369] *See* PAG § D.5.9 (CA Termination) for more information on this topic.

---

[368] *See* PAG APP 2 (*Exemption of Transactions Pursuant to Certain Contracts*, Investment Company Act of 1940, SEC Rule 17a-4, 17 C.F.R. pt. 270 (1947) (hereinafter "SEC Rule"). The following structure is another possible scheme for managing records:

(A) Records required to be maintained and preserved may be produced or reproduced on electronic storage media (as defined in this section) that meet the conditions set forth in this paragraph and be maintained and preserved for the required time in that form.

(i) Preserve the records in a manner that is designed to preserve their integrity over time.

(ii) Verify automatically the quality and accuracy of the storage media recording process,

(iii) Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media. The time-stamp should be acquired from a source that is independent of the automated device (CAs server, subscriber's PC, etc.) that generated or is controlling the event, such as a third-third-party time-stamping service, or other independant automated device.

(iv) Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this.

(v) At all times have available facilities for immediate, easily readable projection or production of electronic storage media images and for producing easily readable images.

(vi) Be ready at all times to provide any copy pursuant to its CPS.

(vii) Store separately from the original a duplicate copy of the record stored on the medium acceptable for the time required.

(viii) Organize and index accurately all information maintained on both original and any duplicate storage media.

(B) At all times, a PKI service provider must be able to have such indexes available for examination as required by the relevant documentation.

(C) Each index must be duplicated and the duplicate copies must be stored separately from the original copy of each index.

(D) Original and duplicate indexes must be preserved for the time required for the indexed records.

(i) The PKI service provider must have in place an audit system providing for accountability regarding inputting of records required to be maintained and preserved in electronic storage media and inputting of any changes made to every original and duplicate record maintained and preserved thereby.

(a) At all times, a PKI service provider must be able to have the results of such audit system available persuant to the applicable documentation.

(b) The audit results must be preserved for the time required for the audited records.

(ii) The PKI service provider must maintain and keep current all information necessary to access records and indices stored in the electronic storage media; or place in escrow and keep current a copy of the physical and logical file format of the electronic storage media, the field format of all different information types written on the electronic storage media and the source code, together with the appropriate documentation and information necessary to access records and indexes.

(iii) It is recommended that for every PKI service provider using electronic storage media for some or all of its record preservation under this section, at least one third party, as specified in its CP, CPS, or other policy document, has access to and the ability to download information from the PKI service provider's electronic storage media to any acceptable medium under this section.

(E) If the records required to be maintained and preserved pursuant to the provisions are prepared or maintained by an outside service bureau, depository, bank or other record keeping service, on behalf of the PKI service provider required to maintain and preserve such records, such an outside entity should state that the records are the property of the PKI service provider and maintain the records in the same manner as the PKI service provider.

The archival and storage procedures that a PKI determines is appropriate should appear in its documentation. The PKI should account for external requirements imposed by law or contract. Moreover, the PKI service providers should follow the documented procedures when gathering and maintaining corporate records.

D.5.7 KEY CHANGEOVER

Issue Summary. This section concerns the procedures by which a CA in particular makes its public key available to relying parties within its domain after a CA has undergone a rekeying procedure.

Relevant Considerations. As mentioned below in PAG § D.6.3.2 (Usage Periods for the Public and Private Keys), key pairs have limited usage periods. Limiting the usage period reduces the possibility that an attacker can discover the private key by cryptanalytic attack. If keys have a limited usage period, however, new keys will need to be generated in order to replace the ones that are being discontinued. Once new keys are generated, new certificates are needed to bind the new public keys to the entities holding them. In turn, it will be necessary to provide relying parties with access to these new certificates to permit them to perform cryptographic operations.

As discussed in PAG § D.6.1.6 (CA Public Key Delivery to Users), it is necessary for relying parties to receive CA certificates in a secure fashion to prevent an attacker substituting the wrong public key for the real public key. Once a CA has generated a new key pair following the decommissioning of the old key pair, the factors applicable to distribution of CA public keys will be applicable to ways in which the CA can securely distribute a new certificate containing its new public key. The Relevant Considerations under PAG § D.6.1.6, therefore, are applicable here.

Appropriate Requirements and Practices. The objective of the key changeover is to provide an uninterrupted PKI service to subscribers. CA certificates are needed to verify the digital signatures in the certificates issued by the CA as part of the cryptographic processes that relying parties perform, and if the CA certificate expires, then relying parties cannot perform these processes securely. Thus, a PKI will want to manage the procedures by which CA keys are replaced and recertified to establish a controlled and managed process.

That process should be reflected in the PKI's documentation, which should dovetail with any applicable external requirements, such as those imposed by applicable law or contract. CAs, then, should adhere to the PKI's documentation when performing CA key changeover operations.

D.5.8 COMPROMISE AND DISASTER RECOVERY

D.5.8.1 Computing resources, software, and/or data are compromised or corrupted

Issue Summary. This section concerns the procedures that a PKI requires or has in place to respond to security incidents and compromises involving security breaches or corruption of computing resources, software, and/or data.

Relevant Considerations. Assessors should consider the need for security with respect to PKI participants' services and ascertain whether regulatory or contractual requirements dictate certain incident and compromise handling procedures. They should review the PKI's documentation to see if it contains procedures that include responses to the compromise or corruption of computing resources, software, and data. Assessors should also determine whether PKI participants do, in fact, comply with such proceduresIncident and compromise handling procedures are a critical function of PKI participants. Such procedures enable a participant, upon detection of an incident or compromise, to handle the event smoothly to minimize disruption, provide an effective response

[369] *See* DSG, *supra* note 2, § 3.13 at 76.

that closes any security vulnerabilities, maintain trustworthy operations, and prevent future similar incidents and compromises.

Appropriate Requirements and Practices. The PKI service provider should have a plan to preserve and authenticate online data and corporate records, in the event that computing resources, software, and/or data are compromised or corrupted through (for example) systems failure, natural disaster, or hostile attack. It may be helpful for the plan to include procedures to isolate the damage and to repair it or replace it with backups. PKI service providers should maintain policies and procedures that comply with ongoing developments in critical infrastructure protection, as applied to the service provider's business model, security environment, and operational assumptions, as well as applicable laws and contractual requirements.[370]

Significant security events should be reported to the appropriate PKI personnel on a timely basis. For all PKI assurance levels, the PKI software will likely want to ensure that the PKI personnel responsible for audit verification of any critical security events or discrepancies are notified as they are logged. For other security events, the required timing of notification should be driven by the requirements in the PKI's documentation.

D.5.8.2 Secure facility after a natural or other type of disaster

Issue Summary. This section relates to the facilities of a PKI participant that a PKI requires or establishes in order to resume operations of some or all of the participant's operations following a natural or other disaster.

Relevant Considerations. Disasters cannot be predicted, but their effects can be mitigated by thoroughly planning for what to do when they do occur. The key consideration for planning for disasters is determining procedures and arranging for facilities and systems intended to provide business continuity. To the extent a PKI provides services that individuals and organizations depend upon, they will want assurances that the services will be available notwithstanding disasters.

One of the options available to PKI participants to provide continuity of operations is ensuring that appropriate backup procedures and systems are in place that can be used in case the data on operational systems become corrupted or otherwise unusable. Disaster recovery procedures can then permit PKI participants to restore the data to systems that can continue operations.

In addition to maintaining backups, another option to ensure business continuity is the use of special disaster recovery facilities or equipment in which backup data can be used to restore operations. Such facilities and equipment can be on site at a participant's facility, such as redundant or backup systems. Another option is the use of off site facilities in which backup systems can recover operations. Off site facilities, especially ones that are geographically separated from a main facility provide more assurances of continuity than on site facilities, because the compromise or destruction of a main facility may affect any redundant or backup systems located there.

Assessors should determine which types of disaster recovery procedures, facilities, and systems make sense for a given PKI, subject to regulatory and contractual requirements. They should then review the PKI's documentation to see if it accounts for these disaster recovery needs. Lastly, assessors should determine whether, in fact, PKI participants have established disaster recovery procedures, facilities, and systems that comply with the requirements and practices in the PKI's documentation.

[370] As of December 2000, the United States has drafted a National Plan to address the protection of critical infrastructures, including although not specifically focusing on critical information infrastructures, which is under peer review and redraft in preparation for the issuance of National Plan version 2.0. Similar efforts are known to be under way in Canada, the European Union, and Australia, and are expected to be quickly initiated in most of the developed world. It is anticipated that, due to the lack of international harmony and immature understanding of precise cross-sectoral commonalities, the development of standards for critical information infrastructure protection will emerge and change rapidly until at least 2010.

Appropriate Requirements and Practices. A PKI should have a business and operational continuity plan for prompt resumption of the business after disasters. The PKI will likely want to include procedures to either recover or to shut down operations after a disaster, secure the primary facility, and transfer operations to a backup system (possibly at a secondary location), as well as procedures describing how the personnel involved in the recovery operations will be contacted and relocated if need be, and a backup plan for worst case scenarios. One useful feature of a continuity plan is provisions to address bankruptcy or other business interruptions, such as denial of service, of PKI service providers.

The validity of the trust provider's disaster recovery plan should be measured against acceptable industry standards for similarly placed enterprises and any applicable external requirements, such as those imposed by law or contract. It may be helpful to refer to disaster recovery plans that have been successfully implemented to determine the merit of the plan in place, as well as to the reputation of the consultants and/or insurance agencies that have signed off on the disaster recovery plan. Planned and unplanned testing of the disaster recovery plan should be considered annually based upon the level of the PKI. Ultimately, PKI service providers will want to adhere to the business and operational continuity plan so that they can demonstrate their disaster recovery capabilities.

D.5.8.3 Entity public key certificate is revoked

Issue Summary. This section concerns the procedures that a PKI participant (usually a CA) must or does follow in the event that the certificate containing its public key is revoked.

Relevant Considerations. Revocation of a certificate containing a public key can occur for a number of reasons. *See* PAG § D.4.9.1 (Circumstances for Revocation). In the case of a CA voluntarily seeking or initiating revocation of its own certificate, revocation may be in response to a CA private key compromise (*see* PAG § D.5.8.4 (Entity private key is compromised)), change of CA, or the termination and transition of service to another CA. Involuntary revocation of a CA's public key may result from the issuing CA discovering a subject CA's private key compromise, the subject CA's unreliability, or its termination of the subject CA by the issuing CA.

Assessors should determine, given the possible scenarios of revocation, which procedures make sense for a PKI in terms of reestablishing operations, rekeying the CA, and possibly revocation of certificates that had been issued by the affected CA. They should consider any external requirements, including those imposed by law or contract. Finally, assessors should check to see if PKI participants are, in fact, following the post-revocation procedures described in the PKI's documentation.

Appropriate Requirements and Practices. The issuing CA has responsibilities with regard to notifying the appropriate relying parties in a timely manner that its public key has been revoked and the reason for revocation. Notification of revocation may include information about:

- any referral, peering, or caching CA,
- the publisher of any applicable CRL, and
- other appropriate relying parties.

Only the most extreme circumstance should cause a moderate or higher assurance CA's public key certificate to be revoked. However, where revocation is required, the CA should have a plan in place to get notice of that revocation to every RA in the CA's chain, all non-affiliated subscribers, affiliated directories, CRL providers, and known relying parties.

For CAs offering any but the most rudimentary levels of trust assurance, there should be an investigation and a plan put into place to preclude, so far as possible, the re-occurrence of the reasons resulting in the revocation.

Where the revocation is due to uncontrollable circumstances, such as the CA facility being destroyed by a tornado or other natural disaster, then efforts should be put into constructing a more resilient facility. But where the flaw is found to be preventable due to failure of procedural controls, to plans designed to overcome such failings must be put into place and strictly adhered to, if the CA would retain its level of trust assurance.

In sum, a PKI should document its post-revocation requirements and practices, which should reflect any applicable external regulatory or contractual requirements. CAs within the PKI should adhere to these procedures in their revocation planning.

D.5.8.4 Entity private key is compromised

Issue Summary. This section concerns the procedures that a PKI participant (usually a CA) must or does follow in the event that the security of its private key is compromised.

Relevant Considerations. The compromise of a CA private key is potentially the most serious type of compromise in the security of a PKI. Therefore, a compromise of a CA's private key may call for special requirements or procedures to mitigate the harm that could arise from the compromise.

Assessors should determine, based on the circumstances of the PKI, what kinds of procedures make sense for responding to a CA private key compromise. They should determine whether or not the PKI has documented such procedures, and the documentation should account for external requirements. Finally, assessors should determine whether or not PKI participants maintain, test, and (if necessary) execute the proper compromise procedures in accordance with the PKI's documentation.

Appropriate Requirements and Practices. CAs and the CAs that have issued them certificates typically have responsibilities with regard to notifying others in a timely manner that a CA private key has been compromised. For all but the most rudimentary PKI, the procedure following a compromise begins with revocation of the CA certificate corresponding to the compromised private key. Thus, the Appropriate Requirements and Practices from the previous section apply here as well. It may be helpful for PKI documentation to mention the post-revocation practices of CAs in the sections corresponding to PAG § D.5.8.3 (Entity public key certificate is revoked), state in the compromise discussion corresponding to this PAG section that the first response to a compromise is revocation, and otherwise cross-reference the PKI documentation corresponding to PAG § D.5.8.3.

D.5.9 CA TERMINATION

Issue Summary. This section concerns the procedures that a CA wishing to terminate its services within, or interoperation with, a PKI must undertake in order to minimize the disruption caused by the termination and, if applicable, assist in the transition of its services to another CA.

Relevant Considerations. CA termination is potentially a highly disruptive event. The subscribers and relying parties may have come to rely on the CA's services. Assessors should consider the business model of the PKI when determining what practices a PKI should implement to minimize disruption. Assessors should also account for any requirements in applicable law or contracts. Finally, they should determine whether or not CAs are planning for termination and adhere to termination procedures when CAs are terminated.

Appropriate Requirements and Practices. PKI service providers should make commercially reasonable efforts to notify subscribers of a planned termination.[371] Commercially reasonable efforts should be made to notify all affected parties. In particular, relying parties should be notified when a CA is no longer actively vouching for the bindings between public keys and identities.

[371] *See generally* DSG, *supra* note 2, § 3.13.

Entities that rely on a CA's CRL should be notified when the CA stops issuing them so they can re-evaluate the trust they have put into that CA. Otherwise, a relying party may be under a false assumption that a certificate not listed on the last CRL is still valid, although in reality the CA has stopped generating CRLs (and certificates).

It may be possible for a CA to "terminate" without its root key being revoked, such as where one CA is acquired by another. Wherever possible, minimization of disruption to subscribers and all other affected parties should lead the acquiring organization to have a plan in place to migrate subscribers over time to the new organization, in the natural course of certificate expirations.

Where the CA is terminated and no option exists but the revocation of all certificates within that CA's chain, it is imperative that a plan be in place to give notice to all affected parties, and that the plan be adhered to in its administration. Moreover, a process should be in place to continue revocation services so that there is no inference based on the discontinuation of revocation information that all otherwise operational certificates may be relied upon.

The PKI should memorialize its termination requirements or practices in its documentation, which should be consistent with external requirements imposed by law or contract. Finally, CAs should adhere to these requirements and practices by planning for termination and, where termination occurs, implementing termination procedures in accordance with the PKI's documentation.

D.6 Technical Security Controls

This section presents the technical security controls used in whole or in part by a PKI to select such things as key size, cryptographic algorithm(s), and delivery mechanisms. Other topics include: (a) the secure performance of such functions, such as key pair generation, private and public key delivery, and parameter generation, (b) private key protection, and (c) computer security controls.

D.6.1 KEY PAIR GENERATION AND INSTALLATION

D.6.1.1 Selection of Algorithm

Issue Summary. This section addresses the issue of which cryptographic algorithms and hash functions subscribers will use when performing digital signature operations and CAs will use when signing certificates.

Relevant Considerations. The selection of a cryptographic algorithm can affect numerous aspects of a PKI, including interoperability, security, and performance. If the selected algorithm is weak or subject to attack, then the resulting value of digitally signed documents or the security of the encrypted information will be diminished.

There are many encryption algorithms in use today, although the most commonly used algorithms for signing functions are the RSA algorithm and the Digital Signature Algorithm defined in the Digital Signature Standard.[372] One effort to enhance efficiency of cryptographic operations involves the use of elliptic curve cryptosystems, such as the elliptic curve variant of DSA known as the Elliptic Curve Digital Signature

[372] *See, e.g.*, PAG APP 2 (*Cryptographic Algorithms for Use by CAs within the Gov't of Canada PKI*, Gov't of Canada (2000), p. 3, *available at* <http://www.cio-dpi.gc.ca/pki-icp/documents/documents_e.asp>, hereinafter "Canadian Algorithms"). Other supported algorithms include DSA and E1-Gamal. *Id*.

Algorithm.[373] By far, however, the most common algorithm in use is RSA. The most common hash functions used for signing certificates are the U.S. government's Secure Hash Algorithm (SHA-1)[374] and RSA Security's MD5 algorithm.

An assessment of the appropriateness of an algorithm that a PKI may choose or has chosen should consider the following:

- Cryptographic strength or its resistance to attack.
- The level of computational efficiency. Some strong algorithms require a significant time for encryption, decryption, signing, and signature verification. As such, the relative speed of an algorithm must be assessed. In addition, the available computing power may play an important role in selecting an algorithm, as a given algorithm may perform at an acceptable level in a Windows-based PC, but perform unacceptably in a cellular phone.
- The required key size produced by the algorithm. Key sizes cannot be easily compared because different algorithms require different key lengths to produce the same relative cryptographic strength. For example, an ECC algorithm using a 163-bit key may be equivalent to an RSA algorithm using 1024 bit keys. The available storage space may dictate the use of an algorithm that produces smaller sized keys.
- Evaluation of Algorithm. It is generally accepted that the strength of the algorithm should not be based on the secrecy of the algorithm. Algorithms that have been subject to public scrutiny would generally be considered stronger than those that have not.
- Message digest size is also important. Message digests should be as secure as the signature algorithm.
- Interoperability may be required throughout the PKI. For example, SSL sessions requiring client authentication would need to support the algorithm used in the client digital certificate.

Assessors should review the PKI's choice of cryptographic algorithms in view of the factors above and any external factors imposed by contract or applicable law. They should also review the PKI's documentation to determine if it adequately discloses the applicable requirements for or use of the chosen algorithms. Finally, an assessment should include an analysis of whether CAs and subscribers actually use the PKI algorithms required or disclosed within the PKI's documentation.

Appropriate Requirements and Practices. The choice of cryptographic algorithm and hash function will likely be driven by the applications for which the certificates are intended and the assurance level provided by the certificates. The algorithms and hash functions chosen by the PKI should be appropriate in light of the security needs of the applications and meet any externally-imposed requirements. The ability to resist attack and the degree of public scrutiny will be relevant to this analysis.

A PKI should also pick algorithms and hash functions that are practical in the context of the application. The factors relevant here are computational efficiency and whether certain legacy applications work with only certain cryptographic algorithms and hash functions. Interoperability may also narrow the choice.

Assuming that the PKI has chosen appropriate cryptographic algorithms and hash functions, the PKI's documentation should require or disclose the use of these algorithms and hash functions. Lastly, the actual use of algorithms and hash functions within the PKI should match what the PKI has documented.

[373] *Id.*

[374] *Id.*

D.6.1.2 Key Size

Issue Summary. This section addresses the issue of the length of key pairs used by subscribers for performing private key operations and CAs when signing certificates.

Relevant Considerations. The selection of the key size will affect the overall strength of the protection available. In general, the longer a key's length, the stronger the resulting encryption or digital signature. However, the longer the key, the more time it takes to generate a key, and to encrypt and decrypt information. Additionally, the CA private keys that are used for signing certificates should have a key size representing a cryptographic strength at least as great as the strength of the public keys being certified.

When evaluating a given key size, the number of potential keys in a given key space must be considered. The longer a key is, the greater the number of keys in a key space. This reduces the risk of a brute force cryptanalytic attack and the potential for duplicate key pairs.

Rigorous, systematic assessment of the relationship between the size of a key and its cryptographic strength is a research topic, and the nature of this relationship depends upon evolving developments in information technology and in mathematical problems such as discrete logarithms and factoring. Factors that contribute to key length selection include:

- Risk assumed (e.g., potential compromise of a top level CA).
- Validity period of the corresponding certificate.
- Key length used should produce a result that is at least as strong as any key generation information conveyed within it.
- The state of the art of attack technologies.
- The ability for software to process keys of a certain length.

Assessors should review the PKI's designation of key size in view of the factors above and any requirements imposed by contract or applicable law. They should also review the PKI's documentation to determine if it adequately discloses the applicable requirements for or use of keys of the chosen size. Finally, an assessment should include an analysis of whether CAs and subscribers actually use the key sizes required or disclosed within the PKI's documentation.

Appropriate Requirements and Practices. As with the choice of cryptographic algorithm, PKIs should choose key lengths for CA and end-user subscriber key pairs that are appropriate for the applications for which the certificates are intended in light of the level of assurance provided by the certificates. The choice should be consistent with applicable external regulatory or contractual requirements. Certificates with very long operational periods should use key lengths longer than the current norm so that they are more resistant to improvements in attack technologies. Issues of software compatibility and interoperability also play a role in the choice of key lengths. If compatibility and interoperability are requirements, a PKI will likely want to use key lengths that subscriber and relying party software within the PKI can process.

Assuming that the PKI has chosen key lengths for CAs, subscribers, and other PKI participants that are appropriate, the PKI should also document key length requirements or usage in its documentation. Finally, the key lengths of the PKI's participants should actually match the key length requirements or disclosures set forth in the documentation.

D.6.1.3 Key pair generation

Issue Summary. This section concerns the controls surrounding the process by which CAs and subscribers generate their key pairs. It applies to the process by which end-user subscribers and CAs generate their own key pairs. It also applies to the process, if applicable, whereby a CA generates key pairs on behalf of subscribers. Examples include the case of key management or key escrow, where a CA may generate an encryption key pair for the subscriber, and the case of a CA generating key pairs on tokens and distributing the tokens to subscribers.

Relevant Considerations. Security within a PKI can only be assured if keys are generated correctly and in a fashion that reduces the risk that they could be compromised.[375] Several aspects of the key generation process can be assessed to determine whether the key generated meets the needs of the particular application.[376] The analysis of these processes often distinguishes between the generation of CA key pairs by CAs and the generation of the key pairs of end-user subscribers. This section may distinguish between controls over the generation of end-user subscriber key pairs by the subscriber and controls over the generation of such key pairs by the CA.

The PKI's choice or an assessor's assessment of the key pair generation process could be based on include some or all of the following factors:

- **Correct form.** Assessors may want to determine whether key pair generation is of the correct mathematical form. Assessors can perform tests (e.g., for prime numbers etc.) that are required in the applicable algorithm standards.

- **Randomness.** Assessors may want to identify the source of randomness in the key generation process. A statistical test proving randomness may be applied to the random number generator. A self-test on the random number generator may be necessary before generating keys.

- **Key generation in a trustworthy or secure environment.** A trustworthy system can be achieved in a number of ways including evaluation under a commonly accepted standard such as the Common Criteria, ITSEC etc.[377] The cryptomodule can be evaluated to the appropriate level of FIPS-140. The standards required for or met by cryptographic modules are discussed in more detail in PAG § D.6.2.1 (Standards for Cryptographic Module).

- **Control.** In some environments, only pre-defined authorized persons are allowed to activate the CA key generation process. Split knowledge access control can be required to begin the key generation process.

Often, however, a PKI sets requirements or adopts key generation practices based on whether the process must take place in hardware or software, and based on the standards that the hardware or software cryptomodules must meet. This or other sections may refer to the physical security controls of the environment in which CA keys are generated and the logging of key generation events. This section may cross-reference the more detailed sections that treat these subjects.[378] In other cases, PKI documentation may make reference to a more general

[375] *See, e.g.*, CIMS Level 3, *supra* note 325, § 5.1.3.1, ¶ 2.

[376] *Id.* (specifies FIPS 140-1, level 2).

[377] For example, ITSEC E4 is mandated for key generation and private key storage in Germany's PKI. *See* German Signature Act, *supra* note 338, § 17(1). Other technical components must conform to E2. *Id*.

[378] *See, e.g.*, PAG § D.6.1.8 (Hardware/Software key generation) and § D.6.2.1 (Standards for Cryptographic Module).

standard. For example, a PKI may be required to use "trustworthy systems and products" in connection with the key generation processes, or in connection with the provision of certification services generally.[379]

Assessors should consider the applications for which the PKI's certificates are intended, the level of assurances they purport to provide, and the security requirements for the applications in determining whether the PKI has required or is using appropriate processes for key generation. Assessors should consider the key generation process for all participants within the PKI generating keys, such as CAs and end-user subscribers. Depending on the need for thoroughness of the assessment, assessors should consider performing some or all of the analyses described in the bulleted list above. Finally, they should determine whether any external requirements bear on the key generation process, whether imposed by contract or applicable law.

Once assessors have determined whether the PKI's key generation process for different PKI participants is appropriate, they should review the PKI's documentation to determine whether the PKI adequately communicates its requirements for or use of key generation processes. Finally, assessors should determine whether the participants within the PKI adhere to the key generation processes documented in the PKI's documentation.

Appropriate Requirements and Practices. The process of key generation should occur with sufficient controls, and should result in a generated key with the strength and correctness, that are appropriate for the intended use of the key within designated applications. Key generation should be consistent with any externally-imposed requirements, such as those imposed by contract or applicable law. For most PKIs, CAs will not likely perform or commission their own laboratory tests of the cryptographic modules in which key generation occurs, although when higher assurance certificates are issued, such tests may be appropriate. Most PKIs will want to identify the person who generates key pairs for end-user subscribers. Then, for each entity generating keys, the PKI will make reference to a requirement or disclosure that key generation will take place in hardware or software and a reference to the standards that the hardware or software cryptographic modules must meet.

To ensure correct key generation, CA signature keys are commonly generated in a validated cryptographic module, under control of the CA.[380] Split knowledge access control and a trustworthy environment[381] are desirable for CA key generation. PKIs will likely want to log the act of key generation and require the attestation of the parties controlling the key generation to their participation.[382]

In terms of end-user subscriber key pairs, the default is for subscribers to generate their own key pairs. In general, this is the preferable approach because it avoids issues of possible key compromise by the CA.[383] In certain cases, however, the PKI may face a business need for a CA or other party to generate key pairs on behalf of the end-user subscriber. For example, the CA or another party may generate key pairs on hardware tokens, such as smart cards, and distribute the tokens to users. In other instances, such as where subscribers do not have

[379] An example of this approach is the requirement of trustworthy systems in the European Directive on a Community framework for electronic signatures. *See* EU Signature Directive, *supra* note 5.

[380] Use of validated modules for key generation will mitigate risk. There is a potential liability issue between the CA and the cryptographic module vendor for any defects in the key generation process.

[381] Some cryptographic modules validated at a high level may provide a self-contained trustworthy environment for key generation. In other cases a trustworthy environment may be achieved by the combination of a validated module and an evaluated secure CA workstation environment. In other cases it may be necessary to perform key generation in a "clean system," that is a system freshly installed from a trusted source that has tamper protection.

[382] These procedures are common to several international PKI schemes. *See* Japanese Guidelines, *supra* note 290, § 3.2.1-2.

[383] There is a tension between the desire to ensure that keys are generated correctly (random number generation is particularly problematic in this respect), and are therefore secure, the desire to make the user accountable, and to offer no dilution of nonrepudiation due to the actions of the CA. CA generation of user keys, or use of a key generation mechanism provided by the CA opens the issue of possible compromise by a CA that generated the private key, or a claim that the user generated the private key with a defective mechanism provided by the CA.

an environment suitable for key generation, the CA or a third party may generate key pairs, and provide them to users by a secure means (e.g., in a strongly-encrypted message).

Another instance in which subscribers may not generate their own key pairs is where key recovery or key escrow is implemented. A CA or other party may generate end-user subscribers' key pairs on their behalf and send them to subscribers by secure means. The CA or other key escrow agent may retain a copy of the end-user subscriber's private key for later recovery, if necessary. When this occurs, the CA or other party generating keys should implement controls appropriate to the level of assurance provided by the certificates and the applications for which the certificates are intended as described above.

Once the appropriate methods of and controls over key generation are identified, the PKI should adequately document key generation requirements and practices. Lastly, the actual key generation practices of a PKI's participants match the PKI's documented requirements and practices.

D.6.1.4 Private key delivery to entity

Issue Summary. Section D.6.1.4 addresses the method, if any, by which CAs or other participants within a PKI deliver private keys to end-user subscribers.

Relevant Considerations. For a particular PKI deployment, the party who generates the key should be readily apparent. If the key owner generates his, her, or its own private key, then there is no requirement for private key delivery, and it may, in fact, be prohibited. Delivery of a private key to the user introduces a vulnerability to attack and the possibility of compromise.[384]

As mentioned in the previous section, however, there may be reasons for a CA or a third party to generate key pairs on behalf of end-user subscribers. For example, the CA may find it desirable to pregenerate key pairs on smart cards and to distribute the smart cards to end-user subscribers. In addition, the CA or other party may need to have key recovery or key escrow capabilities for end-user subscriber private keys.

In either case, the entity generating the key pair will need some method to deliver the private key to the subscriber so that the subscriber can use it for the intended applications. Moreover, the entity generating the key pairs will need to adopt controls and safeguards to address the vulnerability created by private key delivery. Appropriate considerations in the context of private key delivery include:

- the method of delivery of the private key to the key owner (e.g., across the network, a physical token),[385]
- how the key owner is authenticated (e.g., strong cryptographic-based authentication control, face-to-face recognition), and
- protection of the private key during key delivery (e.g., strongly encrypted during transmission, non-extractable from a secure token, PKCS #12, IETF Certificate Management Protocol).

Assessors should determine whether private key delivery to end-user subscribers is necessary within the PKI. If so, assessors should consider the strength of the controls in place to secure the delivery of the private key to the end-user subscriber to determine if the controls are appropriate in light of the applications for certificates and assurance levels of the certificates. They should also determine whether any external requirements, such as those under contract or applicable law, bear on the need for private key delivery and the controls over the delivery process. Assessors should also determine whether the PKI has appropriate documentation of its private

[384] *See, e.g.*, CIMS Level 3, *supra* note 325, § 5.1.3.1, ¶ 3.

[385] For example, the German PKI establishes in-person transfer of private keys as the default mode of delivery. Subscribers may request in writing different means of transfer. *See* German Signature Act, *supra* note 338, § 6.

key delivery requirements or practices. Finally, they should determine whether PKI participants actually deliver private keys in accordance with its documentation.

Appropriate Requirements and Practices. The PKI should identify the situations, if any, in which private key deliver to end-user subscribers. This decision should be consistent with any applicable external requirements, such as those placed on the PKI by contract or applicable law. In general, it is preferable for users to generate their own keys, since this eliminates any possibility of compromise during the delivery to the user. In PKIs where end-user subscribers are required to generate their own private keys, the PKI may want to prohibit private key delivery; there is no reason for the delivery of private keys in this case.

Some users, however, may lack the capability to generate keys. Commonly used algorithms require that keys meet strict mathematical criteria, which may require the generation of a number of trial keys and extensive tests of those keys before one is accepted. In each case it is necessary to begin the process with a suitable "random" seed. While there are many techniques for obtaining this random value, this is an area where problems have commonly arisen. A CA can ensure the quality of user keys by undertaking to generate them itself. Further, when a business requirement exists for pregenerating key pairs on tokens and key escrow/recovery, the CA or other party will need to delivery private keys to end-user subscribers.

Assuming that a reason exists for delivering private keys, the delivery method used should integrate controls commensurate with the assurance level provided by the certificates and the security needs of the applications for which the certificates are intended. Controls over token distribution often center on issues of the physical security of the tokens at the location where the keys are generated, through the distribution process, and to the point where the tokens are delivered to the end-user subscriber, as well as showing a chain of custody from manufacturer to subscriber. Controls concerning keys generated in a key recovery or key escrow system often concern the encryption or other security over the data structure containing the end-user subscriber's private key. The PKI may want to adhere to a standard for the communication to the subscriber, such as PKCS #12 or the IETF Certificate Management Protocol.

In any case, the PKI should document whether or not private key delivery occurs or not, and if so, the situations in which it is appropriate. The PKI documentation should clarify the security controls surrounding the delivery of private keys. Finally, the actual delivery of private keys within the PKI should match the practices required or disclosed within the PKI's documentation.

D.6.1.5 Public key delivery to certificate issuer

Issue Summary. This section relates to the method by which an end-user subscriber presents his public key to the CA so that the CA can issue a certificate to the subscriber that contains the public key. This process is applicable only where the subscriber generates his, her, or its own key pair.

Relevant Considerations. Since a certificate contains the public key of the subscriber, the CA needs to obtain the public key before it can issue a certificate containing it. If end-user subscribers generate their own key pairs, they need to deliver their public keys as part of the enrollment process, so that the CA can return a certificate containing the public key. If, however, the CA generates key pairs on behalf of subscribers, the CA will already have the public key when a certificate is requested and delivery to the CA is unnecessary. If delivery of the private key is necessary because subscribers generate their own key pairs, various controls are available to give the CA assurances that the public key originated from the certificate applicant and assurances of the integrity of the public key demonstrating that an attacker has not tampered with or substituted the public key to be certified.

For instance, a CA could establish an enrollment process requiring the software of certificate applicants to convey public keys to it during an online session in a message structure that complies with a certificate management protocol securing the delivery of the public key. Examples include PKCS #10 and the IETF Certificate Management Protocol. The use of this process may accompany the process by which certificate

applicants demonstrate that they possess the private keys corresponding to the public keys to be certified.[386] A CA could also require that the certificate applicant physically deliver the public key to the CA.

Assessors should determine whether public key delivery is necessary within a PKI, based on the decision as to who will generate end-user subscriber key pairs. If public key deliver is necessary, assessors should determine whether controls over the public key delivery process are feasible and appropriate for the PKI. If so, they should review the PKI's documentation to determine if the PKI requires or discloses the use of such controls. Lastly, assessors should examine whether the enrollment process actually used within the PKI implements the controls listed in the PKI's documentation.

Appropriate Requirements and Practices. If the subscriber generates the key pair, then a CA will likely want to use public key delivery mechanisms that ensure the integrity of public keys and the identity of the certificate subject. The CA will want to know that the public key comes from the prospective certificate subject holding the corresponding private key[387] and that public key delivered to the certificate issuer has not been altered. For instance, the CA may want to verify that the subject possesses the corresponding private key by using a process requiring the subject to use that private key to digitally sign a certification request sent to the CA.

There are many scenarios for registration and delivery of the public key to the CA. The IETF PKIX standards offer a flexible framework for supporting many of these scenarios. PKIs frequently provide for controls by requiring or using mechanisms consistent with certificate management protocols such as PKCS #10 or the IETF Certificate Management Protocol. The procedures used to communicate the public key to CAs should authenticate the source of the key to be the certificate subject, and prevent its alteration.

Ultimately, the choice of which controls a PKI will require or use for public key delivery to the CA, if any, will depend on who generates key pairs for end-user subscribers and the security needs of the PKI. The security needs of the PKI will depend on the assurance levels provided by the certificates and the types of applications for the certificates. Practical choices may be required. For instance, physical delivery of public keys to the CA may not be feasible if the PKI is based on a model of online enrollment. Whatever controls are in place should be consistent with any requirements applicable to the PKI based on contract or applicable law.

Assuming that the PKI has designated public key delivery mechanisms that are appropriate for the PKI, the PKI should document these controls in its documentation. Finally, assessors should ensure that the enrollment mechanisms make use of the public key delivery controls required or disclosed in the PKI's documentation.

D.6.1.6 CA public key delivery to users

Issue Summary. This section addresses the process by which a CA distributes its public keys to potential relying parties, usually in the form of a CA certificate.

Relevant Considerations. Relying parties base their trust on the public keys of CAs and validated certificate paths from those keys.[388] For example, when verifying a digitally signed message, the relying party obtains the subscriber's public key from the subscriber's certificate. The certificate is itself a digitally signed data structure, and the relying party needs to verify the signature on the certificate by using the CA's public key. Therefore, the relying party will need to obtain the CA's public key.

[386] *See* PAG § D.3.2.2 (Method to Prove Possession of Private Key].

[387] For more information, *see* PAG § D.3.2 (Processing of a Certificate Authority).

[388] Other PKI service providers that provide revocation services may also provide digitally signed certificate revocation lists and OCSP responses on which relying parties may need to rely. In that case, the relying party will also need the public keys of these PKI service providers.

A CA's public key is conventionally contained in a CA certificates, *i.e.*, certificates issued to CAs containing their public keys. A single CA issuing certificates within a PKI may simply provide relying party a certificate that it has issued to itself containing its own public key, called a "self-signed" certificate. In a more complex PKI, however, there may be multiple CAs, most commonly in a hierarchical structure. When CAs at the bottom of the hierarchy of CAs issue certificates to end-user subscribers, the relying party may obtain the certificate of the issuing CA as part of the data structure of the communications the relying party is using. For example, the recipient of a digitally signed message may receive, as part of the message structure, certificates issued to CAs below the top CA in the hierarchy (called the "root CA"). The process of relying on the end-user subscriber certificate will, in this case, involve verifying the digital signature on the end-user subscriber's certificate, the certificate issued to the CA issuing the certificate, and all certificates of CAs above it in the hierarchy. At the end of this "chain" of certificates is the self-signed certificate issued by the root CA to itself (the self-signed root certificate). In this type of PKI, the PKI may simply need to ensure that relying parties obtain the needed root certificate, as opposed to the certificates of all of the CAs in the chain, if relying parties otherwise receive the other CA certificates in the chain, if relying parties otherwise receive the other CA certificates in the chain.

Whether the PKI consists of a single CA, hierarchy of CAs, or other structure, the self-signed CA certificate enabling the relying party to verify the signatures on certificates and perhaps ultimately a digitally signed message being verified is sometimes referred to as a "trust anchor." Often, a PKI will have security controls surrounding the process by which trust anchors are provided to relying parties. Relying parties will want to know that the certificate containing the CA key originated from the CA, and not an attacker trying to substitute a different certificate.

A PKI may require or use different techniques to distribute CA certificates that act as trust anchors with varying degrees of security. Some CAs may simply post a trust anchor on a web site or in a repository, which, without other security measures, entails no specific authentication assurances. CAs may also establish a web site from which relying parties can obtain the CA certificate in a secure sockets layer session. SSL provides assurances in this case that the relying party is in communications with the site of the real CA, as opposed to an attacker. In many instances, CAs are able to make arrangements with the manufacturers of relying party software to have their trust anchors placed within the software. When this mechanism is used, the trust anchors have already been distributed in a reliable fashion to relying parties without the need for special distribution mechanisms. Finally, a CA or other party trusted by the CA (such as an RA) may directly provide the CA key to the relying party during a face-to-face meeting at the time of initial registration.

The rekeying of CA certificates as their expiration date approaches raises the issue of how the new CA certificates resulting from the rekeying process can be distributed in an authenticated fashion. The mechanisms described above can be used to provide the new CA certificates. A PKI, however, may also implement additional controls to demonstrate the transition from the old CA certificate to the new CA certificate. For instance, signing the new key with the old key before its expiration or compromise can authenticate a CA re-key. PKIX protocols require the issuance of three certificates that are posted to the repository:

- the new CA public key signed with the old CA private key,
- the old CA public key signed with the new CA private key, and
- the new CA public key signed with the new CA private key.

Another common technique is to include a cryptographic hash of the next CA key in the current CA self-signed certificate. This hash can then be used to authenticate the new key when it is used in a self-signed certificate.

Assessors should determine whether the PKI has required or disclosed a CA public key distribution process and a set of security controls around that process that matches the structure of the PKI and its security needs. They should account for any externally imposed requirements, such as those under the relevant contracts or applicable law. The should also review the PKI's documentation to determine whether the PKI has adequately expressed

the CA public key distribution process. Finally, assessors should determine whether CAs distribute their public keys and implement security controls in the distribution process in accordance with the PKI's documentation.

Appropriate Requirements and Practices. PKIs should aim to establish a CA public key distribution process and associated controls that are feasible under the structure of the PKI, match the business needs of PKI participants, and are commensurate with the level of assurances provided by the certificates. If the PKI is intended for a small community of relying parties, especially one within a single organization, manual processes performed by relying parties to place trust anchors within their systems manually may be feasible. Technicians or administrators may even be able to perform these functions on behalf of relying parties. If, however, the PKI encompasses a large, distributed community of relying parties, it may not be feasible to require relying parties to obtain trust anchors and install them in software manually. This concern also applies if the PKI has a strong business need for simplicity and usability in connection with the configuration of relying party software. When these factors apply, the PKI may find it appropriate to place their trust anchors in the software used by relying parties.

The controls chosen for securing the CA key distribution process will largely be driven by the applications for the certificates and the level of assurances provided by the certificates. For lower assurance certificates, it may not be necessary to provide any security surrounding the CA key distribution process. For higher assurance certificates, however, distributing CA keys typically occurs by pre-placement in software, SSL sessions, or manual distribution.

A CA re-key, particularly in the case of a key compromise, is a significant event. PKIs should have a mechanism to securely maintain and modify the key values and/or certificates of the trusted anchors to account for the lifecycle of CA keys. The methods to distribute a CA's new public key following a re-key will likely be the same as those used to distribute the CA's original public key, but need not be.

Whatever CA public key distribution processes and controls chosen should be appropriate for the PKI and should be communicated clearly in the PKI's documentation. Finally, the CA public key distribution processes and controls actually implemented by the PKI should match what it has documented.

D.6.1.7 Public key parameters generation and quality

Issue Summary. This section applies when end-user subscribers or CAs use the Digital Signature Algorithm (DSA) or the Elliptic Curve Digital Signature Algorithm (ECDSA) for digitally signing messages or certificates. It concerns the parameters required by the use of DSA or ECDSA for the generation of keys and digital signatures. More specifically, this section addresses the issue of who generates such parameters for the PKI and the issue of which controls govern the quality of the parameters.

Relevant Considerations. The DSA and the ECDSA make use of certain parameters in connection with the generation of a private key and public key (which themselves are parameters) and the generation of digital signatures. Some of the parameters, known as p, q, and g can be public and can be used and shared by a community of users. The RSA algorithm, however, does not require the generation of parameters. Since the participants of most PKIs in operation today make use of the RSA algorithm, PKI documentation may state that this section does not apply.

In PKIs in which participants use DSA or ECDSA, each user could in principle use different parameters. In most cases, however, all the participants within a PKI will share common parameters. End-user subscriber systems normally need not include the capability to generate parameters. Since the parameters for DSA are larger than the public key, they are normally specified only in CA certificates that may start a certification path, and are "inherited" by subordinate certificates.

The quality of the parameters to be used in a PKI can affect its security. Incorrectly generated parameters will degrade the trustworthiness of the PKI. FIPS 186 and X9.30 state requirements for DSA parameter generation.

A CA may check the quality of the parameters of the certificates it issues. More specifically, the CA may validate the correctness of any parameters it uses in its own certificate or includes in end-user subscriber certificates that it issues.

Assessors should determine whether a PKI's participant have a need to use DSA or ECDSA. If so, they should determine whether CAs within the PKI have generated parameters for their domains. They should be mindful of any external requirements, imposed by contract or applicable law, that compel them to generate parameters in this way. Assessors should check PKI documentation to determine if the PKI has documented the method of generating parameters and whether the parameters used within the PKI have, in fact, been generated as described in the documentation.

The accreditation aspects of parameter generation and the quality of parameters are best addressed in the laboratory context of cryptographic module validation. Assessors should determine whether such laboratory testing is appropriate in light of the type of PKI and the assurance level provided by certificates. As an alternative, they may simply verify that validated modules have been used. Assessors should also check the parameters of the CA certificate. Assessors should review the PKI's documentation of controls employed with respect to the quality of parameters and ascertain whether the generation of parameters within the PKI is in accordance with the documented controls.

Appropriate Requirements and Practices. To the extent PKI participants have a need to use DSA or ECDSA, CAs within a PKI will likely want to provide public key parameters required by participants within their domains. Public key parameters are typically generated in accordance with a standard such as FIPS 186 or X.9.30. The method of generation should also adhere to any external contractual or regulatory requirements. Where parameters are required within a given domain, PKI documentation should provide ample notice of them so that participants can utilize them. The parameters used within a domain should match the ones required within the domain of the PKI.

The method of determining and controlling the quality of parameters should be appropriate in light of the security needs of the PKI. It is likely that the PKI will want to require that the quality of the parameters be checked upon generation in accordance with an applicable internationally-recognized standard, such as with FIPS 186. The PKI should adequately document controls over the quality of parameters, and the controls used within the PKI should match the PKI's documentation.

D.6.1.8 Hardware/Software key generation

Issue Summary. The issue in this section is whether PKI participants must generate their key pairs in hardware cryptomodules or whether they may generate them in software.

Relevant Considerations. Cryptographic operations may be performed in hardware or software cryptomodules. Hardware generally offers greater protection of the information held inside the cryptomodule, although there has been recent discussion of vulnerabilities of cryptographic modules on smart cards. Hardware modules can provide a sheltered and controlled environment for key generation and storage. In addition, hardware modules can include a "hardware" random number generation capability that, in principle, may be superior to software techniques. Nevertheless, keys generated in hardware cryptographic modules are not necessarily better than those generated by software on a general-purpose computer. Software modules can offer flexibility in that algorithm can be replaced cost-efficiently.

In general, it is only necessary to generate a single random number as a "seed" to a cryptographically strong pseudorandom number generator in order to generate a sequence of a nearly arbitrary length of "random" numbers to be used as keys. Pragmatically, there are a number of sources of randomness available to system implementers that can be used to incorporate enough entropy in the generation of that initial seed. Considerable care may be needed to ensure that sufficient entropy is incorporated. Also, the internal state of the pseudorandom number generator must be kept secret; if it is compromised, then at least all future keys are

compromised. In principle, hardware generators have no such vulnerability, as their current state indicates nothing about their future output.

The analysis of the hardware/software issue may differ for CA key pairs and end-user subscriber key pairs. For end-user subscribers, hardware modules may be too expensive to be cost-effective, especially in the context of lower assurance certificates. Also, end-user subscribers may face distribution, installation, and usability issues with hardware modules. It may be that the security benefits of using hardware modules are not worth the effort needed to overcome these issues. By contrast, CAs do not face the distribution issues of end-users and given the central role of the CA private key, the PKI may find it appropriate to use hardware to protect CA private keys. Since CAs presumably have the expertise to install and use hardware modules, they do not face the same installation and usability issues that end-user subscribers do.

Assessors should determine whether hardware or software cryptomodules are appropriate for CAs, subscribers, and other participants in light of the security needs of the PKI and the assurance levels provided by the certificates. Where hardware modules are used, assessors should determine whether the PKI adequately handles the distribution, installation, and usability issues. Where software modules are used, assessors should determine whether it is possible for the PKI to impose adequate procedural controls to maintain a secure environment for the key generation process. Assessors should also review the PKI's documentation to see which kinds of cryptomodules, hardware or software, are required or used within the PKI. Finally, assessors should determine whether PKI participants are using the type of cryptomodules required by the PKI's documentation.

Appropriate Requirements and Practices. In general, hardware cryptomodules are appropriate for CA private keys for CAs. For CAs issuing certificates providing rudimentary levels of assurance, however, software cryptomodules may be adequate, depending upon the circumstances. Given the distribution, installation, and usability issues, hardware cryptomodules are not widely used by end-user subscribers. Therefore, the use of end-user hardware cryptomodules is generally associated only with the use of certificates providing high levels of assurances. Ultimately, the choice between hardware and software will depend on the applications for which the certificates are intended and the security needs of the participants.

Whichever cryptomodules are appropriate for a PKI, the PKI should document its requirement or use of either hardware or software in its documentation. Moreover, the cryptomodules actually used by PKI participants should match those required or disclosed in the PKI's documentation. Independent validation to a generally accepted cryptomodule standard (i.e., FIPS 140) is useful for independent validation of the implementation to its documentation.

D.6.1.9 Key Usage

Issue Summary. This section governs the purposes for which public keys within certificates may be used. When the PKI makes use of X.509 version 3 certificates, this section will also cover the uses for keys reflected in the key usage extension.

Relevant Considerations. The Key Usage extension, if present, specifies the uses for which a public key in a certificate is or may be used. The extension consists of independent bits, each indicating a separate usage that occurs or is allowed if that bit is set. The bits specify separate cryptographic operations for which the key may be used (e.g., key agreement, data encipherment) or specific data structures that may be signed with the key (e.g., certificates and CRLs).[389] More specifically, X.509 describes the different bits that can be set in the Key Usage extension as follows:

[389] According to the X.509 standard, if the Key Usage extension is marked as critical (i.e., with the critical flag set to TRUE), the CA is indicating that the public key in the certificate should only be used for the purposes indicated by the bits in the Key Usage extension. By contrast, if the extension is not marked as critical (i.e., with the critical flag set to FALSE), the CA is indicating that the public key in the certificate is appropriate for the purposes indicated by the key usage bits. Nonetheless, use is not restricted to the usages identified in the Key Usage extension. The relying party has the discretion to use the certificate

a) **digitalSignature**: for verifying digital signatures that have purposes other than those identified in b), f), or g) below;

b) **nonRepudiation**: for verifying digital signatures used in providing a nonrepudiation service, which protects against the signing entity falsely denying some action (excluding certificate or CRL signing, as in f) or g) below);

c) **keyEncipherment**: for enciphering keys or other security information, e.g., for key transport;

d) **dataEncipherment**: for enciphering user data, but not keys or other security information as in c) above;

e) **keyAgreement**: for use as a public key agreement key;

f) **keyCertSign**: for verifying a CA's signature on certificates;

g) **cRLSign**: for verifying a CA's signature on CRLs;

h) **encipherOnly**: public key agreement key for use only in enciphering data when used with **keyAgreement** bit also set (meaning with other key usage bit set is undefined);

i) **decipherOnly**: public key agreement key for use only in deciphering data when used with **keyAgreement** bit also set (meaning with other key usage bit set is undefined).[390]

A considerable debate exists as to the effectiveness of the nonrepudiation bit in accomplishing the goal of indicating that a subscriber cannot falsely deny some action, such as digitally signing a message. Although an accurate summary of the debate is beyond the scope of the PAG, the debate is based on several factors. First, there is no general agreement as to what can be communicated by setting or clearing a single bit. A bit can only be set to TRUE or FALSE, and therefore cannot capture the nuances common in policies and contractual responsibilities. Second, preventing a person from false denial of an action in theory can occur only after the party seeking to bind the subscriber to an action has initiated and prevailed in a litigation or other dispute resolution proceeding, all appeals are exhausted, and the judgment has been executed upon. Preventing repudiation depends on the effectiveness of the dispute resolution process that can back up the use of certificates. Third, people differ as to what was intended by the adoption of the bit by the drafters of X.509. Under one view, for instance, the nonrepudiation bit may mean no more than the fact that the CA offers a nonrepudiation service to assist in preventing repudiation. Under another view, setting the nonrepudiation bit means no more than the fact that the private key corresponding to the public key in the certificate is not the subject of key escrow.

Assessors should identify the different applications for which certificates can be used and compare them to the functions indicated by the key usage bits. To the extent there is a match, assessors should determine if the PKI's documentation relating to the Key Usage field directs or discloses that the appropriate bits are set. For example, if the PKI issues certificates for end-user subscribers to facilitate digital signatures, assessors should determine whether the PKI's documentation shows that the PKI requires or does in fact set the digitalSignature bit within the Key Usage extension. Any external requirements for the setting of certain bits, for example requirements imposed by contract or applicable law, should factor into the assessment. Moreover, assessors may find it helpful to break down this analysis by certificate type, such as distinguishing between certificates issued to CAs and certificates issued to end-user subscribers. Finally, assessors should determine whether the certificates issued within the PKI set the bits of the Key Usage extension in a way that is consistent with the PKI's documentation.

Appropriate Requirements and Practices. Generally speaking, the only bits set in the Key Usage extension of certificates issued to CA are keyCertSign bit and, if the CA also signs CRLs, the cRLSign bit. Also, CA

for other purposes. Software commonly in use today, however, does not necessarily enforce the criticality flag of the Key Usage extension. Therefore, its usefulness may be limited. *See* PAG § D.7.1.9 (Processing Semantics for the Critical Certificate Policy Extension) describing the use of the criticality flag in more detail.

[390] *See* RFC 2527, *supra* note 193, § 12.2.2.3.

certificates may contain other of the defined key usage bits in, such as digitalSignature for providing authentication and integrity of on-line administration transactions.

With respect to end-user subscriber certificates, when certificates are appropriate for creating digital signatures, the digitalSignature bit is typically set, and when the certificates are used for confidentiality encryption protocols involving the creation of symmetric encryption keys, such as S/MIME, the keyEncipherment bit is commonly set. If certificates are used only for signature creation or used only for encryption purposes, for example in dual key systems involving the escrow or management of a decryption key, the signature certificate typically sets only the digitalSignature bit and the decryption certificate typically sets only the keyEncipherment bit. In any case, the certificate profile for certificates issued within a PKI should set the bits within the Key Usage extension that correspond to applications for which the certificates are intended. The PKI's documentation should disclose which bits are set for which kinds of certificates. And the certificates actually issued by CAs within the PKI should contain Key Usage extension content matching the profile set forth in the PKI documentation.

D.6.2 PRIVATE KEY PROTECTION

D.6.2.1 Standards for Cryptographic Module

Issue Summary. Section D.6.2.1 relates to the standards that cryptomodules used by a PKI's participants must or do meet.

Relevant Considerations. The technical accreditation aspects of key pair generation may be most easily addressed in the laboratory context of cryptographic module validation. Laboratories may make reference to various standards for the purpose of rating cryptomodules. One prominent standard is the FIPS 140-1 standard (which will be succeeded shortly by FIPS 140-2). FIPS 140-1[391] validation procedures include tests of random number and key generation that are appropriate to the algorithm and to the module security level. The FIPS 140-1 validation procedures include tests of the physical security mechanisms of cryptographic modules and of modules' access control features. In some jurisdictions, however, licensure or accreditation schemes may call for the use of standards other than FIPS 140-1. For instance, these jurisdictions may choose to refer to protection profiles and ratings under the Common Criteria.

Assessors should determine whether the PKI has required or disclosed the use of a particular standard by which the cryptomodules of CAs, RAs, end-user subscribers, or other entities must or are rated. Assessors should compare the standard imposed to the business requirements for security of the PKI's cryptomodules. They should also ascertain whether any externally-imposed standards apply to the PKI. Contracts, applicable law, or schemes for accreditation or licensing commonly impose such requirements. Assessors should also check the PKI's documentation to ensure that the standards required or disclosed meet internal or external requirements. Lastly, assessors should see whether the cryptomodules used by PKI participants do, in fact, meet the standards required or disclosed in the PKI's documentation.

Appropriate Requirements and Practices. The most commonly referred-to standard for evaluating the trustworthiness of hardware and software cryptographic modules is the FIPS 140-1 standard. For PKIs requiring the certification of cryptomodules based on FIPS 140-1, the level of certification will depend on the applications for which the certificates are used and the need for security and trustworthiness. As an example, for CAs issuing certificates providing low levels of assurances, it may be sufficient for the cryptomodules to be certified as meeting FIPS 140-1 level 1. This level may also be useful for RA cryptomodules. Some PKIs impose this requirement on end-user subscribers, but such a requirement may not be realistic in other PKIs.

[391] *See* PAG APP 2 (*Security Requirements for the Design and Implementation of Cryptographic Algorithms, and Modules,* FIPS 140-1 NIST (1994), *available at* <http://csrc.nist.gov/publications/fips/fips1401.htm>, hereinafter "NIST Security Requirements").

For PKIs issuing certificates providing higher levels of assurances, the certification requirement is commonly set at FIPS 140-1 level 2. In some cases, however, FIPS 140-1 level 3 is imposed as a requirement for CA cryptographic modules. One example is the European Telecommunications Standards Institute policy document for the implementation of the European Directive on electronic signatures with regard to CAs issuing qualified certificates under the Directive.[392]

In short, the rating or certification for CA, RA, end-user, or other participant's cryptographic module should match the business needs for security and trustworthiness in light of the assurance levels of the certificate and the sensitivity of the information protected. The PKI should document the requirement for or the practice of meeting the standards for cryptographic modules that these entities will implement. The documentation should account for any externally-imposed standards, such as that appearing in the ETSI signature standard. Finally, the cryptographic modules used by these participants should meet the standards set forth in the PKI's documentation.

D.6.2.2 Private Key Split Knowledge Control (n out of m)

Issue Summary. The purpose of this section is to set forth controls placed on the activation and use of a private key that involve splitting the key or splitting the activation data for the key. Controls of these types can enforce a requirement that multiple persons are needed to activate and use a private key. The requirement of multi-person control can be phrased in terms of requiring a threshold number of persons (n) out of a total number of possible persons (m) to activate and use a private key. If so, this section discloses n and m and which persons are chosen to be holders of portions of the private key or of the activation data for the private key.

Relevant Considerations. Technology to split private keys or activation data, "n of m" technology, enforces security requirements to have multiple persons possessing only a portion of the data necessary to activate the private key that enables operation of a CA, RA, end-user, or other system. If N is 3, for instance, then 3 individuals would be required to be present to activate the system (e.g., enable the CA to sign certificates or CRLs). Each person would provide their respective portions of the key or the activation data in order to operate the private key. To ensure that the unavailability of one or more of the individuals does not prevent the operation of the system, it is possible to distribute portions of material to more than 3 individuals (for example, 5 individuals) and have the system operable when any 3 of the 5 people are available.

Appropriate Requirements and Practices. Requiring multiple persons to collaborate to make the private key available for use can reduce the risk of unauthorized access. Therefore, it is often considered important in PKIs issuing certificates providing medium or higher levels of assurance to utilize an "n out of m" system to enforce multi-person control over the operation of a CA private key. In such instance, the PKI's documentation should identify the numbers chosen for n and m. Moreover, it may be helpful for the documentation to indicate whether the n out of m split knowledge control is enforced technically (e.g., Micali scheme) or is controlled procedurally (e.g., having three separate passwords to unlock the box).

Generally, the greater the risks arising from compromise, the greater should be the number chosen for n. While the circumstances will vary depending on the assurance level of the certificates provided by the PKI, lower assurance CAs may involve only dual control (n=2) enforced on the activation or use of CA private keys. Higher assurance CAs may wish enforce the requirement of having a threshold of three or more persons of a total (m) number of holders of key material or activation data in order to activate or use a CA private key. The activation and use of RA keys often entails lower risks than the activation and use of CA keys. Therefore, single user control is often permitted in connection with the activation and use of RA keys.

The PKI should document its multi-person control requirements or practices in its documentation. This documentation is helpful to influence operational manuals that permit CA or CMA personnel to operate CA

[392] *See* ETSI Signature Standard, *supra* note 317, § 7.2.1.

private keys. Finally, the practices of the PKI's participants should meet the requirements and standards set in its documentation.

D.6.2.3 Private key escrow

Issue Summary. This section concerns the extent to which a PKI requires, permits, or forbids the escrowing of private keys. The section may distinguish between private keys used in connection with the decryption of encrypted messages, and private keys used to generate digital signatures or used for access control or authentication. It may also distinguish between end-user (subscriber) private keys and the private keys of other PKI participants, such as CAs and RAs. Finally, if keys are escrowed, the section addresses any controls governing the key escrow process and the escrowed keys.

Relevant Considerations. Various products and services are available on the market to facilitate the backup and escrow of end-user subscriber private keys. Their purpose is to permit the secure storage of subscribers' private keys and permit the subscriber to obtain a new copy of the private key, in case the subscriber inadvertently destroys, loses, or otherwise is unable to use the subscriber's private key. These products and services may also provide the capability of the CA, RA, or organizational sponsor of the subscriber's certificate to recover the subscriber's private key, even without the consent of the subscriber, to decrypt data protected with that private key.

The line between "escrow" and "backup" may not be clear in all circumstances, but the notion of backup focuses on the need for business continuity for the subscriber and the subscriber's activities, on behalf of an employer or with another sponsor, using the subscriber's certificate, and recovery of a backup copy is often with the consent or at the request of the subscriber. The considerations involved with backup are discussed more fully in section PAG § 6.2.4. By contrast, escrow often connotes a potential need for recovery of the subscriber's private key without the subscriber's consent, for example when an employer needs to recover encrypted data of its employee upon termination of the employee or subscriber. The party holding the private key in an escrow situation is outside the control of the subscriber and therefore has the independence to act to recover the subscriber's private key.

Aside from the employer-employee context, the use of key escrow as a requirement imposed on PKIs to facilitate law enforcement's access to subscribers' private keys has been the subject of considerable debate. Various proposals to mandate key escrow have failed in the United States and elsewhere. Currently, key escrow by a third party key escrow agent is not mandatory in the United States or Europe.

Any PKI considering implementing a voluntary key escrow should try to answer two questions. First, is there a business need for key escrow? Second, which system best meets the PKI's business need and how should the system be implemented to ensure its trustworthiness? Assessors should determine whether a PKI does, in fact, have a business need for key escrow and, if so, the degree of protection needed by the system to implement it. Assessors should refer to any externally imposed requirements for key escrow, and they should determine whether the PKI's documentation adequately responds to these requirements and discloses the requirements or practices with respect to key escrow. Finally, assessors should determine whether, in fact, requirements for escrowing keys and protecting escrowing systems have been implemented properly by the PKI's participants.

Appropriate Requirements and Practices. An organization's voluntary escrowing of the private keys of its end-users is normally limited to circumstances where a business need to recover private keys outweighs the inevitable, but perhaps necessary, extra risk of storing a copy of a subscriber's private key outside of the subscriber's system. An organization may see a business case for key escrow where, for business continuity purposes or where the interests of the organization and the subscriber may diverge in the future.

Once a decision has been made to escrow private keys, then the next question is which private keys should be escrowed. Most often, key escrow systems are established in order to recover private keys used by end-user subscribers for the decryption of encrypted messages that they receive. Ideally, signature keys should not be

subject to key escrow. Nonetheless, limitations within end-user software may mean that a key escrow system is unable to support separate keys for signatures and encryption. In such cases, a single key is certified for both digital signature and encryption purposes, and key would be escrowed.

Relying parties should be informed when an encryption certificate is subject to key recovery. An organization implementing key escrow should also ensure that the escrowing system operates in a trustworthy fashion. For instance, it may want to ensure that:

- the service implements the access scheme faithfully.
- the service protects the confidentiality of the information carried (e.g., keys, access requests, etc.).
- the mechanisms used by the service maintain and validate the integrity of access requests, responses and stored key data.
- the service authenticates the source of the key data and protects the data from disclosure to unauthorized parties.
- the service ensures against nonrepudiation of responses it generates; the service should unambiguously tie the request for access to the returned escrowed data.
- the service provider provides timely access request responses; the response time should meet the needs of the requestor.
- the service ensures that security functions are always invoked and can not be tampered with
- the service provides a reasonable audit / logging capability see PAG § D.5.5 (Audit Logging Procedures).

In sum, a PKI's possible requirement for key escrow and the security of key escrow systems should match the business case for key escrow and the business needs for security. The PKI should implement any externally-imposed requirements for key escrow and abide by any externally-imposed prohibitions or limitations upon key escrow. The PKI's documentation should set forth clear requirements or disclosures matching the PKI's business needs. And the participants within the PKI should, in fact, implement the requirements or practices set forth in the PKI's documentation.

D.6.2.4 Private key backup

Issue Summary. This section has a similar focus to PAG § 6.2.4 on the creation of copies of private keys, but focuses somewhat more on business continuity issues for the subscriber and includes the backup of CA private keys. More specifically, PAG § 6.2.4 concerns the extent to which a PKI requires, permits, or forbids the backing up of private keys. As with Section PAG § 6.2.3, this section distinguishes between private keys used to generate digital signatures and private keys used in connection with the decryption of encrypted messages. Finally, if keys are backed up, the section addresses any controls governing the backup process and the backed-up keys.

Relevant Considerations. Private key backup meets the business continuity needs of PKI participants and is intended to protect against loss of keys. Also, in some cases, backup allows the same key to be used in multiple cryptographic modules for performance reasons. Key backup is distinct from key escrow in that key backup normally connotes a situation where the certificate holder, whether a CA, RA, end-user subscriber, or other entity, determines whether to obtain and use the backup copy of the private key. This does not mean that the certificate holder necessarily retains physical possession of the keys; for example, an encrypted copy of a

private key may be stored in the physical custody of another party, provided that the certificate holder retains sole control of the key needed to decrypt the private key.

Considerations related to the backup of private keys include:

- which entities must backup their private keys,
- how securely backup copies of private keys must be stored (e.g., in encrypted form),
- the security of the backup storage location (e.g., off site),
- the identity of who can access or use backup keys, and
- whether multi-party control is required to restore the backed-up key material.

Assessors should assess the need for private key backup by various PKI participants and the need for security relating to the backup process and the storage of backup private keys. They should consult the PKI's documentation to determine whether it matches the security needs of the PKI. Assessors should also determine whether the documentation meets any externally-imposed requirements, such as those imposed by law or contract. Finally, they should ascertain whether PKI participants do, in fact, make backups of their private keys to the extent they are required to do so by the PKI's documentation.

Appropriate Requirements and Practices. The motivation for private key backup by various participants within a PKI is to ensure business continuity. Where the risks and harm associated with the unavailability of a private key are high, it is generally appropriate to require a PKI participant to back up its private key. For instance, PKIs generally require CAs to back up their private key to maintain the uptime of its services and recover from possible disasters. By contrast, the business need to require end-user subscribers to back up their private keys is much lower. It is much easier for an end-user subscriber to generate a replacement key pair and obtain and make available a new certificate than it is for CAs. Therefore, PKIs may not find it necessary to require that end-user subscribers back up their private keys. The following subsections discuss the backup of different kinds of keys in more detail.

CA keys: Backing up a CA private key may be vital to ensure continuity of CA operations. If a CA private key is corrupted a new CA key pair will have to be generated and a new certificate will need to be issued by the CA's certificate issuer. As this amount of work will persuade many CA operators to backup their CA private key, the key backup should be performed to minimize the risk of key compromise. One means of backing up a CA private key is to use technology to split the private key into n of m splits (that is any n of a total of m components will suffice to reconstruct the key) and provide the shares of the private keys to the holders of the shares. Splitting the key material into distinct pieces is important because doing so prevents any single individual from being able to recover the CA private key. CA private keys should be cryptographically split before they are exported from the cryptographic module where they are generated, and the key components delivered directly into the custody of the custodians.

Alternatively, cryptographic modules may be designed to permit direct module to module backup, with the private key encrypted during the transfer. Activation of backup module would then require split control. ISO standard 15782 [ISO 15782], as an example, details specific procedures for key backup using cryptographic modules.

End entity keys: The nature of end-entity private key backup depends upon the business reasons for the backup copy. End entity private keys should be encrypted with strong encryption (the cryptography protecting the key should be at least as strong as the key itself) before they are exported from cryptographic modules. Unencrypted private keys should generally never exist outside a cryptographic module. Backup of private keys corresponding to high assurance certificates may require storage in hardware cryptographic modules.

CAs may elect to impose private key backup restrictions on end entities, or completely forbid end-entity private key backup, as a condition of certificate issuance. The requirements may be different for signature and encryption keys, since there are generally compelling reasons (possible loss of encrypted data) to back up encryption keys. If a corporate key custodian holds an individual user's signature private keys, the keys should generally be encrypted under a key known only to the keyholder. The reason for this requirement is to prevent another party from being able to obtain the backup copy of the private key and forging digital signatures appearing to originate from the subscriber. Moreover, the need for end-entity signature key backup is not as strong as for CA signature key backup. A loss of a signature key does not itself invalidate already signed signatures and the issuance of a new certificate for a new key will restore digital signature functionality to the end-entity. By contrast, encryption private keys may be backup to allow for access after a key corruption to previously encrypted data.

Additionally, a backup copy of a key is another potential point of attack. If software cryptographic modules are used, however, it is nearly impossible to prevent end-entities from backing up their private keys, and routine system backup procedures may create unintended backup copies of private keys.

Some other entities (e.g., web servers) may use encryption keys in only an ephemeral manner and there may be minimal inconvenience if the key is lost.

More generally, whether a PKI requires or forbids the backup of private keys will depend upon business need and the applications secured by the PKI. The procedural safeguards protecting the backup process, if any, should match the security needs of the PKI. Moreover, the PKI's documentation should reflect procedures appropriate for these needs, with due recognition of any externally-imposed requirements. Further, PKI participants should, in fact, backup their keys (or refrain from backing up their keys) in accordance with the PKI's requirements and practices.

D.6.2.5 Private key archival

Issue Summary. As with the previous two sections, this section relates to the creation of copies of private keys. This section, however, focuses on long-term storage of private keys. This section concerns the extent to which a PKI requires, permits, or forbids the archiving of private keys. Again, this section distinguishes between private keys used to generate digital signatures and private keys used in connection with the decryption of encrypted messages. Finally, if private keys are archived, the section addresses any controls governing the archival process and the archived keys.

Relevant Considerations. Private key archival, like backup, involves the storage of a copy of a PKI participant's private key. Nonetheless, the two concepts serve different purposes. Backup meets a short-term need of business continuity to prevent the loss of functionality due to an accidental loss, corruption, or deletion of the private key. By contrast, archival is for the purpose of long-term storage. If decryption keys are archived, the archival permits the archiving party to refer to encrypted historical records that may need to be accessed in the future, perhaps long after the useful operational life of the keys has ended.[393] The archiving of signature private keys, however, may introduce a security risk of signature forgery, even if the usage period of the key has long passed, and is highly discouraged.

Assessors should determine whether a PKI has a business need to require private key archival of various PKI participants. They should also consider whether the risks involved with the archival of signature private keys calls for prohibiting such archiving. Assessors should take into account any requirements imposed externally, whether in law or by contract. They should also determine whether the PKI has adequately documented the requirements and practices relating to the archival of private keys. Finally, they should determine whether PKI participants are in fact adhering to the requirements and practices stated in the PKI's documentation.

[393] *See* Ford, *supra* note 31 at 245.

Appropriate Requirements and Practices. The application for which certificates are used will govern whether private key archival is necessary. In general, the business case for archiving decryption private keys is greater than the case for archiving signature private keys, and the risks are lower. Archiving decryption private keys, for instance, may assist an organization in accessing encrypted historical records in the future, and in certain industries, documentation in electronic form. In the absence of long encrypted record retention requirements, however, it may not be worth it for a PKI to require the archiving of decryption private keys, but rather, to store the records in unencrypted form in a physically secure and integrity protected location.

A major risk in archiving keys is if someone were to obtain a copy of a signature private key, even after expiration, it would be possible to forge a digital signature that would validate properly. Assuming that archiving private keys is appropriate, a PKI should generally require reasonable measures to protect the archived copies to prevent the compromise of these private keys, such as storing the keys in encrypted form. Moreover, these systems may incorporate certain system controls to prevent the unauthorized recovery of the archived private keys.

Ultimately, the need for archiving private keys and the security requirements applicable to any archival system should correspond to the business and security needs of the PKI. Moreover, the PKI should clearly state its archival requirements and practices in its documentation. Finally, whatever archival practices or requirements are mentioned in the PKI documentation, the PKI's participants should abide by such practices or requirements.

D.6.2.6 Private key entry into cryptographic module

Issue Summary. This section covers the means taken to protect the private keys as they are entered into the cryptographic modules and the form in which the private keys are stored in the cryptographic modules.

Relevant Considerations. The entry of private keys into a cryptographic module could take place in at least three situations. First, it may be desirable to generate a key pair outside of the cryptographic module that will use it.. For example, a CA may generate end-user subscriber key pairs on a single secured machine and enter the key pairs into smart cards or other hardware tokens that the CA plans to distribute to end-user subscribers. Second, in the process of creating backup copies of private keys stored in a cryptographic module, it may be desirable to enter the copied private key into another cryptographic module. A CA, for instance, may protect its private keys in a hardware cryptographic module and, for business continuity purposes, keep a backup copy of the private key on another cryptographic module. After creating the backup copy of the private key, it will be necessary to enter the backup copy into the second cryptographic module. Third, it may be necessary to move a private key from one cryptographic module used in daily operations to another. This situation may arise where there is a defect or need to decommission the first cryptographic module.

Entry of private keys into the cryptographic module is a critical process. Security could be compromised if disclosure, modification, or substitution of the keys occurs. Therefore, the systems used to enter a private key into a cryptographic module must contain integrity functionality during the key entry process. Alternatively, the private key may be split prior to being entered into a series of cryptographic modules, such that only a portion of the private key is entered into a given cryptographic module in any one instance.

Once a private key is placed in a cryptographic module, either because it was entered into the cryptographic module from an external source or was generated in the cryptographic module itself, the firmware within the cryptographic module must have functionality to protect the private key. For instance, the cryptographic module may hold private keys in an encrypted form or may be one of several cryptographic modules holding portions of a split private key.

Appropriate Requirements and Practices. The threshold consideration with respect to entry of private keys into cryptographic modules is whether there is any need at all to perform such an operation. The process of moving a private key from one location to another creates a risk of compromise. Therefore, if the process can be avoided, the risks will not arise. A business need to perform the operation would exist in the case of a

centralized generation of keys for tokens distributed by a CA, where it is necessary to back up private keys, or where there is a need to transfer the private key to a new location or vendor. The PKI's documentation should clearly delineate circumstances in which the process of entering private keys into cryptographic modules is needed or required, taking into account any externally-imposed requirements.

Assuming that the entry of private keys into cryptographic modules is necessary, it is best if the private key is never exposed in clear text. This helps prevent unauthorized access to and use of private keys. The key should at least be encrypted using a key held only in the cryptographic module. In n of m schemes, the private key may be split and portions may need to be entered by different people. The same controls can be used to protect private keys once they are entered into a cryptographic module.

The RFC 2527 framework does not contain a separate section governing the form in which private keys reside in cryptographic modules where they are generated within the cryptographic module used for normal operations rather than entered into the cryptographic module from a separate source. Therefore the section, within a CP or CPS corresponding to this section within the PAG, may be the best place to discuss the form in which private keys are stored in cryptographic modules, regardless of whether the private key was entered into the cryptographic module from an external source or whether the private key was generated within the cryptographic module itself.

Whatever the extent to which private keys are entered into cryptographic modules and are secured during and after the entering process, the controls implemented should be appropriate in light of the security needs of the PKI and the assurance levels provided by the certificates. The PKI's documentation should clearly state the requirements, practices, and limitations surrounding the process, and the PKI's participants should adhere to these requirements, practices, and limitations. Any externally-imposed requirements should be reflected in the PKI's documentation.

D.6.2.7 Method of activating private key

Issue Summary. This section relates to the method by which a PKI's participants activate their private keys prior to a private key operation or a session during which private key operations are performed. Once activated, a private key remains usable until it is disabled. The activation (and disablement) process and techniques may be different among end-user subscribers, CAs, RAs, and others, depending on the value of the data that the key will protect and whether the activation is for a personal or organizational private key holder. Finally, a major issue is whether a private key, after activation, remains activated for only one private key operation, one session, or indefinitely .

Relevant Considerations. Various methods of activating private keys exist. For example, some systems may automatically activate private keys when needed, for example, at the time of user login or when a device is turned on. In other systems, automatic activation may occur after a token is inserted in a reader. Other systems may require the user to supply a PIN or password in order to activate the private key. A combination of methods may also be used, such as requiring the placement of a token in a reader and supplying a PIN.

Biometric methods of activating keys (that is, methods based on the physical characteristics of an individual) may offer additional protection, and may be warranted depending on risk and technology cost. Examples of biometrics include fingerprints, retinal scans, voice recognition, and handwriting analysis. Considerations with the use of biometric systems include:

- low error (false negatives and false positives),
- difficulty/impossibility of spoofing,
- cost to implement and operate,

- ease of use, and
- difficulty of securing the stored characteristics database.

The technology underlying biometric systems is still maturing and can be expensive, but the costs are decreasing. The advantage of biometrics is that the characteristics can not be spoofed if the technology for verifying the characteristics is effective. The use of biometrics, as a secondary authentication technique, offers an advantage over memorized activation data in that a biometric can not be forgotten, shared with others, or stolen.[394]

Secondary authentication techniques used in conjunction with biometrics are often considered appropriate to be used for private key activation. Secondary authentication involves activating a private key with what you know (e.g., passwords, knowledge tests) or what you have (e.g., smart cards, USB dongles) or what you are (e.g., biometric). It is this last category that is *believed* to provide the greatest authentication. It is more difficult to repudiate something when, at the time of the transaction, biometric indicia were used as a secondary authentication technique.

Biometrics involves the collection and use of indicia concerning specific personal characteristics. Pattern matching and pattern recognition algorithms are used to compare "presented" biological information with biological information on file, being collected and digitized at some point in the past. Currently available techniques used to collect biometric indicia include fingerprints, retinal scans, voice recognition, facial scans, and handwriting analysis. While the use of biometric techniques is anticipated to increase in the future, it must be recognized that there remain a number of issues to be considered with their use, most notably the security of the captured biometric data as it is rather hard to "revoke" a fingerprint or retina.[395]

Once activated, a private key may remain activated for simply one private key operation, after which it is automatically deactivated and must be reactivated in order to perform subsequent private key operations. Some client applications, for instance, may enforce activation requirements of this kind in order to prevent unauthorized use of the private key between private key operations that the user undertakes. A private key may also be activated and remain activated indefinitely until deactivated. For instance, an online CA may be activated within a secure facility and may need to remain active and available to perform certificate-signing operations on an as-needed basis. The reason for this extended activation is that online CAs may need to sign and issue certificate on a 24x7 basis. In between these two polar opposites are the systems that activate a private key for a particular session, initiated for instance when a token is inserted into a reader. Private key operations may occur during the session, but when the token is removed from the reader, no further private key operations can occur unless the user reinserts the token and reactivates the private key.

[394] For instance, part of the engineering of fingerprint readers ensures that the fingerprint is not coming from an amputated finger or latex facsimile.

[395] First, any application employing biometric techniques being considered must be evaluated in terms of the percentage of "false negative" and false positive" reports it generates. The difficulty in obtaining precision in the comparison of data (which causes false reports) has declined in recent years and has been reduced to the point of irrelevancy in some applications but it is a factor to be considered. Similarly, another issue to be considered is how well the biometric indicia has been bound to the electronic document and what technology has been used to do so. Biometric techniques, in and of itself, do not provide document integrity. The most important points to consider involve security and authentication. From a security perspective, once biometric indicia or information has been digitized and stored in a computer system, it is now vulnerable, in the same manner as other digital data, to attack and must be protected. Biometric indicia, successfully subject to a "capture and replay" attack, can be used to spoof an identity of the "originator" of that information. The authentication issue is simply that biometric indicia cannot necessarily be used for authentication. One can determine that Person X presented their fingerprint or voiceprint but it does not establish the identity of Person X. There is no trusted entity which authoritatively links the biometric indicia to an identity.

In the absence of an infrastructure to link biometric indicia to identities, it is therefore probable that such indicia will be used as a secondary authentication aide to digital certificates (currently public key but possibly attribute certificates in the future).

The procedures mentioned above for the activation of a private key may be performed by the subscriber himself or herself, in the context of the use of a private key held by an individual and used in a client system. Where the subscriber is an organization or an organization is operating a CA, RA, or other entity, however, the organization can only activate a private key through the conduct of individuals acting on behalf of the organization. In that event, administrators, who may be required to have trusted status, may perform the activation functions.

Assessors should assess private key activation methods and personnel requirements in light of the business needs of the PKI and the assurances provided by the certificates. They should also determine whether any external requirements apply to the PKI, which may originate from contracts or applicable law. Assessors should also check the PKI's documentation to determine if the security surrounding the activation procedures matches the PKI's business needs. Finally, they should check whether PKI participants do, in fact, adhere to the requirements and practices in the PKI's documentation.

Appropriate Requirements and Practices. The need for security with respect to the process by which a private key is activated and the extent to which private keys remain activated will depend on a number of factors, such as:

- the role of the participant holding the private key. CAs and RAs will generally want to have greater controls over the activation process than are necessary for end-user subscribers, even within the context of a single PKI,

- the applications for, and the assurance level provided by, the certificates within the PKI. PKIs issuing certificates offering higher level of assurances will want to require or use more robust controls over the activation process than PKIs issuing certificates offering lower levels of assurance. For instance, certificates providing the lowest level of assurance or no assurances at all may not require any particular security around the activation process, and end-users may not even be required to use passwords. By contrast, certificates used to secure high-value transactions or provide strong nonrepudiation support may require the activation process to be secured through multi-factored controls using a combination of two or more of the following factors: 1. what the user knows (such as a password), 2. what the user has (such as a token), and 3. what the user is (such as a biometric system). Controls will range in between these two poles for certificates offering assurances in between these two levels,

- the systems used by the private key holders. Certain applications may be able to interoperate with systems for enhanced protection over private key activation and others may not, and

- the business model of the PKI. It is often easier to enforce requirements for greater protection over private key activation in intra-enterprise PKIs than in PKIs that provide certificates to a large and public community of users.

An organization operating a PKI should consider these factors when setting requirements or establishing practices governing the activation of private keys.

Private key activation should not be possible by unauthorized users. Therefore, a PKI should establish controls relating to who can activate a private key. Generally, an individual should activate his or her own private key, unless the PKI permits agents or fiduciaries to act on behalf an individual subscriber who is a principal or beneficiary. With respect to organizational end-user subscribers and organizational PKI participants (such as CAs and RAs), the PKI will normally want to impose requirements or procedures by which only authorized users can activate a private key on behalf of the organization. In the case of CAs and RAs providing certificates of any but the most rudimentary level of assurances, the PKI may want to require or utilize trusted personnel to perform the activation procedures.

In short, the controls relating to the activation of private keys, the extent to which they remain activated, and the personnel who are authorized to activate them should be appropriate in light of the business and security needs of the PKI. These needs may, in part, depend on any externally-imposed requirements. The PKI should, in its documentation, establish the requirements, practices, and limitations for private key activation that are appropriate to its needs. And the participants within the PKI should, in fact, activate their private keys in accordance with these requirements, practices, and limitations.

D.6.2.8 Method of deactivating private key

Issue Summary. This section relates to the method by which a PKI's participants deactivate their private keys following a private key operation or a session during which private key operations are performed. This section also covers the matter of who can deactivate a private key on behalf of an organizational private key holder.

Relevant Considerations. Just as there are various ways to activate a private key, there are various means of triggering the deactivation of private keys. For instance, the private key may be deactivated automatically once a private key operation is completed. It is also possible to configure a system to deactivate a private key automatically after a certain time has passed following activation during which the private key has been inactive. Moreover, a system may deactivate a private key after a user takes specific steps to end a session, such as removing a token from its reader, logging off the system, or turning off the power. Although very secure, automatic deactivation implemented improperly may irritate users who must repeatedly re-activate the same private key.

The method by which the deactivation process is secured is also an important consideration. Some systems, for instance, ensure that there is no residual information remaining after the deactivation of the private key, to prevent attempts at recovering the private key without authorization. For instance, some systems overwrite the memory in which the private key was stored prior to the allocation of a new process.

The procedures mentioned above for the deactivation of a private key may be performed by the subscriber himself or herself, in the context of the use of a private key held by an individual and used in a client system. Where the subscriber is an organization or an organization is operating a CA, RA, or other entity, however, the organization can only deactivate a private key through the conduct of individuals acting on behalf of the organization. In that event, administrators, who may be required to have trusted status, may perform the deactivation functions.

Assessors should gauge the need for security surrounding the deactivation of a private key with a view to the business and security needs of the PKI. They should also consult the PKI's documentation to determine whether it sets requirements or discloses practices for private key deactivation that are appropriate in light of these needs. Assessors should also check whether any requirements are set by organizations outside the PKI, for example through contracts or applicable law. Finally, they should determine whether the PKI's participants are, in fact, deactivating their private keys in accordance with the PKI's documentation.

Appropriate Requirements and Practices. In settings that involve the use of higher-assurance certificates, when the private key is not in use, it should be deactivated to prevent its use by unauthorized persons. In the final analysis, however the need for controls surrounding the deactivation of private keys will depend on the factors listed in the Appropriate Requirements and Practices section of PAG § 6.2.7. An organization operating a PKI should consider these factors when setting requirements or establishing practices governing the deactivation of private keys.

PKIs offering certificates providing higher levels of assurance will generally want to require and implement controls requiring that the manual deactivation of private keys be performed only by authorized personnel in order to prevent the unauthorized recovery and/or use of these private keys. Generally, where deactivation is not automatic, an individual should deactivate his or her own private key, unless the PKI permits agents or fiduciaries to act on behalf an individual subscriber who is a principal or beneficiary. With respect to

organizational end-user subscribers and organizational PKI participants (such as CAs and RAs), the PKI will normally want to impose requirements or procedures by which only authorized users can deactivate a private key on behalf of the organization. In the case of CAs and RAs providing certificates of any but the most rudimentary level of assurances, the PKI may want to require or utilize trusted personnel to perform the deactivation procedures.

Ultimately, the controls relating to the deactivation of private keys and the personnel who are authorized to deactivate them should be appropriate in light of the business and security needs of the PKI. These needs may, in part, depend on any externally-imposed requirements. The PKI should, in its documentation, establish the requirements, practices, and limitations for private key deactivation appropriate to its needs. And the participants within the PKI should, in fact, deactivate their private keys in accordance with these requirements, practices, and limitations.

D.6.2.9 Method of destroying private key

Issue Summary. The destruction of private keys, if needed, by PKI participants is covered by this section. The destruction process and mechanism may be different for end-user subscribers, CAs, and an organizational private key holder.

Relevant Considerations. If a private key is not destroyed (i.e., rendered unusable) once it is no longer needed, unauthorized use could occur. Various means exist to perform the process of private key destruction (or at least incapacitation), such as overwriting the media or memory in which the key is stored, destroying the token in which the key resides, or at least confiscating from the user the token or system in which the private key is stored. Certain methods of overwriting the data in media or memory are more secure than others.

As with private key deactivation, the procedures for the destruction of a private key may be performed by the subscriber himself, in the context of the use of a private key held by an individual and used in a client system. Where the subscriber is an organization or an organization is operating a CA, RA, or other entity, however, the organization can only destroy a private key through the conduct of individuals acting on behalf of the organization. In that event, administrators, who may be required to have trusted status, may perform the destruction functions.

Assessors should determine how secure the process of private key destruction must be in the context of the business and security needs of the PKI. In addition, assessors should check the PKI's documentation to ascertain whether the private key destruction requirements and practices are sufficiently robust in relation to these needs. They should consult external sources to determine if any outside requirements for private key destruction apply to the PKI, such as those appearing in applicable contracts or law. Finally, assessors should check whether participants within the PKI are performing private key destruction as required or disclosed in the PKI's documentation.

Appropriate Requirements and Practices. In the context of certificates providing higher assurances, it is generally advisable to make provisions for the destruction of private keys when they are no longer valid , except to the extent they are archived. The destruction must be done by a secure and consistent means. The need for destruction and the security surrounding the destruction process will, however, depend on the factors listed in the Appropriate Requirements and Practices section of PAG D.6.2.7. An organization operating a PKI should consider these factors when setting requirements or establishing practices governing the destruction of private keys.

PKIs offering certificates providing higher levels of assurance will generally want to require and implement controls requiring that the destruction of private keys be performed only by authorized personnel in order to prevent the unauthorized recovery and/or use of these private keys. Generally, an individual should destroy his or her own private key, unless the PKI permits agents or fiduciaries to act on behalf an individual subscriber who is a principal or beneficiary. Higher assurance PKIs may require notice to the CA upon destruction of a

still valid private key. With respect to organizational end-user subscribers and organizational PKI participants (such as CAs and RAs), the PKI will normally want to impose requirements or procedures by which only authorized users can destroy a private key on behalf of the organization and to document and/or witness the action. In the case of CAs and RAs providing certificates of any but the most rudimentary level of assurances, the PKI may want to require or utilize trusted personnel to perform the destruction procedures.

In sum, the business and security needs of the PKI will determine the appropriate extent of the controls relating to the destruction of private keys and the personnel who are authorized to destroy them. These controls should account for any requirements imposed from outside the PKI. The PKI's documentation should set forth requirements, practices, and limitations for private key destruction appropriate to its needs. Finally, the participants within a PKI should adhere to the requirements, practices, and limitations within the PKI's documentation relating to private key destruction.

D.6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

D.6.3.1 Public key archival

Issue Summary. This section concerns whether the public keys of CAs, RAs, end-user subscribers, or other PKI participants must be or are archived. If archiving occurs, this section also covers who does the archiving and the controls in place to secure the archive of public keys.

Relevant Considerations. PAG § D.5.6 (Corporate Records Management) covers records management of PKI participants, especially CAs. One component of a PKI's record keeping practices may include the archiving of public keys of various PKI participants, including CAs, RAs, end-user subscribers, and others. Archiving public keys facilitates the ability to verify a digital signature on a record after the certificate has been removed from the directory. In some businesses, it may be necessary to verify a signature long after the signature has been created. Therefore, archiving the public key may be a critical component of a CA's nonrepudiation services.

Assessors should determine whether the applications for which certificates are used require archiving public keys. If so, they should determine whether the need for security and availability calls for the off-site storage of the keys or whether internal archiving is sufficient. In addition, they should determine the degree of security needed to prevent unauthorized addition, deletion, or modification of entries in the archive. Assessors should determine whether any external requirements, whether from contract, law, or otherwise, apply to the process of public key archival. They should check the PKI's documentation to determine if the requirements and practices match the PKI's business needs and any external requirements. Finally, they should determine whether the archival process is actually taking place in accordance with the PKI's documentation.

Appropriate Requirements and Practices. Archival is needed so that digitally signed documents can be validated after the certificate has expired or been removed from the directory. Generally, public keys are archived by archiving the certificates in which they appear. The need for archiving certificates and the public keys they contain will depend on whether the applications for which the certificates are used require verifying digital signatures with them long into the future. If not, certificates in the directory can suffice for providing public keys in the short run. Typically, a certificate will remain in the directory until it has expired or has been revoked. After that, the archive will be the definitive source for certificates and the public keys they contain.

The business needs of the PKI will also determine the identity of the party creating and holding the archive of public keys. If high availability and business continuity are important priorities due to the relatively high assurances provided by the certificates, it may be important to have at least a copy of the archive stored off-site.

Appropriate security measures should be taken to ensure that information in the archive is not lost and that the integrity of the information is maintained for the promised life of the archival record. Procedures such as limiting the personnel who are authorized to add, delete, or modify archived records to trusted personnel may be

appropriate. Moreover, it may be appropriate to have physical, network, and computer security controls in place to prevent the unauthorized addition, deletion, or modification of records in the archive.

Some PKIs may wish to state requirements and practices for archiving public keys in the sections of their CPs or CPSs corresponding to this section. Others may refer to the sections of their documents that cover records retention generally and add certificates to the list of items maintained in their records generally.

In any case, whether a PKI archives public keys, which keys are archived, how long they are archived, who archives them and maintains the archive, and the security controls surrounding the archive needs to be appropriate in light of the business need of the PKI to verify digital signatures over the long run and the level of assurances provided by the certificates. Appropriate requirements and practices should appear in the PKI's documentation. PKI participants should, in fact, maintain an archive of public keys in accordance with the PKI's documentation.

D.6.3.2 Usage periods for the public and private keys

Issue Summary. This section concerns the usage period in which various PKI participants use or are permitted to use their private and public keys. Such usage periods may or may not correspond to the operational period of the certificate containing the public key.

Relevant Considerations. Key pairs often have limited usage periods. Limiting the usage period serves to reduce the possibility that an attacker, through cryptanalysis, can discover the identity of a private key by a mathematical analysis of the ciphertext created by the private key. The longer a user makes use of a private key for digital signature operations, the more ciphertext there will be that an attacker can use to mount a cryptanalytic attack. A limitation on the usage period of a key pair limits the amount of ciphertext a user can create and thereby limit the ability of an attacker to mount such an attack.

Another reason for limiting the usage of a key pair and the certificate corresponding to it is that it limits the damage that may be caused by a compromise of the private key where the subscriber either fails to notify the CA or RA to revoke the certificate or is unaware of the compromise (for example, in the case of a successful cryptanalytic attack). For instance, if a key pair and corresponding certificate may only be used for one year and an undetected or unreported compromise occurs in the first week of use, then the limitation on usage prevents the damage from extending beyond the remaining 51 weeks of the usage period.

The usage period for a private key may or may not correspond to the operational period of the certificate corresponding to the key; in some cases, it may be shorter. For instance, it may be necessary to limit the usage period of a CA private key so that the operational period of the CA's certificate extends for a period beyond the usage period of the private key by an amount of time corresponding to the operational period of the certificates it issues. The CA's certificate is needed to validate the certificate chain that includes the end-user subscriber's certificate. If the CA's key and certificate expired on the same day, then the following day, the signature on certificates signed on the previous day could not be verified. By contrast, if the usage period of the CA key ends before the operational period of the CA certificate ends, then there can be a period of time in which the CA is no longer signing new certificates, but its certificate is still operational and can be used to verify the signatures on the certificates it issued before the end of its private key usage period.

In setting a proper usage period, a PKI should consider the following factors:

- length of keys (longer keys are generally more resistant to cryptanalysis than shorter keys and can therefore have a longer life),
- cryptographic algorithm (some are stronger than others), and
- uses to which keys will be put (higher value or criticality implies shorter lifetimes).

Assessors should determine whether the PKI has set an appropriate usage period for the certificates in light of the factors above. They should also take into account whether there are any applicable external requirements, whether by contract or applicable law. In addition, they should consult the PKI's documentation to determine whether the PKI has expressed its requirements and practices. Finally, assessors should determine whether PKI participants are using their key pairs within the limitations provided in the PKI's documentation and whether a CA issues certificates containing operational periods that are appropriate in light of the key usage periods.

Appropriate Requirements and Practices. A CA will need to set usage period for its own keys, and the PKI should specify the usage periods for keys used by other PKI participants. The PKI will likely want to set usage periods based on the factors set forth above. The operational period of the certificate corresponding to the key pair will then be a function of the usage period of the key pair. With end-user subscriber certificates, the two periods may be the same, but in the case of CA certificates, the usage period of the private key may be shorter than the operational period of the CA certificate. The certificate will specify a beginning and ending date for the key pair.

The usage period for key pairs and the operational period of the corresponding certificates should match the business needs of the PKI in light of the applications for the certificates and their assurance level, taking into account any externally-imposed factors. The PKI's documentation should clarify usage periods for key pairs and, where different, the operational periods of certificates. Finally, the CA should issue certificates that are operational for the periods of time specified in the PKI's documentation, and the PKI's participants should use their keys within the limitations set by the documentation.

D.6.4 ACTIVATION DATA

D.6.4.1 Activation data generation and installation

Issue Summary. This section concerns the types of activation data used in connection with the activation of the private keys of the various PKI participants, as well as the methods in which such activation data are generated and installed on the system of PKI participants.

Relevant Considerations. Activation data are data (other than keys themselves) that are used and needed to activate a private key, such as a PIN, password, or portion of a key or other data used to enforce multi-person control over a private key. A system can be configured to require the input of such information as a condition of activating the private key. The type of authentication data required or used within a particular PKI may be addressed in the portions of a CP or CPS corresponding to PAG § D.6.2.7 (Method of Activating a Private Key). Schemes for splitting private keys and/or their authentication data may also be covered by documentation corresponding to PAG § D.6.2.2 (Private Key Split Knowledge Control).

This section, however, addresses the additional topics of how activation data must or are generated and installed. For example, where a PKI uses passwords as activation data, this section may address requirements or practices used to generate secure passwords.

Assessors should determine the type of activation data needed in light of the applications for the PKI's certificates and the assurance level they provide. Assessors should also account for any external requirements imposed, for instance, under law or by contract. This analysis should be coordinated with the analysis of the need for activation data under PAG §§ D.6.2.2 (Private Key Split Knowledge Control) and D.6.2.7 (Method of Activating a Private Key). Assessors should also determine whether requirements and practices for the use, generation, and installation of activation data appear within the PKI's documentation. Finally, they should check whether PKI participants are using, generating, and installing activation data in accordance with the requirements and practices in the documentation.

Appropriate Requirements and Practices. A PKI will likely want to require that activation data (where used) be generated in a secure manner and installed in the system in a manner that minimizes or prevents exposure. Frequently, activation data is used in conjunction with a two factor authentication (i.e., in addition to some physical token) so that losing the token alone or compromise of the PIN alone does not compromise security.

In the case of higher-assurance certificates, it is preferable that activation data never be visible to anyone but the individual who will be responsible for activating the system. Moreover, if activation requires m of n individuals (split knowledge), the portions of the activation data should never reside in fewer than m hands. Successful guessing of the activation data should be infeasible. It should not be possible to make and confirm guesses outside the system, and the system should protect against too many incorrect guesses. Ultimately, which activation data the PKI decides to use, and the means for their secure generation and installation, should be commensurate with the security needs of the applications for the PKI and the assurance levels provided by the certificates. The PKI should account for any external requirements, and its documentation should clarify the requirements or practices for generation and installation. Finally, the generation and installation practices of the PKI's participation should match the requirements and practices set forth in the PKI's documentation.

D.6.4.2 Activation data protection

Issue Summary. Section D.6.4.2 relates to the controls surrounding the use of activation data that protect the activation data from compromise for the various PKI participants that use activation data.

Relevant Considerations. Activation data protection involves controls to ensure that the activation data, after generation and installation, are not compromised. The controls to protect activation data will depend on whether the activation data are PINs or passwords on one hand or, on the other hand, are a means of enforcing multi-person control of a private key through splitting the private key or its activation data.

In the case of PINs and passwords, there are various well-known practices relating to preventing compromise, such as requiring users to memorize them rather than writing them and forbidding users from sharing them with unauthorized personnel. Educating activation data users as to these practices and the importance of protecting activation data also facilitate protection.

In the case of schemes to split private keys or activation data for the purpose of requiring n of m shares to activate the private key, the splitting itself is a method of protecting the activation data. The PKI may have options for enforcing security controls regarding the handling of the shares themselves by the holders of the shares. For example, the PKI might require that shares, when not being used, reside in a physically secure location.

Assessors should determine the need for security controls for the protection of activation data in light of the applications for which the certificates are used, the assurance levels provided by the certificates, and any externally-imposed requirements such as those appearing in applicable contracts or laws. They should also determine whether the PKI's documentation contains requirements or practices that appropriate in light of these needs or requirements. Finally, the assessors should see whether or not PKI participants are using the controls mandated or disclosed in the PKI's documentation.

Appropriate Requirements and Practices. Generally, the need for security controls over the handling of activation data will be commensurate with the sensitivity of the information protected by the certificates' applications and the assurance levels provided by the certificates. The data must be protected in a manner consistent with the value of data that could be disclosed or transactions that could be made if the activation data were to fall into the wrong hands.

Where certificates provide higher assurance levels, activation data should generally be stored only ephemerally and preferably in a form not useable by an intruder. Any residue of the activation should be removed from the system. In the case of passwords or PINs used in this context, the PKI should enforce requirements to prevent

their compromise. To prevent unavailability of the CA and great inconvenience to users with certificates from the CA, steps should be taken to ensure that death, non-cooperation, forgetfulness of a single (or small number of) persons does not prevent operation of the CA. Therefore, in the case of higher assurance levels, and in the case of CA or RA activation data, may call for the use and protection of split activation data for multi-purpose control over the CA or RA private key. The PKI should also in this context enforce the secure handling of the shares and maintain an audit trail to show the proper chain of custody and use of activation data.

Whatever requirements or practices enforced by the PKI should appear in its documentation. Moreover, the conduct of the PKI's participants in protecting activation data should match the requirements and practices appearing in the PKI's documentation.

D.6.4.3 Other aspects of activation data

Issue Summary. This section concerns whether activation data for the private keys of CAs, end-user subscribers, or other PKI participants must be or are archived. If archiving occurs, this section also covers the controls in place to secure the archive of public keys. This section also covers the usage periods for activation data.

Relevant Considerations. It is possible for PKI participants to back up or archive their activation data. A PKI may also be able to enforce requirements and practices under which activation data only have a limited usage period, after which a user needs to change the activation data. For example, a system can be established to require that passwords be changed periodically.

The backing up of activation data may promote the interests of business continuity. The long-term archiving of activation data beyond the usage period of the keys, however, may introduce the risk of unauthorized use of the private key beyond its limited usage period.

Assessors should determine the security and business needs for storing copies of activation data and the security controls to protect the stored copies. They should also determine whether there is a need for limiting the usage period of activation data and requiring that they be changed periodically. Assessors should account for any requirements imposed by law, contract, or other external sources. They should check to determine whether the PKI's documentation reflects these needs and requirements. Finally, they should determine whether PKI participants are adhering to the requirements and practices in the PKI's documentation.

Appropriate Requirements and Practices. For the reasons mentioned above, it is generally not be desirable to archive activation data. Even the backup of activation data is uncommon, since the business continuity purpose of ensuring the availability of CA and RA activation data can often be satisfied simply by enforcing an "n out of m" splitting scheme. Password-changing requirements may be more common, but may not be appropriate where changing the activation data would requiring revoking and rekeying the certificate.

In any case, the creation of extra copies of activation data and enforcing an activation data usage period should only take place where there is a business need and is feasible. Any such requirements or practices should be reflected in the PKI's documentation, taking into account any external requirements. Finally, the PKI participants should adhere to the practices and requirements relating to activation data copying and usage periods that appear in the documentation.

D.6.5 COMPUTER SECURITY CONTROLS

D.6.5.1 Specific computer security technical requirements

Issue Summary. This section covers technical security controls concerning a single platform and applications on it.[396] Often, this section concerns systems involved with CA and RA operations, as opposed to the systems of end-user subscribers.

Relevant Considerations. Computer system security controls are of vital importance to PKI participants, especially service providers, such as CAs, RAs, CMAs, and repository service providers. Compromises to their systems could involve security breaches in systems protecting private keys, approving certificate applications, and other vital certification functions.

Some of the specific mechanisms that PKI participants can use to protect the integrity of their systems include the list of suggestions in RFC 2527: "trusted computing base concept, discretionary access control, labels, mandatory access controls, object reuse, audit, identification and authentication, trusted path, security testing, and penetration testing."[397] Mechanisms to assist in controlling access to computing systems include:

- Requiring the identification and authentication of users to computer systems before allowing them access to computing resources,
- "[U]ser account management, auditing, and timely modification or removal of access,"[398]
- Differentiating access based on the separation of duties and the different functions of trusted personnel,[399]
- Maintaining restrictions and controls on the use of system utility programs,[400]
- Using object re-use controls to prevent unauthorized access to deleted files,[401] and
- The use of monitoring and alarm facilities to detect, register, and react in a timely manner in the event of unauthorized access to computing resources.[402]

In particular, access controls are important on systems used for certificate lifecycle services.[403] Other computing controls relevant here include protections against viruses and malicious code and secure media handling practices.[404]

The difficulty in compiling such a list of computer security controls is that in PKIs offering higher assurance certificates, it is not practical to compile a comprehensive list of controls. Such PKIs may have entire

[396] *See* PAG § D.6.7 (Network Security Controls) addresses the technical security controls concerning networks and networking.

[397] RFC 2527 § 4.6.5.

[398] ETSI TS 101 456 § 7.4.6(c).

[399] *See id.* § 7.4.6(d).

[400] *See id.*

[401] *See id.* § 7.4.6(g).

[402] *See id.* § 7.4.6(i), (l).

[403] *See id.* § 7.4.6(k), (m).

[404] *See id.* § 7.4.5(a), (c), (e).

operational manuals devoted to computer security controls. Listing all such controls in a CP or CPS would not only create excessively lengthy documents, it may also create security vulnerabilities by giving attackers information they could use to exploit weaknesses in the PKI's computer security practices.

Accordingly, assessors will likely see that practice documents treat the "Specific computer security technical requirements " section in one of six ways:

1) The PKI does not attempt to list all computer security controls, but rather creates a general standard of conduct or controls to be implemented and imposes that standard in its documentation. The most common general standards here are a requirement to utilize "trustworthy systems"[405] or a requirement of reasonableness and the use of reasonable computer security controls.

2) The PKI documentation refers to detailed computer security controls in other documents, such as operational manuals.

3) The PKI documentation attempts to record a comprehensive listing of computer security controls.

4) This section within the PKI documentation contains a summary and brief listing of, or series of cross-references to, the applicable computer security controls.

5) This section does not attempt to cover all computer security controls, but does set out some general controls and the remaining controls appear in other documents.

6) A combination of some of the above approaches.

Assessors should determine which approach is implemented within the PKI's documentation and whether the documentation successfully carries out that approach. They should also determine whether the controls identified are appropriate for the level of assurances provided by the certificates and the security needs of the applications for which the certificates are intended. Finally, assessors should determine whether the PKI's participants are, in fact, implementing the security controls required or disclosed in this section.

Appropriate Requirements and Practices. The choice of which of the six approaches above for covering computer security controls will depend on the circumstances of the PKI. Approach (1) is a legitimate one, and has brevity as a virtue. It has a great disadvantage of vagueness, however, and in many instances PKIs do wish to enforce specific controls on their participants. Approach (2) permits a PKI to enforce specific controls, but such enforcement depends on the incorporation of the more specific document by reference. Moreover, splitting the responsibilities among multiple documents makes review of any particular document more difficult. In most circumstances, approach (3) is impractical since listing all the applicable computer security controls would very likely make the PKI's documentation extremely lengthy. Approach (4) may be a nice compromise among the above choices, but assessors may find that the effort to summarize all computer security controls is either futile or misleading, and not worth the effort. Approach (5) is problematic. While it does not attempt an impractical comprehensive listing, it may not be effective in enabling the PKI to enforce more specific requirements in these other documents. Without a reference to other controls appearing in these other documents, readers may mistakenly believe that this list of most important controls is exclusive and that no other controls are binding on PKI participants.

For these reasons, a combination, Approach (6) may be the most effective choice. One common combination includes Approach (5) (a brief list of some critical controls), coupled with approach (2) (a reference to controls appearing in operational documents), may prove to be the most effective choice. PKIs may also find it helpful to include a general trustworthiness requirement as a "backstop" measure, although referring to a set of criteria, such as criteria for an audit or rating will help flesh out the nature of "trustworthiness" and counter any impression that a "trustworthiness" requirement is hopelessly vague.

[405] *See id.* § 7.4.7.

Regardless of the approach to presenting controls, the controls established for a PKI should be consistent with its security needs and the assurance level of the certificates it provides, while accounting for any externally-imposed requirements appearing in applicable law or contract. Moreover, the PKI should ensure that its documentation clearly communicates the controls that it has established. Finally, PKI participants' practices should be consistent with the computer security controls required by the PKI's documentation.

D.6.5.2 Computer security rating

Issue Summary. This section covers independently generated security ratings that products or systems may have, especially products or systems used to perform CA or RA functions.

Relevant Considerations. A PKI may wish to require or seek a rating for particular CA or RA products or systems to assure a base level of assurances relating to their reliability. Such ratings also help to flesh out the concept of "trustworthy systems," the use of which may be required in other sections. The possible kinds of ratings identified in RFC 2527 are ones based on: "the Trusted System Evaluation Criteria (TCSEC), Canadian Trusted Products Evaluation Criteria, European Information Technology Security Evaluation Criteria (ITSEC), or the Common Criteria."[406] A PKI could also require that such products or systems undergo other assessments, such as "product evaluation analysis, testing, profiling, product certification, and/or product accreditation related activity."[407]

Assessors should determine whether, in light of the circumstances of a PKI, it makes sense for a PKI to require or undertake the assessment of the products or systems that it uses. If so, they should determine which assessments meet the PKI's business needs, taking into account any external requirements, and they should ascertain whether such assessment policies appear in the PKI's documentation. Finally, they should determine whether PKI participants are, in fact, using products or systems that have the ratings or that have undergone the assessments required or disclosed in the PKI's documentation.

Appropriate Requirements and Practices. In reality, the use of components with a certain computer rating is driven by external regulatory or licensing requirements of the PKI, as a mechanism to reduce the development or lifecycle costs of PKI components the security needs of the applications of the certificates, and the assurance levels provided by the certificates. Nonetheless, such ratings or assessments are typically performed only in environments requiring higher assurance certificates. The expense and effort involved in obtaining such ratings and assessments is frequently not worthwhile in the context of lower assurance certificates.

Assuming that obtaining some rating or assessment makes sense for a PKI, the next question is which kind of assessment makes sense. Such a decision must rest on the needs of the application for the certificates and any externally-imposed requirements, such as those appearing in contracts or applicable law. The selection of an appropriate computer security rating should be done in conjunction with the auditor of the PKI as the auditor may feel more comfortable, and have expertise in successful evaluations, with a certain criteria. As the security and assurance level of a PKI consists of many parts the use of "certified" or "endorsed" products may or may not have an overall effect on the security of the PKI. PKI operators are encouraged to follow the guidance of their auditors and insurers in this regard. The decision to obtain certain ratings should be reflected in the PKI's documentation. Finally, PKI participants should use products and systems that have the ratings and that have undergone the assessments required by the PKI's documentation.

[406] RFC 2527 § 4.6.5.

[407] *Id.*

D.6.6 LIFE CYCLE TECHNICAL CONTROLS

D.6.6.1 System development controls

Issue Summary. PAG § 6.6.1 relates to the controls surrounding the development of systems used in the PKI, most often the software used to perform CA and RA operations.

Relevant Considerations. System development controls listed in RFC 2527 include development environment security, development personnel security, configuration management security during product maintenance, software engineering practices, software development methodology, modularity, layering, use of fail-safe design and implementation techniques (e.g., defensive programming) and development facility security.[408] If an assessor has knowledge of the software development environment, the assessor can determine the rigor of the development process, the quality assurance steps, the use of development tools that help avoid programming errors. Frequently, however, a system is bought as a commodity and assessors do not have insight into the development process.

It may be helpful to consider the following topics when conducting a comprehensive assessment of the development of particular software.

Life-cycle model:

- does the developer use a standardized life-cycle model (i.e., one that has been approved by some group of experts)
- identify the type of review procedures done on the design
- identify the procedures for making changes to the design
- identify the test methods used

Development security:

- identify the security of the development facility
- identify the security measures used in hiring development personnel

Flaw remediation:

- identify the tracking of reported security flaws
- identify the means for distributing corrections to flaws
- identify the time required to distribute security flaw reports

Software development:

- identify the software engineering practices that are used
- identify if a fail-safe design techniques was used
- identify if the implementation made use of defensive programming techniques

[408] *Id.* § 4.6.6.

Assessors concerned with assisting a PKI to determine from a high-level policy perspective which controls are important for a PKI should take into consideration the circumstances of the PKI and what makes sense in light of the applications for the certificates. They should also review the PKI's documentation to determine whether it adequately expresses requirements or disclosures concerning the controls established for system development. Finally, assessors will want to determine whether PKI participants have chosen systems that have met the requirements or practices disclosed in the PKI's documentation. By contrast, assessors conducting an assessment of a PKI participant that is subject to an external requirement for the use of products developed under certain controls need only determine whether the assessed entity did, in fact, make use of a product that was developed under the required controls.

Appropriate Requirements and Practices. As with ratings or assessments of CA or RA products or systems, the need for requiring certain controls to be in place during the development of CA or RA software will depend on the PKI, the security needs of the applications of the certificates, and the assurance levels provided by the certificates. Typically, such controls are expected only in the context of PKIs providing higher assurance certificates. The cost of such controls would need to have been factored into the price charged by the vendor and the extra cost is likely not worth the extra security in the case of PKIs offering lower assurance certificates.

Therefore, PKIs should establish requirements relating to system development controls or disclose the use of products that have been developed under such controls only if the extra assurances provided by such controls are worthwhile for the PKI in light of its security needs. PKIs, however, will need to obtain software that meets any externally-imposed requirements relating to system development controls. The PKI's system development control requirements or standards should appear in its documentation, and PKI participants should obtain products that meet the requirements or standards in the documentation.

D.6.6.2 Security management controls

Issue Summary. This section concerns controls used to ensure that systems, especially CA and RA systems, are operating correctly and consistent with their intended configurations on an ongoing basis.

Relevant Considerations. As suggested in RFC 2527, security management controls include execution of tools and procedures to ensure that the operational systems and networks adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.[409] CAs and RAs may use these controls to ensure that their systems are working properly, such systems are operating as intended, and no one has tampered with them.

Other possible specific controls to ensure correct operation include:

- Maintaining an inventory of information assets, classifying them in accordance with their security requirements, and performing checks of the inventory,[410]
- Preventing the tampering with cryptographic modules during their lifecycle,[411] and
- Monitoring the configuration of CA and RA systems so that changes in the configuration would trigger an alarm.

Assessors should determine the extent to which such security management controls are necessary in the context of the assessed PKI. They should also account for any externally-imposed requirements, such as those stemming from applicable law or contracts. Assessors should, in addition, review the PKI's documentation to

[409] *Id.*

[410] ETSI TS 101 456 §§ 7.4.2(a), 7.4.6(h).

[411] *Id.* § 7.2.7.

determine whether the documentation imposes such controls. Finally, they should determine whether or not PKI participants are abiding by the requirements and standards in the PKI's documentation by implementing the required or disclosed controls.

Appropriate Requirements and Practices. A PKI's choice of which security management controls would be appropriate for its participants will be driven by the application for the certificates, their assurance levels, and the commensurate need for security. Usually, these controls are used only in the context of PKIs that provide higher assurance certificates.

The controls chosen by the PKI should be clearly stated in the PKI's documentation. Such controls should account for any requirements imposed from without the PKI. Finally, the PKI participants should implement the controls set forth in the PKI's documentation.

D.6.6.3 Life cycle security ratings

Issue Summary. This section addresses any security ratings earned by a developer that apply to the process by which it developed systems used in a PKI, especially CA or RA systems.

Relevant Considerations. This section extends the concept of placing controls on the development of systems used in the PKI, most often the software used to perform CA and RA operations, one step further than that described in PAG § D.6.6.1. Not only must certain controls be in place during the development process, but the development process must have been subjected to an assessment resulting in a specific rating. Life-cycle security ratings provide a measurement of the overall technical development process. These can include, for example, ratings based on the Trusted Software Development Methodology (TSDM), independent life-cycle security controls audit, and the Software Engineering Institute's Capability Maturity Model (SEI-CMM).[412]

Assessors should analyze whether the cost and effort to undertake an assessment to achieve such a rating is worthwhile to the PKI. If so, they should ascertain whether such a rating requirement is reflected in the PKI's documentation, with due consideration given to any external requirements imposed by law, contract, or otherwise. Finally, they should determine whether or not PKI participants are, in fact, using products that have been given the ratings required or disclosed within the PKI's documentation.

Appropriate Requirements and Practices. As was the case with respect to computer security ratings in PAG § D.6.5.2, the need for specific life cycle security ratings of CA or RA products or systems will depend on the PKI, the security needs of the applications of the certificates, and the assurance levels provided by the certificates. Generally speaking, requirements for using products that have certain life cycle security ratings are imposed only in PKIs providing higher assurance certificates. The extra expense associated with such products is often not worthwhile for PKIs providing lower assurance certificates.

If a PKI has a business need for using products that are the subject of a life cycle security rating, the PKI should consider which type of rating makes sense to obtain. The choice of which rating makes sense may be driven by an external requirement, such as one applicable by operation of law or contract. Whichever rating is appropriate for a PKI should appear in the PKI's documentation. Moreover, PKI participants should adhere to requirements or practices in the PKI's documentation regarding their choice of CA or RA products that have certain life cylce security ratings.

[412] RFC 2527 § 4.6.6.

D.6.7 NETWORK SECURITY CONTROLS

Issue Summary. This section concerns controls over networks, especially those used by CAs and RAs. It may cover both the production systems of CAs and RAs and their networks used for general corporate or organizational functions.

Relevant Considerations. Just as computer security controls are important for PKI participants with respect to the protection of single platforms and their applications, it is also important to protect the networks that tie such platforms together. These controls are especially important to certification service providers, such as CAs, RAs, CMAs, and repository service providers. As with single computing platforms, compromise to their networks could involve security breaches in systems protecting private keys, approving certificate applications, and other vital certification functions.

Some possible network security controls include:

- The use of firewalls and other controls to protect the integrity of the networks of PKI participants from intrusion from external domains;[413]
- Sufficiently strong authentication to ensure that the appropriate entities are communicating, e.g., an RA communicating with a CA, integrity mechanisms to ensure that the information being exchanged will not be modified, and confidentiality mechanisms to ensure that selected information is protected from unauthorized examination, for example through the use of digitally signed and encrypted messages,[414]
- Access controls protecting networks from unauthorized use, and
- Mechanisms to prevent damage from denial-of-service attacks.

As with the discussion of computer security controls in PAG § D.6.5, a comprehensive list of all the possible network security controls in the context of a PKI issuing higher assurance certificates, would be too long to be practical. Moreover, a comprehensive list could create security vulnerabilities when it is disclosed to others. Therefore, the six approaches discussed in PAG § D.6.5 would apply to network security controls, as well as computer security controls: (1) creating a general standard of conduct, such as the use of "trustworthy systems," (2) referring to the details in operational documents, (3) comprehensively listing all network security controls, (4) summarizing all network security controls, (5) setting out some controls and leaving others for operational documents, and (6) a combination of approaches.

> Assessors should determine which approach is implemented within the PKI's documentation and whether the documentation successfully carries out that approach. They should also determine whether the controls identified are appropriate for the level of assurances provided by the certificates and the security needs of the applications for which the certificates are intended. Finally, assessors should determine whether the PKI's participants are, in fact, implementing the security controls required or disclosed in this section.

Appropriate Requirements and Practices. When the components involved in issuing and/or managing any but the most rudimentary-assurance certificates are distributed, the network used by those components to exchange information should be secure enough to support the stated overall security and confidentiality requirements of the PKI. The first issue, then, is how the PKI should document its network security controls.

A PKI's assurance level, the use for certificates, and security needs will dictate the choice of which of the six approaches above for covering network security controls will depend on the circumstances of the PKI. The

[413] RFC 2527 § 4.6.7; ETSI TS 101 456 § 7.4.6(a).

[414] ETSI TS 101 456 §§ 7.3.3(e), (f), 7.4.6(b).

analysis in PAG § D.6.5 describing the advantages and disadvantages of the six approaches is applicable here as well. Under that analysis, Approach (6) may be the most effective choice, if the PKI uses a combination that includes Approach (5) (a brief list of some critical controls), coupled with approach (2) (a reference to controls appearing in operational documents. As with computer security controls, PKIs may also find it helpful to include a general trustworthiness requirement as a "backstop" measure. Again, however, referring to a set of criteria, such as criteria for an audit or rating will help flesh out the nature of "trustworthiness" and counter any impression that a "trustworthiness" requirement is hopelessly vague.

The network security controls, regardless of presentation, should be appropriate in light of the security needs of the PKI and the assurance level of its certificates. For instance, a PKI will likely want to require that PKI service providers have intrusion detection systems and software, firewalls and virus detection that are fully implemented to preclude purposeful attacks against PKI data including centers from succeeding. Such controls include technical measures taken to stop hacker-friendly packets or hostile employees from penetrating the PKI network, as well as training efforts designed to educate employees against allowing their systems to be duped into accepting virus-laden email or software.

The PKI should include a clear statement of the network security controls it wishes to impose in its documentation, which should also account for any external requirements. Lastly, PKI participants should implement the network security controls established by the PKI's documentation.

D.6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Issue Summary. This section concerns the controls required or utilized for the design, production, and delivery of cryptographic modules. In this section, the term 'cryptographic module' refers to a functional module with an identifiable boundary. Although not required, the use of a hardware-based cryptographic module makes the module boundary easy to identify and test.

Relevant Considerations. The use of a cryptographic module[415] can reduce the risk of unauthorized access to, or use of, the private key. As the biggest risk to a PKI is unauthorized use of a private key, and the cryptographic module may be its only countermeasure, the selection and evaluation of an appropriate cryptographic module is critical. A secure cryptographic module should operate as a black box exhibiting no externally observable phenomena that are detectable outside the box (e.g., power consumption, radiation, timing of blinking lights) or are dependent in any way on the cryptographic operations or keys.

There are several aspects to be considered when evaluating a cryptographic module. Examples include:

- the appropriateness of the cryptographic algorithm, e.g., characteristics such as key reversibility, strength.
- the selection of the variables of the cryptographic algorithm, e.g., key length,
- the cryptographic module is resistant to probing attacks,
- the module is protected by pick resistant locks, tamper evident seals, opaque removal-resistant coatings, etc.,
- the module has undergone environmental failure testing (i.e., it protects the private keys despite fluctuations in the operating temperature and voltage outside its normal operating ranges), and
- the module authenticates the user before importing, exporting, or activating keys. *See* PAG § D.6.2.6 (private key entry) and D.6.2.7 (private key activation).

[415] *See* NIST Security Requirements, *supra* note 391.

The use of a generally accepted evaluation and testing criteria for cryptographic modules, such as FIPS 140, is encouraged as correct module design involves non-readily apparent techniques. The quality of the process is best addressed by a laboratory validation of the cryptographic module. Consequently, "[r]equirements may be expressed through reference to a standard such as U.S. FIPS 140-1."[416] As a result, this section may overlap to some extent with the information corresponding to PAG § D.6.2.1 ("Standards for Cryptographic Module"). Nonetheless, the overlap can be minimized if the PKI discusses standards in the section of PKI documentation corresponding to PAG § D.6.2.1, cross-reference that section here if necessary, and discuss other engineering controls in this section.

Assessors should consider which engineering controls are important for cryptographic modules, other than the controls that would be in place automatically by virtue of meeting a certain standard. Assessors will generally want to rely on independent or third party cryptographic module evaluations as a basis for determining the appropriateness of a cryptographic module for a PKI. They should also determine whether there is a need for a specific level of assurance or trust in the module.

Assessors should then determine whether the PKI has documented such controls in its documentation. Documentation should account for any externally-imposed requirements, such as those arising from contracts, applicable law, or other external source. Finally, they should determine whether PKI participants are, in fact, using cryptographic modules that adhere to the requirements and practices in the PKI's documentation.

Appropriate Requirements and Practices. Cryptographic modules supporting the components of the PKI, including the CA, RA, subscriber systems, and relying party systems, should possess an appropriate level of assurance and should function properly. Many of the controls needed for proper functioning and security are addressed by a security rating in accordance with a standard, such as FIPS 140. Therefore, it is relatively uncommon to see a list of engineering controls for cryptographic modules in a PKI's documentation.To the extent a rating does not address all of a PKI's needs for security and trustworthiness, however, the PKI can establish additional requirements for engineering controls, taking into account any external requirements. Such requirements should appear in the PKI's documentation. Moreover, the PKI's participants should, in fact, utilize cryptographic modules that have incorporated the controls reflected in the PKI's documentation.

D.7 Certificate, CRL, And OCSP Profiles

Section 7 within a PKI document, such as a CP or CPS, sets forth the certificate profile and, where certificate revocation lists (CRLs) or the Online Certificate Status Protocol (OCSP) are used, the CRL and/or OCSP profiles used within a PKI. A profile refers to the content and format of certificates or CRLs. In particular, Section 7 addresses which fields are present in certificates or CRLs, what content populates these fields, and how this content should be interpreted.

D.7.1 CERTIFICATE PROFILE

Issue Summary. Section D.7.1 relates to the content and format of certificates used within the PKI. It includes information concerning version number of certificates, usage of extensions contained within the certificates, the cryptographic algorithm used to sign the certificates, naming forms, and constraints on naming. Specific topics within this section address requirements for or disclosures of the usage of certain certificate fields, what must appear within these fields, and the interpretation of the required or disclosed content.

[416] RFC 2527, *supra* note 193, § 4.6.8.

Relevant Considerations. The X.509[417] standard defines the required and optional technical contents of a certificate. The optional contents may not be applicable to all environments. A PKI may specify the contents, syntax, and use of these optional components. In fact, the PKI may set forth the required or actually used certificate formats in a separate certificate profile document. Certificate profiles have been constructed for many environments, including the IETF (e.g., the PKIX working group), the automobile industry (e.g., Automobile Network Exchange – "ANX"), a portion of the on-line credit card industry (e.g., SET), and the US government (e.g., DOD/MISSI, Federal PKI TWG, GSA ACES). Whether placed in a separate certificate profile document or included within a CP or CPS, certificate profile information facilitates interoperation among CAs.

The technical definition of certificate, CRL, and OCSP[418] message content provides for optional elements. Further, mandated elements of these technical objects may vary in the technical structure of their values. Given this flexibility, the contents of certificates, CRLs and OCSP messages will predictably vary in response to the local needs of a given PKI. Such variation may inhibit cross-domain interoperability. In some cases this effect is welcome in that it limits the likelihood a certificate may be relied on for purposes unrelated to its issuance.

A compelling need exists, however, for interoperability between autonomous trust domains in part to facilitate PKI-based commerce, particularly when such commerce is initiated on an ad-hoc basis across the Internet. The notion of a *profile* has emerged as a means to address interoperability concerns. Various standards bodies and industry trade groups have defined such profiles.[419] The nature of a profile depends critically upon the scope of its relevant domain. Typically, the broader the scope, the less restrictive the profile. The IETF's profile of certificate and CRL fields (RFC 2459[420]) is more relaxed in its specification of required certificate and CRL fields than other profiles, such as ANX. Conversely though, the ANX profile is intended to only be operational within a subset of the scope that is to be addressed by RFC 2459.

Failure to conform to RFC 2459 or equivalent broad industry standard does not *inherently* make a PKI less trustworthy. Nonetheless, certain fields in a certificate, CRL, or OCSP message may be necessary in order to establish a reliable degree of protection against known risks or legal requirements. For example, the key usage extension in a certificate is used to specify whether or not a key pair should or should not be relied on to create and validate a digital signature or whether such key pair is restricted to encryption purposes only (among other similar defined attributes).

PKI assessors should determine if the definition of a certificate profile is suitable to its intended scope. For example, a certificate containing extensive technical content in the Subject Directory Attributes field of an X.509-formatted certificate may inhibit interoperability across the Internet. Assessors should also confirm that any claimed conformance to a standard profile is in evidence. Finally, assessors should obtain detailed technical knowledge of all proprietary extensions that may be included.

In addition, assessors should review certificate content requirements applying to a PKI, whether those requirements are imposed by the PKI itself or externally by contract or applicable law. Assessors should then review the certificate profile requirements or disclosures of the PKI in this section of a CP, CPS, or a separate certificate profile document. Based on this review, they should determine whether all required certificate components appear in the PKI's certificate profile documentation.

Appropriate Requirements and Practices. The extent to which specific requirements and disclosures concerning certificate profile information is needed will depend on the PKI. For lower assurance certificates, utilizing specific certificate content, or setting forth detailed certificate content requirements, may not be worth

[417] *See* RFC 2527, *supra* note 193.

[418] *See* RFC 2560, *supra* note 348.

[419] *See e.g.*, PAG APP 2 (*Internet Public Key Infrastructure - X.509 Certificate and CRL Profile*, RFC 2459, Housley, R., Ford, W., Polk, T, Solo, D., IETF, *available at* <http://www.ietf.org/rfc/rfc.2459.txt>, hereinafter "RFC 2459").

[420] *Id*.

the trouble. Similarly, some PKIs may make use of only the basic fields within a certificate. If so, it may not matter what content, if any, appears in certificate extensions. Likewise, if a PKI makes use of only a single technology vendor's CA products or services, the applicable CP or certificate profile may not need to specify much detail to facilitate interoperation. A PKI may also want to simplify these requirements by referring to an external standard as a source of guidance for which fields are permitted or required, and how they should be populated. If nothing else, a standard may act as a default where the PKI does not specify more particular requirements. A failure to disclose technical structure does not inherently reduce a PKI's trustworthiness, although doing so may inhibit a party from choosing to rely in the absence of this information.

In other PKIs, however, it may be necessary to specify in great detail the certificate profile required or used, especially where the PKI is intended to accommodate disparate technology vendors' products or services. In such cases, the PKI may want to use a comprehensive listing of the contents of a certificate so that CAs within the PKI will know how to meet the PKI's requirements. Comprehensive certificate profiles should generally include the fields that must appear in certificates, requirements for the content of these fields, and permissible values for any optional fields.

PKIs need to balance the need to specify technical content and the possible need to facilitate interoperability. Local trust management needs may dictate technical content unique to a given trust domain, thereby inhibiting interoperability. On the other hand, cross-domain interoperability is vital to Internet commerce. The balance to be drawn will depend on the PKI.

Assessments of profiles also need to take into account that fact that profile content may be driven by associated technical needs. For example, S/MIME and SSL generally require the inclusion of an email address and Web server domain name in each certificate while IPSEC specifies the use of subject alternative name and extended key usage extensions. Another example is the use of OCSP by a PKI, which points strongly towards the use of the Authority Information Access extension (as defined in RFC 2459). PKI assessors may wish to evaluate the extent to which the profiles under their review are known to be compatible with the relevant software and hardware and, in particular, if that software or hardware implements functions that are implied by the technical description of a given profile.

Whatever balance the PKI draws when drafting certificate profile information, the PKI's requirements or disclosures concerning certificate content and a certificate profile should be consistent with requirements imposed externally by contract or applicable law. The PKI should create sufficient documentation of certificate profile information to enable PKI participants to implement the PKI's requirements. Finally, CAs should adhere to the PKI's documentation when configuring and issuing certificates.

D.7.1.1 Version Number(s)

Issue Summary. This section addresses the version of certificate issued within a given PKI. The question here is usually whether certificates are in X.509 format and, if so, whether they are X.509 version 1, version 2, or version 3 certificates. If the PKI supports non-X.509 certificates, this section addresses the format used and the version number of the applicable format.

Relevant Considerations. Most certificates in use today adhere to the X.509 certificate standard promulgated by the International Telecommunications Union (ITU) in conjunction with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)[421]. The basic certificate format appeared in version 1 of X.509 in 1988. Version 2 of the X.509 specification added the Issuer Unique Identifier and Subject Unique Identifier fields in 1993. In 1996, version 3 of the specification added a general extension mechanism to the basic format. The X.509 version 3 standard governs the use of certificate "extensions," additional fields added to the basic certificate format to provide extra information. X.509 version 3 described

[421] *See* RFC 2527, *supra* note 193.

the use of a set of standard certificate extensions, although a PKI can create and use its own privately-used extensions. Of the three versions of X.509, the most commonly used today is version 3.

Non-X.509 formats include Wireless Transport Layer Security (WTLS) certificates (in accordance with the Wireless Application Protocol or "WAP"), XML certificates, the Simple Public Key Infrastructure certificates (SPKI), and Pretty Good Privacy (PGP) certificates.

Assessors should review the PKI's documentation to determine which specification and version the PKI purports to adhere to in issuing certificates. They should ascertain whether the specification and version that the PKI uses are appropriate for the applications for which the certificates are intended. Assessors should also review requirements placed on the PKI by contract or applicable law to see whether the PKI's certificates meet these requirements. Finally, assessors should check to see whether the specification and version match the types of certificates actually issued by the PKI.

Appropriate Requirements and Practices. The types of certificates chosen by the PKI will be based on the intended applications for certificates issued within the PKI. For example, if PKI participants use applications that use X.509 certificates and it is important to the application that the certificate contain a reference to a particular certificate policy for machine processing or for legal liability management reasons, the PKI will want to require the use of X.509 version 3 certificates. Policy information is contained within the certificate's policy extension, and of the X.509 certificates, only X.509 version 3 certificates have extensions.

Similarly, specific applications may call for specific kinds of certificates. For example, the communications between a wireless WAP handset and a server to secure wireless communications will require the use of WTLS certificates. Likewise, XML and SPKI certificates are appropriate if, and only if, the applications using certificates are configured to accept these kinds of certificates.

Assuming that the type and version number of certificates are appropriate for the application, the type and version number should be consistent with requirements placed on the PKI by law and contract. In addition, the type and version number should be documented in the PKI's documentation, assuming that this level of detail is necessary to set forth interoperation criteria or otherwise. Moreover, the certificates actually issued within the PKI should match the type and version number set forth in this section of the PKI's documentation.

D.7.1.2 Certificate Extensions

Issue Summary. This section concerns the certificate extensions required by or used within a PKI issuing X.509 version 3 certificates.

Relevant Considerations. This section will apply only if the PKI is issuing X.509 version 3 certificates. Extensions are fields added to the basic certificate format to provide information in addition to that provided by the basic certificate fields. Standard certificate extensions fall into four categories:

- Extensions relating to keys or key usage,
- Extensions relating to certificate policies and policy documents,
- Extensions relating to specific attributes of the certificate subject or the issuer, and
- Extensions relating to controls over certification paths in connection with interoperation among PKIs.

Extensions relating to public or private key usage include:

- The key usage extension, which sets forth the permissible uses for the public key within the certificate,
- The extended key usage extension, which sets forth usage of the public key in addition to or instead of the purposes set forth in the basic purposes enumerated in the key usage extension,
- The subject key identifier extension, which contains an identifier of the public key of the subject of the certificate, such as a hash of the public key,
- The authority key identifier extension, which contains an identifier of the public key of the CA that issued the certificate, such as a hash of the CA's public key, and
- The private key usage period extension, which specifies the usage period of the private key corresponding to the public key within the certificate.

Extensions relating to certificate policies and policy documents include:

- The certificate policies extension, which contains references to the certificate policy, certification practice statement, and/or other documents, as well as other policy information,
- The policy mappings extension, which is used in a certificate issued from one CA to another as a declaration that one or more of the issuing CA's certificate policies is deemed equivalent to a certificate policy of the subject CA, and
- The policy constraints extension, which, when it appears in a certificate, can either require that certificates following in the certification path contain an acceptable certificate policy OID (in the certificate policies extension, the policy mappings extension, or both) or prohibit the use of policy mapping for the certificates following in the certification path.

Extensions relating to specific attributes of the certificate subject or the issuer include:

- The subject alternative name extension, which contains one or more names (other than the one appearing in the subject field) that act as an alternative name for the subject,
- The issuer alternative name extension, which contains one or more names (other than the one appearing in the issuer field) that act as an alternative name for the issuer,
- The subject directory attributes extension, which contains any information about the subject of the certificate, such as title, telephone number, or address,
- The authority information access extension, which indicates how to access a CA's information and services, such as OCSP services and policy information, and
- CRL Distribution point extension contains the location (URL, X.500 name, or e-mail address) at which a CRL can be obtained which would show the certificate if the certificate were to be revoked.

Extensions relating to controls over certification paths in connection with interoperation among PKIs include:

- The basic constraints extension, which shows whether the subject of the certificate can act as a CA or is limited to being an end-user and, if the subject is a CA, the extension can limit the length of the acceptable certification path (to prevent CAs from issuing certificates to too many layers of subordinate CAs),

- The name constraints extension, which limits certification path processing to certificates whose subjects having a certain names or limits certification path processing by excluding certain names, and

- The policy constraints extension (as described above).

In addition to the foregoing standard extensions, the X.509 version 3 specification is extensible. CAs can create their own private (local) extensions and populate them as they see fit. The critical factor with private extensions is whether their usage is documented properly so that the intended relying parties know how to understand their content and how to make use of it.

Assessors should review the PKI's documentation to see which extensions are used or required in certificates issued within the PKI, either standard or private extensions. They should determine whether the extensions used or required are appropriate for the applications for which the certificates are used. In addition, assessors should determine whether any external requirements, imposed by law or contract, require the usage of certain extensions. Finally, assessors should determine if the certificates issued contain the extensions required or disclosed in the PKI's documentation.

Appropriate Requirements and Practices. Certain optional certificate extensions are more relevant to an assessment of trustworthiness than others. These include basic constraints, key usage, and certificate policies. These fields, at a minimum, should generally be included in any profile, although local issues may dominate.

Also, to the extent that optional fields or extensions requiring object identifiers (OID) are employed in the profile, PKI assessors should confirm the existence and documentation of all relevant values. This need is particularly acute with respect to the use of the certificate policies extension, wherein a PKI's CP, CPS or other policies may be technically identified with OIDs.

It is appropriate for a trust domain to define private extensions. In the interests of interoperability and transparency of intent, however, standardized fields, extensions or values should be used whenever feasible.

A PKI should only use certificate extensions to the extent needed to support the applications for which the certificates are intended. For example, as noted above, IPSEC specifies the use of subject alternative name and extended key usage extensions and OCSP use points strongly towards the use of the Authority Information Access extension. Moreover, the PKI's use of extensions should be consistent with external requirements, such as those imposed by applicable law or contract.

D.7.1.3 Algorithm Object Identifiers

Issue Summary. This section addresses the question of which cryptographic algorithms and hash functions are used by the CA to create the digital signature on the certificate. A CA can use this section to identify the object identifier that corresponds to the cryptographic algorithm/hash function combination applicable to the private key that it used to digitally sign the certificate, which the CA may place in the signature algorithm identifier field.

Relevant Considerations. There are many encryption algorithms in use today, although the most commonly used algorithms to sign certificates are the RSA algorithm and the Digital Signature Algorithm defined in the Digital Signature Standard. By far, the most common algorithm used is RSA. The most common hash functions used for signing certificates are the U.S. government's Secure Hash Algorithm (SHA-1) and RSA Security's MD5 algorithm. Object identifiers have been registered for various combinations of encryption algorithms and hash functions.

Assessors should determine whether the PKI's documentation states which encryption algorithm and hash function were used to sign the certificate and whether the PKI identifies the corresponding object identifier.

Also, assessors should consider whether the encryption algorithm and hash function are appropriate and sufficiently secure for the applications for which the certificates are intended and whether they are consistent with any requirements imposed by contract or applicable law. Finally, assessors should determine whether certificates issued within the PKI were in fact signed using the encryption algorithm and hash function identified in this section.

Appropriate Requirements and Practices. The appropriate encryption algorithm and hash function will depend on the application for which the PKI's certificates are intended. Consistency with the vast bulk of the installed commercial software base, however, militates strongly in favor of the RSA algorithm. In terms of hash function, SHA-1 is considered to be more secure than MD5, but both are widely used. Whichever algorithm is chosen should be usable by the installed software base, and the PKI should consider the extent to which legacy applications can or cannot use one or the other.

In addition, the encryption algorithm and hash function that the PKI chooses should be consistent with any applicable requirements imposed externally on the PKI. The encryption algorithm and hash function actually used by the PKI should match the ones disclosed in the documentation and, the PKI should use the proper object identifier to identify the encryption algorithm and hash function.

D.7.1.4 Name Forms

Issue Summary. The issue covered by this section is what name forms do or should appear within the subject and issuer fields of certificates.

Relevant Considerations. The specific technical structure and values associated with Subject and Issuer names is often highly relevant to an environment's decision to accept and trust a certificate.[422] PKI assessors should confirm that a PKI has defined such naming rules and fixed name content, if any, in its documentation. Often, such content appears within section 3.1.1 of a PKI document and a cross-reference to that section may appear in section 7.1.4. Assessors should also check to determine if the applications for which the certificates are used require certain name forms, or whether certain name forms are required by applicable law or contract. For example, interoperability may require that name forms be identical throughout the PKI, and the CA may be subject to a contractual requirement to abide by a CP stating that requirement. Finally, assessors should determine if a PKI is using the name forms it purports to use in its documentation.

Appropriate Requirements and Practices. To the extent that name content is used to provide relying party notice (notwithstanding the guidance given above), this content too should be well documented and available for review. Name forms used within a PKI should be appropriate for the application and should be consistent with section 3.1.1 of the PKI's documentation and any externally-imposed requirements. Finally, the name forms actually used in certificates issued within the PKI should match the requirements or practices set forth in the PKI's documentation.

D.7.1.5 Name Constraints

Issue Summary. The issue with this section is whether the PKI makes use of the name constraints extension and the scope of the name space within which certification path processing must take place or the scope of the name space excluded from certification path processing.

Relevant Considerations. The name constraint's extension, as mentioned above, limits certification path processing to certificates whose subjects having certain names or limits certification path processing by excluding certain names. More specifically, the name constraints extension permits a CA to issue a certificate

[422] *Cf.*, PAG § D.7.1 (Certificate Profile) (requirements for inclusion of email address in an S/MIME certificate or a URL in a Web Server certificate).

or cross-certificate to another CA that limits the ability of relying parties to process a certification path containing that certificate or cross-certificate. For example, if ABC CA issues XYZ CA a certificate limiting the certification path to {C=US, O=XYZ . . .},[423] the XYZ CA must issue certificates to subjects having a distinguished name beginning with {C=US, O=XYZ} if relying parties will be able to process a certification path containing the certificate issued by the ABC CA.[424]

The name constraints is not a technical mechanism preventing XYZ from issuing certificates beyond that name space. To the contrary, the XYZ CA can continue to issue certificates to anyone it wants. The name constraint extension merely precludes a relying party from processing a certification path that includes the certificate issued by ABC to XYZ and a certificate from XYZ to someone outside that name space. This limitation is appropriate where ABC trusts XYZ and subjects within the XYZ domain, but ABC does not want to take the risks involved with certificates issued outside XYZ whose certification paths include a certificate that ABC has issued.

The name constraints extension can also be used to exclude a certain name space. For example, if ABC does not trust the DEF domain, ABC can place a limitation in the name constraints extension of the certificate it issues to XYZ excluding the DEF name space {C=US, O=DEF . . .}. Again, the name constraints extension does not technically prevent the XYZ CA from issuing certificates to subjects whose distinguished names begin with {C=US, O=DEF . . .}. Rather, such a limitation within the name constraints extension only prevents a relying party from processing a certification path that includes the certificate issued by ABC to XYZ and a certificate from XYZ to someone within the DEF name space. This limitation is appropriate if ABC does not trust DEF and does not want to take on the risk associated with having relying parties rely on certificates issued to DEF subjects whose certification paths include a certificate that ABC issued.

Assessors should determine whether the applications for which a PKI's certificates are intended call for the limitation of certification path processing, either limiting processing to a certain name space or excluding a certain name space. They should also be aware of any externally-imposed requirements, for instance requirements set by contract or applicable law. Assessors should also ensure that all appropriate limitations, and only such appropriate limitations, are documented in the PKI's documentation. Finally, assessors should determine whether the PKI populates the name constraints extension of certificates it issues in accordance with its documentation.

Appropriate Requirements and Practices. The need to limit certification path processing using the name constraints extension will depend on the circumstances of the PKI. If a CA issues no certificates to other CAs, this section will not be relevant. In addition, if all subordinate CAs within a PKI are in the control of a single entity, the single entity will likely have no need for name constraints. Moreover, a CA issuing certificates for use within a broad, public community will also find little use for name constraints in that the purpose of the PKI may be to disseminate certificates within as broad a population as possible. Further, if the relying party software is unable to process the name constraints extension, then the PKI will need to find other means for accomplishing the purpose of the name constraints extension.

Name constraints will be of most use when one organization's CA is certifying, either on a unilateral or cross-certification basis, the CA of another organization and a need exists to establish technical mechanisms to reduce the risk associated with the certified organization's practices. In other words, the names constraints extension is most useful in an interoperation context.

[423] The information in the brackets represents a distinguished name where the country equals the United States, and the applicable organization is XYZ.

[424] It is not necessary for name forms to be X.500 names for the name constraints extension to be used. For example, name constraints may be used in conjunction with e-mail addresses contained in certificates such that a relying party can process a certification path containing the certificate only if subsequent certificates are issued to subjects having e-mail addresses containing a specific domain name or if subsequent certificates are not issued to subjects having e-mail addresses containing a specific domain.

In any case, the name constraints extension should only be in use where an application and its business requirements raise a need for it. The PKI should abide by any requirements imposed by contract or law either to use the extension or not use the extension, as appropriate. The PKI should document how the name constraints extension is populated when it makes sense to use the extension, and certificates issued within the PKI should contain the name constraints extension content called for by the PKI's documentation.

D.7.1.6 Certificate Policy Object Identifier

Issue Summary. The issue raised in this section concerns whether the PKI populates the certificates it issues with a certificate policies extension containing an object identifier corresponding to a policy document.

Relevant Considerations. The certificate policies extension is intended to convey policy information or references to policy information. Specifically, a PKI can place the object identifier of a certificate policy within the certificate policies extension. The object identifier can enable a relying party to configure its systems to cause its software to look for the OID of an acceptable certificate policy, permit the transaction to continue if the system finds the OID of an acceptable CP in the certificate, and halt the transaction if it does not.

The use of an OID in the certificate policies extension assumes that relying parties are aware of the OID of the relevant certificate policy and have the capability of programming their systems to look for it. That is, unlike a URL, an OID does not tell a person unfamiliar with the number how to find the document corresponding to the OID. Moreover, certain legacy applications may not be able to parse the certificate and find the OID in the certificate policies extension.

Even if applications cannot today process an OID in the certificate policies extension, it may make sense from a legal perspective to include an OID in the certificate policies extension. A PKI's policy documents may contain disclaimers of warranty and limitations of liability, to which it may hope to bind relying parties. It may be better to attempt to provide notice to relying parties of the relevant policy, even with software limitations, than make no attempt at all.

Assessors should determine whether placing an OID in the certificate policies extension would facilitate machine-processing of certificates by the relevant application and whether use of a certificate policy OID makes sense from a technical and legal perspective. They should also ascertain whether applicable law or contract dictates the use of an OID. Assuming that OID usage makes sense for the application for which the certificates are intended, assessors should review the PKI's documentation to determine whether the PKI does actually populate the certificate policies extension and, if so, which OID it uses. Assessors should check which document corresponds to the OID and whether that document is an appropriate policy for the PKI. Finally, assessors should check whether the OID in the certificates issue in the PKI matches the OID disclosed in the PKI's documentation.

Appropriate Requirements and Practices. The need to place an OID within the certificate policies extension will depend on the PKI, whether it uses extensions at all, whether a CP applies to the PKI, whether applications will be able to make use of it, and whether legal considerations militate in favor of its use. The PKI will want to abide by any requirements for including a certain OID if imposed by contract or applicable law. If the PKI requires or uses an OID, the PKI should determine how relying parties will use it. An OID placed in a certificate policies extension does not itself indicate where to find the document corresponding to it, if a relying party is unfamiliar with it. Therefore, a policy-creating body will likely want to provide notice of its policy's OID if relying parties are to make use of it, including through placement in the PKI's documentation, assuming that the relying party or relying party community is not the policy-creating body itself. Finally, certificates issued within the PKI should contain OIDs to the extent required in the PKI's documentation.

D.7.1.7 Usage of Policy Constraints Extension

Issue Summary. Section D.7.1.7 concerns a PKI's use of the policy constraints extension and, if the PKI uses it, the policy limitations placed within the extension.

Relevant Considerations. The policy constraints extension, as noted above, can either require that certificates that follow in the certification path of a certificate contain an acceptable certificate policy OID or prohibit the use of policy mapping for the certificates following in the certification path. If the extension includes the required explicit policy indicator, certification paths that include the certificate must include certificates containing a specific object identifier in the certificate policies extension if relying party systems are to process the certification path.

The require explicit policy indicator is useful in the context of interoperation. If one organization's CA issues a certificate or cross-certificate to another organization's CA, the first CA may want to minimize the risk associated with certificates issued by the certified CA to the extent relying parties could process a certification path that includes the certificate issued by the first CA. The first CA may be willing to certify the second CA and permit certification path processing, but only if the second CA issues certificates with a certain policy OID indicating the CA's compliance with the policy.

The policy constraints extension may also include the inhibit policy mapping indicator. If the extension includes this indicator in a certificate, policy mapping is not permitted in certification paths that include the certificate. Again, in the context of interoperation, where one CA certifies or cross-certifies with another CA, the first CA may be willing to certify the second CA but only if the second CA does not permit policy mapping. The first CA may perceive risk involved with relying parties processing a certification path including one of its certificates where, through policy mapping, the relying party is not relying on a certify that is subject to the specific policy desired by the first CA.

As with name constraints, the policy constraints extension does not preclude a certified CA from issuing certificates outside the limitations in the require explicit policy or inhibit policy mapping indicator. Rather, it merely stops the successful processing of a certification path including a certificate containing the indicator if the limitations set by the indicator are exceeded.

Assessors should determine whether policy constraints are appropriate within the context of a PKI's operations. In addition, assessors should account for any requirement of policy constraints imposed either by contract or applicable law. If policy constraints are appropriate, assessors should review the PKI's documentation to see whether the PKI has disclosed or required policy constraints. Finally, assessors should determine whether certificates issued within the PKI contain the policy constraints disclosed or required by the documentation.

Appropriate Requirements and Practices. Whether policy constraints are appropriate for a given PKI will depend on whether the PKI needs to facilitate interoperation and whether the goals of limiting policies within a certified domain can be accomplished just as well through appropriate contracts. Even if the domain of a certified CA is required by contract to adhere to a given policy or is forbidden by contract from issuing certificates that permit policy mapping, a PKI may find it helpful to use the policy constraints as an extra measure of protection. The PKI should also populate the policy constraints extension if required to do so by contract or applicable law. Any use of the policy constraints extension should be documented and the certificates issued by CAs in the PKI should contain the policy constraints limitations set forth in the PKI's documentation.

D.7.1.8 Policy Qualifiers Syntax and Semantics

Issue Summary. The issue in this section is whether the PKI requires or uses the policy qualifiers within the certificate policies extension to convey policy information and, if so, what policy information is conveyed.

Relevant Considerations. The certificate policies extension, in addition to providing a field for an OID pointing to the certificate policies under which a certificate was issued, contain two fields for additional kinds of information. First, the certificate policies extension can include a user notice qualifier. The user notice qualifier includes either notice text that a CA places within it or a number that causes the software of certificate viewers to display certain text pre-placed within the software. The user notice qualifier is useful from a legal perspective, because the CA can place critical notices, disclaimers of warranty, and limitations of liability within the text of the user notice qualifier or in text pre-placed within the software, which a number in the user notice qualifier causes the software to display.

The certificate policies extension can also include a CPS pointer qualifier, which is a field intended by the drafters of X.509 to contain the URL of the CPS under which the certificate was issued. The CPS pointer qualifier information must be in the form of a URL. The CPS pointer qualifier is also useful from a legal perspective, because the document located at the designated URL can contain critical notices, disclaimers of warranty, and limitations of liability.

Assessors should determine whether the applications for which a PKI's certificates are intended would benefit from notices included in policy qualifiers within certificates. They should also determine whether the PKI is required, by contract or applicable law, to include certain information within policy qualifiers. If the PKI does or must use policy qualifiers, assessors should determine if the PKI's documentation includes the requisite policy qualifiers. Lastly, assessors should see if the certificates issued within the PKI contain the appropriate policy qualifiers as documented.

Appropriate Requirements and Practices. The desirability of policy qualifiers for a given PKI will depend on the application for which the certificates are intended. For example, if a PKI is used only for intra-organizational communications, it may not be worth the effort to use policy qualifiers. The organization's members are only dealing with other members. In addition, if the only relying party for the certificates is the CA itself, the CA will not have a need to dictate terms and conditions to the relying party through policy qualifiers.

In many if not most cases, however, a PKI will find it desirable to include policy qualifiers within its certificates. The certificate policies extension and the policy qualifiers within it are the fields that are expressly intended to convey legal and other policy information to relying parties. If the PKI wishes to convey any legal or other policy information at all, this is the intended place to do it. Some software, however, especially legacy applications, will not be able to display policy qualifier information to end users. Therefore, CAs may need to find alternative ways to convey legal information to relying parties. Nevertheless, it may be better to populate the policy qualifiers, even if some cannot see the information, than not make the attempt at all.

Assuming that populating the policy qualifiers is appropriate in the PKI, or if they are required by contract or applicable law, the PKI should clarify its use of policy qualifiers in its documentation. In addition, the policy qualifiers that appear in certificates should match the ones described in the documentation.

D.7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Issue Summary. Section D.7.1.9 addresses the issue of whether a PKI sets the criticality flag of the certificate policies extension or requires that the flag be set in certificates issued within the PKI.

Relevant Considerations. X.509 version 3 certificate extensions contain an extension flag. According to the X.509 standard, if the certificate extension criticality flag is marked as TRUE, then the certificate processing software of the relying party should consider the certificate valid only if the certificate can be processed in accordance with the extension. If the certificate cannot be processed in accordance with the extension or if the certificate processing software does not recognize the extension, then the certificate processing software should consider the certificate invalid. By contrast, if the certificate extension criticality flag is marked as FALSE, then

the certificate processing software should be able to consider the certificate valid even if it cannot process the certificate in accordance with the extension or does not recognize the extension at all.

With respect to the certificate policies extension, the criticality flag, if set, is intended to indicate that the relying party software and the relying party must be able to rely on the certificate in accordance with one of the certificate policies whose object identifier appears within the certificate policies extension. According to the X.509 standard, if the relying party is unwilling to abide by at least one of the certificate policies listed in the certificate policies extension, the relying party should not rely on the certificate. If, however, the criticality flag is not set, the relying party is permitted to ignore the certificate policies extension or process the certificate in accordance with one or more of the policies listed in the extension, at the option of the relying party.

Many software applications, however, are unable to process extensions, including the certificate policies extension. If the software is unable to process the certificate policies extension, it will not be able to process the criticality flag of the extension. Even if a CA makes the certificate policies extension critical, therefore, some relying party software may not show that a certificate is invalid even if the relying party is unaware of the certificate policies extension content, or even if the relying party does not or would not agree to the policy terms referred to in the certificate policies extension. Accordingly, the ability to enforce policies using the criticality flag does not exist in all environments.

Even if the relying party software does process the certificate policies extension and its criticality flag, a relying party can process the certificate by listing the object identifier in the certificate policies extension as an acceptable CP. A relying party designating an OID as an acceptable certificate policy in the relying party's own software, however, is not the same thing as manifesting assent to a CP from a contractual perspective. That is, the relying party may set its software to accept a certain OID appearing in a certificate, but attempt to argue in a subsequent litigation that doing so does not bind the relying party to any agreement. It is still an open question whether designating the OID within the relying party software constitutes assent to a CP or other document referred to in a certificate policies extension.

Finally, the criticality flag may cause certain applications to fail, especially legacy applications. Consequently, assessors should determine the appropriateness of the use of the criticality flag first by determining whether its use would cause applications to malfunction. If it does not, assessors should determine whether relying party software will be ale to process the criticality flag. They should also determine if the relying party software shows a certificate to be invalid, if the relying party software does not show that the certificate policies extension contains an OID acceptable to the relying party. Assessors should also ascertain whether the use of the criticality flag is otherwise appropriate for the PKI and whether any external requirements, such as those imposed by contract or law, require the use of the criticality flag. Assuming that the use of the criticality flag is appropriate within a given PKI, assessors should determine if the PKI has documented its use of the flag and whether certificates actually set the criticality flag within the certificates issued within the PKI.

Appropriate Requirements and Practices. The usefulness of the criticality flag of the certificate policies extension as a technical means of ensuring assent to the information within the certificate policies extension is uncertain for the reasons described above. As a result, most PKIs will need to make a choice of either requiring that relying parties use the software needed to process the criticality flag or else depend on other mechanisms to enforce policy requirements, such as a relying party agreement implemented in a way that it binds relying parties. Assessors should ensure that the use of the criticality flag makes sense for the applications for which the certificates are intended. Even if the criticality flag can be used within a PKI, the PKI will likely want to have other legal means, such as the use of a relying party agreement, to enforce specific policies to act as an additional mechanism to bind relying parties to a particular policy.

If the use of the criticality flag makes sense for the application for the certificates, or if external requirements mandate the use of the criticality flag, the use of the criticality flag should be noted within the PKI's documentation. Moreover, the certificates actually issued should in fact set the criticality flag.

D.7.2 CRL PROFILE

Issue Summary. This section concerns the content and format of certificate revocation lists used within the PKI, assuming that the PKI makes use of CRLs. It includes information concerning the version number of CRLs used and the usage of extensions contained within the CRLs.

Relevant Considerations. The CRL profile determines the technical content that a certificate-using entity will use to determine the validity of a particular certificate. As such, explicit guidance as to how to interpret the syntax of a CRL is stated in the CRL Profile. The CRL profile is also used by a PKI to determine what data, extensions, and attributes to include within a CRL before it is issued.

As with certificates, the X.509[425] standard defines the required and optional technical contents of certificate revocation lists. The optional contents of CRLs may not apply to all environments. A CRL profile may document the contents, syntax, and use of these optional components. Use of a CRL profile permits interoperation among the different participants within a PKI.

Assessors should determine the extent to which the PKI needs a detailed certificate profile and what items should be included within the CRL profile, based on the needs of the applications using CRLs. Assessors should also consider the level of detail for the CRL profile to set minimum requirements to permit interoperability, without excessive technical content specific to one environment that may act to inhibit interoperability among different environments within the PKI.

In addition, assessors should review CRL content requirements that apply to a PKI, which may be imposed by contract or applicable law. Assessors should check to see if these requirements are met, according to the PKI's documentation. Moreover, assessors should also determine if private extensions to CRLs would be useful and, if so, ensure that the PKI documents the use of these private extensions. Finally, assessors should determine whether the CRLs actually issued within the PKI contain the content provided for in the PKI's documentation.

Appropriate Requirements and Practices. Since the number of optional components in a CRL pales in comparison to a certificate, the CRL profile is often relatively short. If there is significant overlap between the certificate and CRL profiles, they may be combined to produce one profile for a community. A short CRL profile may also be appropriate for PKIs issuing lower assurance certificates or where the PKI makes use of a single technology vendor's products or services. A PKI may also prefer to simplify its requirements by referring to an external standard, such as RFC 2459.

In some instances, however, the need to assure interoperability may require a somewhat detailed CRL profile. Where a detailed CRL profile is needed, the profile should specify the contents of a CRL, including all mandatory and optional components, and issue guidance to the default values of missing components, to the extent needed by the participants within the PKI to interoperate.

At a minimum, the PKI should generally document whatever requirements placed on CRL content that are appropriate for the PKI. Also, the PKI should also include in its documentation CRL content components that are required by contract or applicable law to be included. Finally, the CRLs actually issued within the PKI should contain the information required or disclosed by the PKI's documentation.

D.7.2.1 Version Number(s)

Issue Summary. This section specifies the X.509 version number of the CRLs issued within the PKI, either version 1 or version 2.

[425] *See* RFC 2527, *supra* note 193.

Relevant Considerations. With the adoption of the X.509 version 3 specification in 1996, the extension mechanism was defined, which permits a PKI to extend certificate content beyond the basic fields and, in fact, the mechanism permits the creation and use of new fields to cover any specialized content that a PKI may care to place within a certificate. At the same time, X.509 applied the extension mechanism to CRLs to permit the expansion of CRL content in the same way that certificate content can be expanded. CRLs containing the basic information originally defined in X.509 are known as version 1 CRLs, while CRLs making use of the extension mechanism are known as version 2 CRLs.

Two important considerations regarding v2 CRLs are the use of CRL Distribution points and reason codes; neither are mandated. Exclusion of each does not diminish the trustworthiness of a PKI. The relevant technical standards (e.g., RFC 2459) provide more extensive guidance use of these and other options fields and extensions.

Assessors should consider whether a particular PKI needs CRL extensions, based on the applications that use the CRLs. If so, assessors should see whether or not the PKI documents the fact that it requires or uses version 2 CRLs and, if not, assessors should see whether or not the PKI documents a requirement or use of version 1 CRLs. In making this analysis, assessors should take into account any contractual or regulatory requirements for either version 1 or version 2 CRLs. Finally, assessors should determine whether the PKI's CRLs are version 1 or version 2 CRLs and whether the version used is in accordance with the PKI's documentation.

Appropriate Requirements and Practices. The need for CRL extensions dictates the version number of CRLs appropriate for a PKI, and the need for CRL extensions will in turn depend on the CRL-processing applications. It is important to note that a v2 CRL profile that contains no v2 technical content is in fact a v1 CRL and should be identified as such. Moreover, it is acceptable to publish v1 CRLs even though the certificates listed are X.509 v3 certificates. Conversely, an X.509 v1 certificate may be listed on a v2 CRL.

To the extent the use of CRL extensions are appropriate within the PKI, the PKI's documentation should reflect to the usage of version 2 CRLs, and the CRLs actually issued within the PKI should state that they are version 2 CRLs and contain the specified CRL extensions. If, however, CRL extensions are not needed or are inappropriate for a PKI, the PKI documentation should reflect the usage of version 1 CRLs, and the CRLs actually issued should show the version 1 designation and not contain CRL extensions.

D.7.2.2 CRL and CRL Entry Extensions

Issue Summary. This section applies where the PKI uses version 2 CRLs. It addresses the question of how optional fields and CRL extensions should be implemented.

Relevant Considerations. Assuming that a PKI uses CRL extensions, it may use some of the following standard extensions:

- The CRL number extension, which indicates a number assigned to the CRL so that a relying party can determine if any it has missed any past CRLs,

- The reason code entry extension,[426] which provides a code indicating a reason why the certificate appears on the list, such as key compromise or that the certificate was superseded by a new certificate,

[426] A CRL entry extension, as opposed to an extension, is an extension that is associated with the entry for each certificate that appears within the CRL. That is, if there are four certificates listed in the CRL, there will be four instances of an entry extension. By contrast, there is only one CRL extension for each CRL, no matter how many certificates are listed in the CRL.

- The invalidity date entry extension, which can provide a date in the past in which a private key corresponding to the public key in the revoked certificate was known to be secure prior to a compromise of the private key,

- The hold instruction code entry extension, which provides a code corresponding to the response that should be undertaken in response to a suspended certificate,

- The delta CRL indicator extension, which indicates that the CRL is a so-called "delta CRL," that is, a CRL that shows only changes in information from the last full CRL,

- The issuing distribution point extension, which provides information about the name of the CRL (to prevent substitution attacks), whether the CRL is limited to end-user subscriber certificates or CA certificates, and whether the CRL is to include revocations for only certain reasons, and

- The certificate issuer entry extension, which identifies the CA issuing the certificate, important information in the event the CRL is issued by a different authority from the CA that issued the revoked certificate, as in the case of the use of so-called "indirect CRLs."

Assessors should determine whether the use of any standard or private extensions would be useful or helpful for the applications processing CRLs, and whether the applications can process CRL extensions. If so, assessors should review the PKI's documentation to determine if the PKI has documented the use of CRL extensions to implement the extensions appropriate for the PKI. Finally, assessors looking at a PKI purporting to use CRL extensions should determine whether the CRLs issued within the PKI actually make use of these extensions.

Appropriate Requirements and Practices. A PKI's decision to use or not use CRL extension will largely depend on the applications and types of CRLs that it uses. For example, it will need to use the delta CRL indicator extension if it is using applications that create and make use of delta CRLs. If the PKI does not require or make use of these applications, it will not likely want to take the effort to populate the CRL extensions corresponding to these applications.

If the use of applications requiring certain extensions is helpful or required, by contract or regulatory mandate, then the PKI should document its use or requirement of CRL extensions. In addition, the CRLs actually issued within the PKI should contain the extensions set forth in the documentation.

D.7.3 OCSP PROFILE

Issue Summary. Section D.7.3 relates to the content and format of requests for certificate status and responses to certificate status queries using the Online Certificate Status Protocol (OCSP),[427] to the extent OCSP is used within the PKI. It includes information concerning the version number of OCSP adhered to and the usage of OCSP extensions.

Relevant Considerations. This section only applies if the PKI is using OCSP. OCSP (RFC 2560) is a relatively new protocol that is intended to supplement or in some instances wholly replace the use of CRLs. Its chief characteristic lies in it being an on-line mechanism. Issues associated with OCSP thus largely involve questions of response timeliness and its relationship to CRLs.

At present, there are no known standardized profiles per se of OCSP other than that currently documented in RFC 2560. OCSP does however enable the inclusion of optional elements and variant content within its mandated elements and some standardized extension are either defined directly in RFC 2560 or proposed for Internet-wide standardization.

[427] *See* RFC 2560, *supra* note 348.

PKI assessors should be aware that a PKI's use of OCSP does not require the existence of CRLs. All "definitive" OCSP responses are digitally signed; requests may be signed as local needs require. OCSP shares with certificate and CRLs the characteristic of extensibility. RFC 2560 defines certain standard extensions, none of which are mandated.

As with certificates and CRLs, OCSP message content provides for optional elements. Mandated elements of these technical objects may vary in the technical structure of their values. Again, with this flexibility, the contents of OCSP messages will predictably vary in response to the local needs of a given PKI, which may inhibit cross-domain interoperability.

Assessors should determine whether the use of OCSP is helpful or useful within a PKI and for the applications used by the PKI participants. This analysis should be made in conjunction with the analysis of OCSP under PAG § D.4.9 (Certificate Revocation and Suspension) and any requirements imposed by applicable law or contract. If the PKI uses OCSP, assessors should determine whether the PKI has documented its OCSP profile and practices. Finally, assessors should check whether the OCSP requests and responses issued within the PKI correspond to the documented OCSP profile.

Appropriate Requirements and Practices. As with CRLs and certificates, the need for a detailed OCSP profile is likely to be greater where interoperation is important, especially where the products or services of different technology vendors are in use. In the case of a PKI issuing lower assurance certificates, the PKI may not be using OCSP at all or such PKIs may not need much detail relating to OCSP responses. A PKI may simply wish to refer to a standard to simplify its requirements for OCSP.

The need for detail relating to an OCSP profile, where the PKI uses OCSP, will depend on factors such as the need for extensive interoperability guidelines. Where detail is needed, the OCSP profile should include the mandatory and optional components of the request and response and provide guidance on the default values of missing components. The PKI should balance the need for detail with the need to avoid excessive detail that may in fact inhibit interoperation. Any OCSP profile should include elements required by contract or applicable law. The PKI should place its OCSP profile within its documentation. Finally, the content of a PKI's OCSP requests and responses should match the content required or disclosed within the PKI's documentation.

D.7.3.1 Version Number(s)

Issue Summary. The issue in this section is which version of OCSP is being used as the basis for establishing an OCSP system.

Relevant Considerations. Work is currently underway in the IETF to define and develop OCSP v2.[428] This work augments OCSP with features that enhance its usability in certain use cases. Work is also underway to define two additional standard extensions, or request types. These are Delegated Path Validation (DPV)[429] and Delegated Path Discovery (DPD).[430] PKI assessors should note well that at this time these draft work products are subject to revision. This work is nonetheless relevant to the appropriate use of OCSP as defined in RFC 2560 and discussed elsewhere in this section.

Assessors should determine whether the features provided by OCSP version 2 are useful or helpful to a PKI, and if they are required by contract or applicable law. Assessors should also look at the PKI's documentation to determine whether the PKI purports to require or use one version or another of OCSP. Lastly, assessors should check to see whether the OCSP requests and responses issued within the PKI are in accordance of one or the other version of OCSP.

[428] *Id*.

[429] *Available at* <http://www.ietf.org/ids.by.wg/pkix.html>.

[430] *Id*.

Appropriate Requirements and Practices. The decision to use version 2 of OCSP will be driven by the applications producing and receiving OCSP requests and responses. If version 2 OCSP requests and responses are needed or appropriate for the applications, or if they are required by external constraints, such as applicable law or contract, the PKI should document its use of OCSP v2. Otherwise, the PKI documentation should reflect OCSP v1. Finally, the OCSP requests and responses actually issued within the PKI should be in accordance with the version of OCSP disclosed in the PKI's documentation.

D.7.3.2 OCSP Extensions

Issue Summary. This section concerns the use of OCSP extensions, and which extensions, if any, a PKI is using or requires.

Relevant Considerations. The standards relating to OCSP extensions are somewhat in flux, although OCSP permits the use of the four entry extensions that apply to CRLs, namely the reason code, hold instruction code, invalidity date, and certificate issuer entry extensions. Moreover, OCSP makes use of five additional extensions:

- The nonce extension, which cryptographically binds an OCSP request and a response to prevent replay attacks,
- The CRL references extension, which indicates the CRL on which a revoked or suspended certificate can be found and is useful where OCSP is used between repositories or as an auditing mechanism,
- The acceptable response types extension, which specifies the kinds of OCSP response types that an OCSP client understands,
- The archive cutoff extension, which indicates that an OCSP responder is retaining revocation information beyond a certificate's expiration in an effort to provide evidence that a digital signature was or was not reliable on the date produced, even if the certificate has since expired, and
- The service locator extension, which enables an OCSP server to route an OCSP request to the OCSP server that is known to be authoritative for the identified certificate.

Assessors should determine whether applications using OCSP within the PKI need or would benefit from the use of OCSP extensions. They should also consider whether any external requirements, imposed by contract or applicable law, require the use of one or more of the OCSP extensions. If so, assessors should review the PKI's documentation to determine which OCSP extensions are required or disclosed there. They should also check the format of OCSP requests and responses actually produced by PKI participants to see if their use of extensions matches the extension use disclosed or required in the PKI's documentation.

Appropriate Requirements and Practices. The use of OCSP extensions will likely be useful only where needed to meet specific needs based on the applications using OCSP. If the applications cannot make use of OCSP extensions, it is probably not worth the effort of documenting and using OCSP extensions. If OCSP extensions are appropriate for a PKI, the PKI's documentation should reflect the use of these extensions and the requests and responses should use extensions in accordance with the documentation.

D.8 Specification Administration

D.8.1 SPECIFICATION CHANGE PROCEDURES

Issue Summary. Section 8.1 addresses the issue of how a PKI participant changes a particular PKI document, such as a CP or CPS. That is, what procedures does the corresponding section of the PKI document require or disclose for the amendment of that document?

Relevant Considerations. An author of a PKI document will, at some point, need to update the document. Contractual and policy documents, including those relating to PKI, commonly state the procedures that must be followed if they are to be amended. Vendor agreements commonly follow the pattern of other contracts in requiring that amendments be in writing and signed by the parties to be bound by the amendments. Web-based form agreements often have less formal change procedures because they may apply to single certificates or acts of reliance and it may not be possible to administer and keep track of amendments. Sophisticated change procedures most often appear in larger policy documents such as CPs and CPSs.

Change procedures for more sophisticated documents may include topics such as:

- materiality of the change,
- frequency of review of the document,
- whether comments from or the assent of PKI participants or others must be solicited before the amendments can be effective,
- acceptable notification mechanisms,
- the timing of notification and comments (if permitted),
- who, within the organization that wrote the document, has been designated to receive comments to the document (if comments are permitted),
- how permitted comments are processed, and
- how and when the document becomes final following the receipt of permitted comments.

Change procedures may also include those items that can change without notice and those items where notification is required. Change procedures may also include a threshold list of items or degree of change, beyond which the PKI participant writing the document must change the version number or identification (OID or URL) of the document. Minor changes not affecting material contract terms or the rights and obligations of the parties may not trigger the need to change an OID, while a major change may.

The notification procedures used by PKIs generally fall within two categories, the "push" category and the "pull" category. "Push" procedures refer to methods by which the document's author takes active steps to deliver ("push") notice of an amendment to the affected parties. "Pull" procedures refer to methods by which an author makes amendments available for viewing as they are written, but does not take steps to deliver them to affected parties. Rather, these mechanisms require interested parties to monitor the document when they feel the need to do so, and retrieve (or "pull") amendments whenever they occur.

The issue of "push" versus "pull" notification becomes relevant if the document being modified is part of a contract or is itself a contract. The author of the document may confront the issue of how, from a contractual perspective, parties affected by the amendment will be bound by it. In the absence of any contractual provisions to the contrary, binding an affected party often means that the affected party must assent to the amendment

following actual or constructive notice of it. Such a requirement would suggest a preference or requirement for "push" mechanisms.

The author of the document may, however, specify change procedures for the document to be amended in the original document or another agreement, to which the affected party does manifest assent. The change procedures assented to may call for "pull" notification and vary, by contract, what otherwise might be a right to "push" notice prior to an amendment under applicable law. The issue with these contractual specifications of "pull" change procedures is whether they are enforceable. The enforceability of pull mechanisms will depend on the applicable law in the relevant jurisdiction and whether affected parties include consumers.

A related issue is the way in which parties effected by an amendment assent to the amendment. Indicating assent may be an actual, as in the process of obtaining a signed (by handwriting or digital signature) communication that indicates assent to the amendment. Assent may also be deemed to occur, as in stating that the continued use, of a certificate, certification product, or certification service, to be assent to an amendment. Continued use, however, where no effective notice of changes in terms has taken place, may not serve as such assent. There is a range mechanisms for assent that fall between these two opposites. In the absence of any contractual provision to the contrary, binding a party to an amendment may mean that the party must assent to the amendment by affirmative conduct indicating agreement to it.

As with the case of notice, however, a contract may vary the requirement for assent to amendments. For instance, a contract may state that assent is deemed to occur upon certain events, such as the continued use of a product or service. These contractual terms are common in the banking and credit card world, where a credit card issuer changes the terms and conditions applicable to a card holder and the card holder's use of the card past a certain date is deemed to constitute acceptance of the new terms and conditions. Assessors may, however, want to determine whether such deemed assent terms are enforceable under applicable law.

Assessors should review a PKI's documents to determine what they say about change procedures and which change procedures make sense for each document. In ascertaining what makes sense for a given document, assessors should consider whether the PKI serves the public and could benefit from public comment, whether the PKI serves important customers or constituents from whom it may want to gather comments, or whether the PKI is strictly internal where commenting may not be necessary. Assessors should consider whether push or pull mechanisms are appropriate, and whether assent needs to be affirmative under applicable law or whether it can be deemed to occur upon certain conduct. Assessors may also want to check the track record of the PKI when making changes to its documents to ensure that the PKI is following the change procedures that it purports to follow.

Appropriate Requirements and Practices. The change process for PKI-related documents should be clearly stated, including the treatment of some or all of the bulleted topics listed above in the Relevant Considerations. Also, assessors should ensure that change procedures are administrable in view of the type of document. That is, the PKI must be able to administer the change process efficiently and effectively.

Cumbersome change procedures for simple documents are likely to be impractical. On the other hand, change procedures that do not provide sufficient mechanisms to gather input from among the key constituents of the PKI may not be acceptable to those constituents. In making this analysis, assessors should focus on whether the notification mechanism required by the change procedures is one of push or pull, whether assent to the amendments is affirmative or deemed to occur upon certain conduct, and whether the system of notice and assent is enforceable under local law. Where a document is or is part of a contract, PKIs will generally want to establish change procedures that are enforceable under applicable law.

Once a PKI has determined appropriate change procedures, it should reflect such procedures in its documentation. Finally, PKIs should follow their own documented procedures when making changes to PKI documents.

D.8.2 PUBLICATION AND NOTIFICATION POLICIES

Issue Summary. This section concerns the issues of to what extent and how a PKI participant publishes or notifies people of a particular PKI document it has written.

Relevant Considerations. Certain PKI documents, especially CPs and CPSs, contain a discussion of the extent to which they are publicly available and the methods by which they are distributed to their intended audience. The first issue, the extent of disclosure, arises because the details of some PKI documents may contain information that, if disclosed, would create security vulnerabilities or may disclose trade secret information of value to the document's author. For some PKIs, however, it is important that the relying party have assurances that the infrastructure of the PKI has been established and operates in a trustworthy manner. Even if the PKI does not disclose portions of a document to the public, the PKI may disclose these portions to an assessor, under appropriate non disclosure requirements, for review as part of an assessment. An assessment may be important as a showing of due diligence by the PKI, especially in the implementation of commercially reasonable security precautions for protection of its CA systems and supporting infrastructure.

The second issue concerns the means by which a document is published, to the extent that the PKI publishes it or notifies people of it. Publication may include mechanisms such as posting the document in one or more electronic forms for display or downloading on a web site. Publication and notification mechanisms may also include delivery of the document via e-mail, postal mail, fax, courier, or other delivery mechanisms, automatically, upon certain conditions, or upon request to the author or administrator submitted by one or more of the above mechanisms.

Assessors should determine whether there is a need to publish or notify constituents of the PKI and/or members of the public of a PKI document. They should also determine whether the document contains any security sensitive information or trade secret information. Assessors should also review the PKI document itself to determine the extent to which the document purports to be made available to constituents and/or members of the public. They may also wish to review the past publication practices of the PKI to determine if the PKI does in fact publish the document in accordance with the procedures listed in the document and whether the PKI maintains security sensitive and trade secret information as internal, unpublished information.

To the extent that the PKI purports to publish information, assessors should determine whether the means of publication are sufficient based on the needs of the PKI's participants and other constituents. Assessors should also determine if the means of publication are reflected in the document to be published. Finally, assessors should if possible determine whether or not the PKI is actually making the document available to those who have a right and a desire to obtain it, in accordance with the procedures set forth in the document. PKI providers would thus be well advised to maintain records of notice practices and compliance procedures.

Appropriate Requirements and Practices. The author of a PKI document should clearly state its publication and notification policies, including the nature of the PKI-related information that will be published and the types of information that will not be published because it is security sensitive or includes trade secrets. Assessors should ensure that these practices are appropriate in light of the sensitivity and nature of the information contained in the document, in order to prevent the inadvertent disclosure of sensitive information or trade secrets. They should also make sure that the publication practices of the PKI actually matches the procedures set forth in the documentation.

The author should also state which mechanisms it uses to publish a document or portion of a document that it is willing to publish. These procedures should be appropriately based on the needs of the PKI's constituents. For example, if people will likely need to obtain copies of the document while online, a PKI will want to make the document available on a web site and/or via e-mail. Finally, the PKI should actually make the document available in accordance with the procedures set forth in the document.

D.8.3 APPROVAL PROCEDURES FOR CPSS AND OTHER PRACTICE DOCUMENTS

Issue Summary. This section concerns the issue of how a policy-making authority approves a CPS or other practice document of a CA, RA, or other PKI participant that wishes to begin operations within, or begin interoperation with, a PKI. The approval process also encompasses how the policy-making authority determines whether or not the CPS or other document comports with the requirements stated in a CP or other document, when the policy-making authority's assent to the CPS or other practice document is a prerequisite for operations within, or interoperation with a PKI.

Relevant Considerations. The policy-making authority may want to examine and approve the CPS or other practice document of an entity before it agrees to permit that entity to operate within the PKI or to permit interoperations between the PKI and the entity. Such an approval process may be in the context of a CA cross-certifying or unilaterally certifying another CA. It may also occur before an RA begins operations within the PKI. In the case of CAs, the relevant document may be a CPS. By contrast, an RA may have a similar document containing a subset of CPS topics focusing on the functions performed by the RA. The examination and approval process of the policy-making authority may be a prerequisite to permitting the CA, RA, or other entity to begin operations or interoperation.

The main purpose of the examination and approval process is often to ensure that the entity's practices are consistent with the PKI's requirements. Those requirements often appear in a CP. The PKI may have adopted the CP in order to impose a uniform set of requirements on all participants within the PKI. The PKI's policy-making authority may want to ensure the new entity meets the PKI's requirements to prevent the new entity from diluting the trust established by the PKI.

This section may contain provisions relating to the mechanics of the approval process, such as the person to whom a document should be sent, the means by which the document should be provided, the people reviewing the document on behalf of the PKI, the timing of the approval process, and the methods by which the results of the examination are communicated. This section may also contain a discussion of the criteria against which the CPS or other document will be judged. The criteria often appear in a document, such as a CP, an industry standard, or a standard specified by an accrediting or licensing authority.

Assessors should determine whether a formal approval procedure for CPSs or other practice documents is important for a PKI in view of the level of assurances provided by the certificates issued within the PKI. If so, assessors should determine whether the PKI has assigned the appropriate kinds of persons to undertake the approval process and whether the process adequately ensures continued trustworthiness of the PKI. Assessors should also review the PKI's documentation to ensure that they set forth appropriate approval procedures for the PKI. Finally, assessors should determine whether or not a PKI does in fact follow the approval procedures set forth in its documentation.

Appropriate Requirements and Practices. The need for an approval process over CPSs or other practice documents will depend on the level of assurances provided by certificates within the PKI. Where a PKI is intended to provide lower assurance certificates, it may not be worth the effort to undertake a formal, time-consuming review process for documentation of new CAs, RAs, and other participants. The review process may be informal, less detailed, or even non-existent under such circumstances.

Where the PKI is intended to provide certificates with higher levels of assurance, however, a PKI will likely want to implement a formal approval process over CPSs and other practice documents of entities wishing to operate within or interoperate with the PKI. In fact, the PKI may want to make it clear that such approval is a precondition of beginning operations or interoperation. The approval process may be part of a more comprehensive assessment, such as an audit, but need not be.

The PKI should institute a set of approval procedures and mechanics appropriate to the PKI's business model to ensure that the PKI can accommodate new CAs, RAs, or other participants in an efficient fashion. The people evaluating the CPS or other document should be qualified to do so. The PKI should capture these practices in

clear documentation, which should also identify or describe in clear terms the criteria against which the document will be judged. A common pattern is one in which a policy-making authority judges a CPS to determine whether a CA's practices described in it are sufficient to meet the requirements of the PKI's CP. The PKI should document its approval procedures in a clear fashion and should actually follow the procedures set forth in its documentation when approving CPSs or other practice documents.

E. APPENDICES

Appendix 1 (APP 1): Glossary

APP 1.1 DEFINITIONS

This glossary provides definitions of terms used in this document. Critical terms are also defined in the summary glossary section of the introduction to assist the reader.

ACCESS

Opportunity to make use of an information system (IS) resource.[431]

ACCESS CONTROL

Limiting access to information system resources only to authorized users, programs, processes, or other systems. *Id*.

ACCOUNTABILITY

Process allowing auditing of IS activities to be traced to a source that may then be held responsible. *Id*.

ACCREDITATION

Procedure by which an authoritative body declares that an assessor has satisfied the designated criteria for assessing a PKI component.

Commentary

- Unless otherwise stated, the terms accredit and accreditation apply to the results of assessing an assessor/evaluator of a PKI component.
- *Cf., Accreditation Authority*: A PKI management entity with the authority to permit a subordinate PKI entity (such as a CA) to operate within a particular domain.[432]
- Note that the EU Signature Directive has adopted a very specific meaning for "voluntary accreditation."[433] However, regarding conformance to standards, "accreditation" means assessment and approval of assessors/evaluators.
- "Formal declaration by a Designated Approving Authority that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk."[434]

[431] *See* PAG APP 2 (*National Information Systems Security (INFOSEC) Glossary*, rev. 1, NSA, National Security Telecommunications And Information Systems Security Committee, No. 4009 (Jan. 1999) hereinafter "NSTISSI Glossary").

[432] See PAG APP 2 (Digital Signature and Confidentiality Certificate Policies for the Gov't of Canada Public Key Infrastructure, v. 3.02, Gov't of Canada (Apr. 1999), available at <http://www.cio-dpi.gc.ca/pki-cp/documents/Certificate_Policy/cp-pctb_e.asp> hereinafter "Canadian Confidentiality Policies").

[433] Voluntary accreditation "means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body". *See* EU Signature Directive, *supra* note 5, art. 2(13).

[434] *See also* NSTISSI Glossary, *supra* note 431.

ACCREDITING BODY

A recognized entity that accredits an assessor or evaluator as being qualified to perform assessments of CAs or other PKI components, applying designated criteria (such as standards derived from the certificate policies adopted by the policy-adopting body).

Commentary

- Examples of bodies who have or might perform such a role include NIST's National Voluntary Laboratory Accreditation Program (NVLAP), or the American Institute of Certified Public Accounts which accredits CPAs to audit various entities.

- *Cf.*, PKI Accreditation Body**.** An independent agent, member of an accounting body, or other qualified professional recognized by the PKI Accreditation Body. A PKI Accreditation Body is responsible for Evaluating the CA Operational Authority's compliance with the target CP, CPSs, RFC 2527, and other specific evaluation guidance, criteria and standards sanctioned by the PKI Accreditation Body Accreditation Body, to develop an "audit opinion" that there are adequate controls in place and these controls are operating effectively, such that reliance can be placed on transactions that are recorded, processed, executed, or maintained by the Operational Authority in question; Evaluating other evidence of compliance with the target CP where the parties have effected obligations through mechanisms such as contracts and membership agreements and through the implementation of related operational safeguards or business methods within the enterprise; and Producing a CP Compliance Evaluation Report.

- *Cf.*, Assessor Accreditation Body**.** An independent body, industry association or other agency that is recognized by the competent authority. Responsible for: approving and giving formal recognition that CA Evaluators are professionally competent to perform evaluations of CAs' compliance to Certificate Policies or other requirements that may be provided by the competent authority; and Sanctioning, selecting and/or developing CA evaluation guidance, criteria and standards.

ACTIVATION DATA

Data values, other than keys, that are required to operate cryptographic modules and that need to be protected e.g., a PIN, a pass-phrase, or a key share.

AFFECTED INDIVIDUAL

In the context of key recovery, a person whose private or commercial interest is affected by the use, misuse, or inability to access the information.

AGENCY

Agency is a relationship between two parties in which one party (agent) has the authority to act on behalf of another (principal), and any acts by an agent on behalf of the principal legally bind the principal.[435]

ANCILLARY SERVICES

Services other than certificate lifecycle services, performed in support of digital signatures and other uses of certificates, and in support of other related areas of secure electronic commerce.

APPROVE

Procedure by which an assessor/evaluator declares that a certification authority or other PKI component has satisfied designated criteria.

[435] *See* PAG § C.2 (Agency Prinicples) (detailed discussion on agency).

Commentary

- The results of an approval may include: (a) the right to provide certification services within a designated community, (b) to obtain favorable status under application rules, (c) to interoperate or otherwise obtain recognition of the certificates that it issues and manages, (d) denoting a particular level of competence or trustworthiness, and (e) permitting the operation in a particular mode using a particular set of safeguards.

- This definition has conceptual similarities and has created confusion with the terms *certification*, *certified*, and *licensed*. In practice, these terms are frequently used interchangeably yet inconsistently. *Note*: there is little consensus and indeed a remarkable divergence in their use.

ARCHIVAL RECORD

The key elements (e.g., data, metadata, and security tokens) that comprise the information pertaining to a business event such as enrollment, use, maintenance, and destruction of certificates. These elements typically need to be preserved for legal, regulatory, dispute resolution, auditing, investigation of potential security breaches, other operational, or historical purposes.[436]

ASSESSMENT

A procedure for determining whether an assessor, or a certification authority (or another PKI component) meets defined criteria.

Commentary

- An assessment may take various forms, including but not limited to informal review, formal audits, and rigorous technical and procedural review and will normally result in an assessment report.

ASSESSMENT REPORT

The result of an assessment of the specified security features of a PKI component.

ASSESSOR

One who undertakes an assessment of a certification authority (or another PKI component).

ASSURANCE

Grounds for confidence that an entity meets specified security requirements.

ASSURANCE LEVEL

A particular point on a relative scale of assurance.

ASYMMETRIC CRYPTOSYSTEM

A system using two different but mathematically related keys, one for creating a digital signature or decrypting data, and another key for verifying a digital signature or encrypting data. Computer equipment and software utilizing such key pairs are often collectively termed an "asymmetric cryptosystem." For at least one key of the key pair, it should be computationally infeasible to calculate the complementary key of that pair.

ATTRIBUTION

In a legal context, the determination that a message or record was originated by a particular party. *See* authentication**.**

[436] In the U.S., X9 and ASTM are "doing stuff" and in the EU, ETSI is working on TS 101 733 EU; also, IETF is publishing the ETSI specification as an Informational document.

AUDIT

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.[437]

AUTHENTICATION

The process of confirming an identity claimed by or for an entity. An authentication process is the second of two steps comprising: the *identification step* – presenting an identifier to the security system and the *authentication step* – presenting or generating authentication information that corroborates the binding between the entity and the identifier. *Cf*., Identification.

AUTHORIZED ASSESSOR

In the context of key recovery, an entity that accesses information when authorized by either criminal or civil justice systems.

AVAILABILITY

Timely, reliable access to data and information services for authorized users.[438]

BINDING

Process of associating two related elements of information. For example, a certificate binds its subject to a particular public key. *Id.*

BIOMETRICS

Automated methods of authenticating or verifying an individual based upon a physical or behaviorial characteristic. *Id*.

BURDEN OF PROOF

A legal evidentiary principle of evidence that loosely refers to the obligation that proof of a fact that falls on the party who is the proponent of that fact. There are two separate components. First is the *production burden,* or the obligation to come forward with some evidence in support of a claim in order to avoid dismissal of that claim. Second is the *risk of non-persuasion,* the obligation to convince the finder of fact (jury or judge) of the fact, by the applicable standard of proof, e.g., preponderance of the evidence, clear and convincing evidence, or proof beyond a reasonable doubt.

CA CERTIFICATE

A certificate issued by one CA to another CA. CA certificates are issued within a PKI and, to facilitate interoperation, where a new CA is included within a PKI via unilateral or cross-certification.

Commentary

- **Alt:** A data record in digital form containing the public digital signature verification key, belonging to a certification authority (CA), that has been signed by the private signing key of another (certifying) CA.

CA DOMAIN

A CA domain consists of as CA and its subjects. Sometimes referred to as a PKI domain.

[437] *See* NSTISSI Glossary, *supra* note 431.

[438] *See* NSTISSI Glossary, *supra* note 431.

CA SYSTEM

The collection of the information technology components (including one or more trustworthy systems), along with the procedures and operations of the CA System, as specified in the CPS.

CERTIFICATE, PUBLIC KEY CERTIFICATE

1. A Public Key Certificate is a message that at least:

- identifies the certification authority issuing it,
- names or identifies its subscriber,
- contains the subscriber's public key,
- identifies its operational period, and
- is digitally signed by the certification authority issuing it.

2. A data record in digital form that at a minimum names the subscriber that is the subject of that certificate, contains the public key of that subscriber that corresponds to the subscriber's private key, names the CA issuing the certificate, is digitally signed by the private key of the issuing CA, contains a serial number unique to that certificate, and specifies the certificate's operational period.

CERTIFICATE MANAGEMENT AUTHORITY

A PKI component that performs back-end functions on behalf of a CA, consisting of processes whereby certificates are generated, stored, protected, transferred, loaded, used and destroyed.[439]

CERTIFICATE POLICY CP

A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

Commentary

- For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of parties engaging in transactions for goods and services within a given price range. Each digital certificate contains an identifier for the particular certificate policy(s) applying to that certificate, and each such identifier is a reference to a particular certificate policy definition. This method of including object identifiers in the certificate is the system by which relying parties relying on the certificate will be able to determine which particular certificate policy definitions apply to and govern the technical and legal rules for use of the certificate. Relying parties who wish to use object identifiers will need to program their relying party software systems to look for the desired object identifier and permit certain conduct.

CERTIFICATE REVOCATION LIST CRL

A list of revoked certificates, which is digitally signed and made available by the CA to relying parties. *Cf.* Online Certificate Status Protocol (OCSP).

CERTIFICATION/CERTIFY

See Approve.

[439] *See* NSTISSI Glossary, *supra* note 431.

CERTIFICATION AUTHORITY (CA)[440]

- A person who issues a certificate.
- An entity responsible for registering and issuing, revoking and generally managing certificates.
- An authority trusted by one or more users to create and issue certificates.
- An authority trusted by one or more users to create and assign certificates. Optionally, the CA may generate end-user subscribers' keys.

CERTIFICATION AUTHORITY CERTIFICATE

A certificate that lists a certification authority as subscriber and contains a public key corresponding to a private key used by the subject certification authority to digitally sign certificates and certificate status information.

CERTIFICATION AUTHORITY SOFTWARE

The cryptographic software required to manage the keys of End-Entities.

CERTIFICATION PATH

An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain via a chaining of signature key bindings.

CERTIFICATION PRACTICE STATEMENT (CPS)

A statement of the practices that a certification authority employs in issuing certificates.

Commentary

- The CPS can be used to disclose the systems, policies and procedures the CA uses to satisfy the requirements specified in the certificate policies that are supported by it.

CIVIL LAW REGIME

The legal tradition of jurisdictions that base fundamental legal principles primarily upon statutory codes such as the Code Napoléon.

CLICKWRAP CONSENT

In a legal context, the technique of giving approval or consent to an agreement presented online with opportunity to review it, by a mouseclick on a button stating "I Agree" or words to that effect.

COMMON LAW REGIME

The legal tradition of Anglo-American jurisdictions that accumulates legal principles primarily in reaction to actual cases that are used as precedent in future cases, supplemented by statutes.

COMPETENT AUTHORITY

An agent responsible, within the legal jurisdiction, for:

- Issuing licenses, setting minimum CP requirements and giving formal recognition to standards, authorization, regulations or other government or legal recognition to open community CAs as managed by the respective CA Policy Authorities and Operational Authorities.

[440] A CA is sometimes referred to as a "Certificate Authority," which is considered equivalent to the usage recommended here.

COMPROMISE

Disclosure of information to unauthorized persons or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.[441]

COMPUTER SECURITY

Measures and controls that ensure confidentiality, integrity, and availability of IS assets including hardware, software, firmware, and information being processed, stored, and communicated. *Id.*

CONFIDENTIALITY

Assurance that information is not disclosed to unauthorized persons, processes, or devices. *Id.*

CONFIRM

To ascertain through appropriate inquiry and investigation.

CONTRACT

A promise or set or promises for the breach of which the law gives a remedy, or the performance of which the law recognizes as a duty.

CORRESPOND

To belong to the same key pair.

COVENANT

One type of contractual responsibility, being a promise to perform certain tasks (affirmative covenant) or to refrain from certain conduct (negative covenant), to be distinguished from a representation and a warranty.

CRITICAL INFRASTRUCTURES

Physical and cyber-based systems that are essential to the minimum operations of the economy and government.[442]

CROSS-CERTIFICATION / CROSS CERTIFICATE

Before a user can verify a digital signature generated by a subscriber of another CA he must obtain the verification public key of the generating CA. To prevent various masquerade attacks this public key must be provided to the user in a manner that will assure its integrity. This is accomplished by having the user's CA and the signer's CA cross-certify whereby each CA provides the other with a verification certificate – called a cross-certificate – containing the other CA's public verification key. The user is then able to verify the integrity of the cross-certificate generated by its own CA for the other and, with the public key it contains, verify the integrity of the signer's certificate.

DATA INTEGRITY

Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.[443]

DATA SECURITY

Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. *Id.*

[441] *See* NSTISSI Glossary, *supra* note 431.

[442] *See* NSTISSI Glossary, *supra* note 431.

[443] *See* NSTISSI Glossary, *supra* note 431.

DIGITAL SIGNATURE

A transformation of a message using an asymmetric crypto-system and a hash function such that a person having the initial message and the signer's public key can accurately determine (1) whether the transformation was created using the private key that corresponds to the signer's public key, and (2) whether the initial message has been altered since the transformation was made.

- "A cryptographic process used to assure message originator authenticity, integrity, and nonrepudiation."[444]

- *Cf.,* electronic signature**,** *infra.*

Commentary

- If there is an intention to sign, a digital signature falls within the definition of *electronic signature* within the meaning of E-SIGN.

- The U.S. Food and Drug Administration expressly recognizes a **digital signature** as a type of **electronic** signature:

  Digital signature means an **electronic signature** based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.[445]

  Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.[446]

DIGITAL SIGNATURE KEY PAIR

A pair of asymmetric keys composed of a private signing key and a corresponding public digital signature verification key.

DIRECTORY

A directory system that conforms to the ITU-T X.500 series of Recommendations.[447]

DISTINGUISHED NAME (DN)

An unambiguous name given to an entry within a directory conforming to the ITU-T X.500 series of Recommendations. The distinguished name of a given object is defined as that name which consists of the sequence of the RDNs of the entry which represents the object and those of all of its superior entries (in descending order). Because of the one-to-one correspondence between objects and object entries, the distinguished name of an object is the distinguished name of the object entry. *Id.*

- *Cf.* relative distinguished name **(**RDN**):** A set of one or more attribute type and value pairs, each of which matches a distinct distinguished attribute value of the entry. *Id*., § 9.1.8.

- Globally unique identifier representing an individual's identity.[448]

[444] *See* NSTISSI Glossary, *supra* note 431.

[445] *See* PAG APP 2 (U.S. Food and Drug Administration *Electronic Records*, 21 C.F.R. 11, Subpart C, 62 Fed. Reg. 13,464 (20 Mar. 1997) § 11.3(a)(5) hereinafter "FDA Glossary").

[446] *Id.*, § 11.3(a)(7).

[447] *See* PAG APP 2 (*Information Technology - Open Systems Interconnection: The Directory: Authentication Framework*, ISO/IEC 9594-8/ITU-T Recommendation X.5, (1998) § 9.7, hereinafter "ISO X.5 Recommendation").

DomainUnique context in which a program is operating; in effect, the set of objects a subject has the privilege to access. *Id*.

ELECTRONIC RECORD

The term 'electronic record' means a contract or other record created, generated, sent, communicated, received, or stored by electronic means.[449] *See* Record.

ELECTRONIC SIGNATURE

- 'Electronic signature' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.[450]

- Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.[451]

- 'Electronic signature' means data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message.[452]

- Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.[453]

ENCRYPTION KEY PAIR

A pair of asymmetric keys composed of a public encryption key and a corresponding private decryption key.

END-ENTITY

An Entity that uses the keys and certificates created within the PKI for purposes other than the management of the aforementioned keys and certificates. An End-Entity may be a Subscriber, a Relying Party, a device, or an application.

ENTITY

Any autonomous element within a public key infrastructure. An entity is not necessarily an individual, but may be a computer or a particular application. For example, a CA, an RA, a subscriber, a relying party, a Web server application are all entities.

ESTOPPEL

Following misrepresentations by one party that have induced detrimental reliance by the other party, a legal theory that rejects a subsequent attempt by the first party to deny those misrepresentations.

[448] *See* NSTISSI Glossary, *supra* note 431.

[449] *See* E-SIGN, *supra* note 73, § 106(4).

[450] *Id*., § 106(5).

[451] *See* EU Signature Directive, *supra* note 5.

[452] *See* PAG APP (*Draft Uniform Rules on Electronic Signatures*, UNCITRAL, 33rd Sess., U.N. Doc. A/CN.9/WG.IV/WP.82 (29 Jun. 1999) art. 2(a), *available at* <http://www.uncitral.org/en-index.htm>, hereinafter "U.N. Draft Rules").

[453] *See* FDA Glossary, *supra* note 445, § 11.3(a)(7).

EVALUATION

In the context of a PKI, an evaluation is generally a analysis of a CA or its components (such as an RA, repository, or cryptomodule) in relation to specified criteria. The target of an evaluation may be either a product or a service. *Note*: Given the complexity of PKIs, it is generally thought that a comprehensive evaluation is neither cost effective nor necessarily feasible.

EVALUATOR

The Evaluator is an entity that actually evaluates a CA or its components.

HACKER

Unauthorized user who attempts to or gains access to an IS.[454]

HASH FUNCTION

An algorithm mapping or translating one sequence of bits into another, generally smaller set (the hash result), such that (1) a message yields the same hash result every time the algorithm is executed using the same message as input, (2) it is computationally infeasible that a message can be derived or reconstituted from the hash result produced by the algorithm, and (3) it is computationally infeasible that two different messages can be found that produce the same hash result using the same algorithm.[455]

HASH RESULT

The output produced by a hash function upon processing a message.[456]

- "Hash Total" is the value computed on data to detect error or manipulation.[457] *See* Checksum.

HOLD A PRIVATE KEY

To use or be able to use a private key.

IN ALL MATERIAL RESPECTS

In the context of the Evaluator's report, the attestation that requirements are satisfied "in all material respects" is based upon a determination that there are no facts or circumstances known or should have been known by the evaluator that would cause a user of the evaluator's report to come to a different conclusion then that described in the evaluator's report. In addition, the use of the term "material" recognizes that there may be a negative observations that do not significantly impact the Balanced Approach to Security and the overall achievement of the CP or other criteria.

INCORPORATE BY REFERENCE

To make one message a part of another message by (1) identifying the message to be incorporated, (2) providing information that enables the receiving party to access and obtain the incorporated message in its entirety, and (3) expressing the intention that it be part of the incorporating message. The incorporated message shall have the same effect as if it had been fully stated in the incorporating message, to the extent permitted by law.

IDENTIFICATION

Identification is the first of two steps comprising "I&A": the *identification step* – presenting an identifier to the security system. The second step is the *authentication step* – presenting or generating authentication information that corroborates the binding between the entity and the identifier. *Cf.*, Authentication.

[454] *See* NSTISSI Glossary, *supra* note 431.

[455] *See* DSG, *supra* note 2, § 1.12.

[456] *Id.*, § 1.14.

[457] *See* NSTISSI Glossary, *supra* note 431.

INDEMNIFICATION

A legal remedy under which the damaged party is compensated completely and held harmless against any or all damages or expenses caused by a breach of contractual or other responsibility.

INFORMATION CUSTODIAN

In the context of private key recovery, the Information Custodian is the person or organization with legal ownership of the information.

INFORMATION OWNER

In the context of private key recovery, the Information Owner is the person or organization with legal ownership of the information.

INFORMATION SYSTEM (IS)

The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.[458]

INSPECTION

An assessment performed on a regular basis to ensure ongoing compliance with a CP (or other applicable requirement or documents). A formal inspection is normally referred to as an audit.

ISSUE A CERTIFICATE

The acts of a certification authority in creating a certificate and notifying the subscriber listed in the certificate of the contents of the certificate.

ISSUING CA

In the context of a particular certificate, the issuing CA is the CA that issued the certificate.

KEY PAIR

In an asymmetric cryptosystem, a private key and its mathematically related public key, having the property that the public key can verify a digital signature that the private key creates, or in the case of data encryption, keys having the property that the private key can decrypt data encrypted with the public key. For encryption, the public key is used to encrypt; the corresponding private key to decrypt. A signature is generated with the private key and verified with the corresponding public key.

KEY RECOVERY AGENT

In the context of private key recovery, the Key Recovery Agent is the entity that performs the key recovery function as a function of agreement or contract, or on another stakeholder's information as a byproduct of a primary agreement or contract.

LIABILITY

The legal consequence of having breached responsibilities (contractual, tort or other) and having caused damage to another.

LIABILITY-LIMITATION PROVISIONS

Contractual provisions that purport to limit liability, consisting of disclaimers of liability, provisions limiting certain elements of damages, and provisions limiting the amount of damages recoverable.

[458] *See* NSTISSI Glossary, *supra* note 431.

LICENSE

See Accreditation.

MESSAGE

A digital representation of information.[459]

MESSAGE INTEGRITY

The assurance of unaltered transmission of a message from the sender to the intended recipient.

N* OUT OF *M

"N out of M" describes a multi-person control technique. An example would be the case in which multiple persons each have only a portion of the data necessary to activate the private key that enables operation of the system. Thus *if* N is 3, then 3 individuals would be required to be present to activate the system (e.g., enable the CA to sign certificates or CRLs). To ensure that the unavailability of one or more of the individuals does not prevent the operation of the system, it is possible to distribute portions of material to more than 3 individuals (for example, 5 people) and have the system operable when any 3 of the 5 people are available.

NONREPUDIATION

Strong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents.[460]

In a legal context, sufficient evidence to persuade the ultimate authority (judge, jury or arbiter) as to such origin, submission, delivery, and integrity, despite an attempted denial by the purported sender.

Contrast the above legal definition with the following technical definition: "Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data."[461]

NOTARIAL SERVICE

Notarial services are undertaken by notaries. There are two different major types of notaries: common law notaries and Latin notaries. *Common law notaries* are found mostly in the English speaking world; i.e., America and the UK. Latin notaries are predominately found in the rest of the world. We expand on these definitions and the differences between the two because each provides a different service to the requestor. *Latin notaries* are responsible for the correctness of the notarized data; they may also act as an archivist of the document. Common law notaries authenticate the execution of the document but do not authenticate the accuracy of the data in the notarized document.

NOTIFY

To communicate or make available information to another person as required under the circumstances.

OBJECT IDENTIFIER (OID)

The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. They are used to uniquely identify a policy, which policy is subject to change, despite the constancy of the identifier.

[459] *See* DSG, *supra* note 2.

[460] *Id.*, § 1.21.

[461] *See* NSTISSI Glossary, *supra* note 431.

ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)

A specification for online and real-time inquiries concerning the status of a particular certificate and for online and real-time responses to such inquiries communicating the status of that certificate. An alternative to a CRL . The OCSP protocol, RFC 2560, enables online validation of the reliability of a digital certificate. RFC 2560 defines a mandatory-to-implement mechanism supporting the revocation status of the certificate and defines an optional extension mechanism to support a richer set of semantics (e.g., full path validation by the OCSP server).[462]

- *Cf.*, Certificate Revocation List (CRL)

OPERATIONAL AUTHORITY

Personnel who are responsible for the overall operation of a CA. Their responsibility may cover areas such as staffing, finances, dispute resolution, and policy decisions.

Commentary

The Operational Authority is responsible to the Policy Authority for: (a) interpreting the certificate policies selected or defined by the Policy Authority; (b) developing a Certification Practice Statement (CPS), to document the CA's compliance with the Certificate Policies and other requirements; (c) maintaining the CPS to ensure that it is updated as required; and (d) operating the CA in accordance with the CPS.[463]

OPERATIONAL PERIOD OF A CERTIFICATE

The operational period of a certificate begins on the date and time it is issued by a certification authority (or on a later date and time certain if stated in the certificate), and ends on the date and time it expires or is earlier revoked or suspended.

ORANGE BOOK

Trusted Computer System Evaluation Criteria (TCSEC).

PERSON

A human being or an organization (or a device under the control thereof that is capable of signing a message or verifying a digital signature).

PKI DOMAIN

A PKI Domain consists of a CA and its subjects. Sometimes referred to as a CA Domain.

PKIX

The Public Key Infrastructure X.509 Working Group of the Internet Engineering Task Force.[464]

POLICY AUTHORITY

An agent of the CA domain or enterprise that may perform one or more of the following functions: (a) selecting and/or defining certificate policies for use in a PKI; (b) approving any cross-certification or interoperability agreements with external CA Domains; (c) approving practices that a CA must follow by reviewing the CPS to ensure consistency with the Certificate Policies; and (d) providing policy direction to the Operational Authority.

[462] *See* RFC 2560, *supra* note 348.

[463] See PAG APP 2 (Certification and Accreditation for PKIs and Certification Authorities – Survey of Standards, Trends and Identification of Potential Models, v. 2.0, William Dziadyk, Report to Industry Canada (7 Aug. 1998), available at <http://www.lgs.com/Services/adobe/m2svy_21.pdf>, hereinafter "Canadian Certification Survey").

[464] *Available at* <http://www.ietf.org/ids.by.wg/pkix.html>.

POLICY MANAGEMENT AUTHORITY

A body responsible for setting, implementing, and administering policy decisions regarding CPs and CPSs throughout the PKI.

POLICY QUALIFIER

Field within the certificate policies extension of an X.509 certificate that conveys policy information in addition to the identification of the applicable CP.

POLICY-ADOPTING BODY

An entity that adopts certificate policies for a particular class of certificates applicable to a particular community.

PRESUMPTION

In a legal context, an evidentiary rule that eases the burden of proof as to a particular fact, usually so that the proponent of the fact is relieved of the burden of coming forward with evidence in support of such fact. Presumptions are usually rebuttable, so that the presumption may be overcome by introduction of sufficient contrary evidence of the fact by the opposing party. For example, the Utah Digital Signature Law[465] sets forth a presumption that a digital signature verified by a certificate issued by a licensed CA is attributed to the subscriber named as subject in the certificate. One method of rebutting this presumption might be to introduce evidence that the applicant for the certificate was an imposter who fraudulently convinced the CA to issue the certificate to the imposter in the name of the subscriber.

PRIVACY

The legal right of an entity (particularly a person, and even more so when the person is a consumer) to be free from intentional or unintentional disclosure of his or her identifiable personal information without consent. *Cf.*, confidentiality**,** which is the assurance that the system has the capability to resist disclosure and therefore protect privacy.

PRIVATE DECRYPTION KEY

See Encryption key pair.

PRIVATE KEY

The key of a key pair used to create a digital signature or to decrypt data.[466] Also, the key of an asymmetric key pair that is kept secret. *Cf.*, public key.

PRIVATE SIGNING KEY

See Digital signature key pair.

PROTECTION PROFILE (PP)

A statement conforming to the CC that clearly expresses a particular community's security needs, together with a derived set of implementation-independent security measures that have been shown to meet those needs.[467]

PUBLIC DIGITAL SIGNATURE VERIFICATION KEY

See Digital signature key pair.

[465] *See* Utah Signature Act, *supra* note 80.

[466] *See* DSG, *supra* note 2.

[467] *See* PAG APP 2 (*Common Criteria for Information Technology Security Evaluation*, ISO 15408, hereinafter "ISO Common Criteria").

PUBLIC ENCRYPTION KEY

See Encryption key pair.

PUBLIC KEY

The key of an asymmetric key pair that is typically made available to the "public." Also, the key of a key pair used to verify a digital signature or to encrypt.

PUBLIC KEY CRYPTOGRAPHY (PKC)

Encryption system using a mathematically linked pair of keys. What one key encrypts, the other key decrypts.[468]

PUBLIC KEY INFRASTRUCTURE (PKI)

The sum total of the hardware, software, people, processes, and policies that, together, using the technology of asymmetric cryptography, facilitate the creation of a verifiable association between a public key (the public component of an asymmetric key pair) and the identity (and/or other attributes) of the holder of the corresponding private key (the private component of that pair), for uses such as authenticating the identity of a specific entity, ensuring the integrity of information, providing support for nonrepudiation, and establishing an encrypted communications section.

PUBLISH

To record or file in one or more repositories.

RECORD

The term 'record' means Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.[469]

Commentary

- *Cf.*, Federal Record. Records include all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them.[470]

- Electronic record means any information that is recorded in a form that only a computer can process and that satisfies the definition of Federal record in 44 U.S.C. § 3301.[471]

- Electronic records include numeric, graphic, and text information, which may be recorded on any medium capable of being read by a computer and which satisfies the definition of a record. This includes, but is not limited to, magnetic media, such as tapes and disks, and optical disks. Unless otherwise noted, these requirements apply to all electronic records systems, whether on

[468] *See* NSTISSI Glossary, *supra* note 431.

[469] *See* E-SIGN, *supra* note 73, § 106(9).

[470] *See* PAG APP 2 (*Definition of Records--Electronic Communications*, 44 U.S.C. § 3301.3 (1991), hereinafter "U.S.C. Definitions").

[471] *Id.*

microcomputers, minicomputers, or main-frame computers, regardless of storage media, in network or stand-alone configurations. . . .[472]

- Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.[473]

REGISTRATION AUTHORITY (RA)

An entity that is responsible for validating the identity (or other attributes) of certificate applicants but does not issue or manage certificates (i.e., an RA is delegated to perform certain tasks on behalf of a CA, such as approving certificate applications). The extent to which an RA is [exclusively] responsible for its acts depends on the applicable CP and agreements.[474]

RELYING PARTY AGREEMENT

An agreement between a certification authority and relying party that typically establishes the rights and obligations between those parties regarding the verification of digital signatures or other uses of certificates.

RELYING PARTY

The recipient of a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them or person who otherwise relies on the binding in a certificate between the public key appearing in it and the identity (and/or other attributes) of the person named in the certificate.

Commentary

- The terms "*certificate user*" and "*relying party*" are often used interchangeably in this document.
- A relying party with respect to a particular certificate issued by a CA may or may not be a subscriber of another certificate issued by that CA.

REMEDY

In the legal context, one of several methods by which a party can redress wrongs and reimburse damage caused by a breach of responsibilities. Examples of remedies include the payment of money damages, and specific enforcement by an affirmative or negative injunction.

REPOSITORY

A trustworthy system for storing and retrieving certificates or other information relevant to certificates.

REPRESENTATION

One category of a party's contractual responsibilities, being a promise that a fact is true at the present time and/or was true as of an earlier time, to be distinguished from a warranty and a covenant, but sometimes also loosely used to also refer to the truth of a fact at a time in the future.

RESPONSIBILITIES

Contractual provisions (representations, warranties and covenants), or a duty to meet a behavior standard imposed by tort or some other source of law.

---

[472] *See* PAG APP 2 (*Records Management--Electronic Records Management*, 36 C.F.R. pt. 1234.2 (1995), hereinafter "C.F.R. Definitions").

[473] *See* FDA Glossary, *supra* note 445.

[474] The term Local Registration Authority (LRA) is used elsewhere to describe the same concept.

REVOKE A CERTIFICATE

To permanently end the operational period of a certificate from a specified time forward.

RISK MANAGEMENT

Process concerned with the identification, measurement, control, and minimization of security risks in information systems to a level commensurate with the value of the assets protected.[475]

ROOT CA

The endpoint in a chain of trust.

SECURITY CRITERIA

A commonly agreed source for evaluating security properties of IT products and systems or entities. Examples are the European Union's Information Technology Security Evaluation Criteria (ITSEC) and the international Common Criteria for Information Technology Security Evaluation (equivalent to ISO standard 15408).

SECURITY TARGET

A Common Criteria-based construct defining the structure and content for an implementation-specific set of security requirements for an IT product or system.[476]

SIGNER

Entity identified as subject in the certificate whose public key verifies a digital signature for a message or a record.

SPONSOR

A Sponsor is the person that has authorized the issuance of a certificate to a specific individual or organization. For example, an employee's manager may be the Sponsor of a certificate to be issued to the employee. In the case of a certificate for a citizen or a commercial enterprise, the Sponsor could be the manager of the business unit that has a requirement to communicate with that Entity. The Sponsor might suggest an appropriate DN for the certificate and will be responsible for either supplying or confirming the certificate attribute details to the RA. The Sponsor may also be responsible for informing the CA or RA if the business unit's relationship with the Subscriber is terminated or has changed such that the certificate should be revoked or updated.

SUBJECT CA

In the context of a particular CA certificate, the subject CA is the CA whose public key is certified in the certificate. *See* Issuing CA.

SUBJECT OF A CERTIFICATE

The person, process, or device named in a certificate as the subscriber.

SUBSCRIBER

A person who (1) is the subject named or identified in a certificate issued to such person, and (2) holds a private key that corresponds to a public key listed in that certificate.[477]

Commentary

A subscriber is sometimes defined as:

[475] *See* NSTISSI Glossary, *supra* note 431.

[476] *See* ISO Common Criteria, *supra* note 467.

[477] *See* DSG, *supra* note 2.

- An entity whose public key is certified in a public key certificate,
- A member of the CA domain, or
- A party who is the subject of a certificate and who is capable of using, and is authorized to use, the private key, that corresponds to the public key in the certificate.

Subscribers may have one or more certificates from a specific CA associated with them. In some cases, a subscriber may have one certificate containing their digital signature verification key, and the other containing their confidentiality encryption key.

SUBSCRIBER AGREEMENT

An agreement between a subscriber and either a CA, RA, or both that establishes the right and obligations of the parties regarding the issuance and management of certificates.

SUSPEND A CERTIFICATE

To temporarily suspend the operational period of a certificate for a specified time period.

THIRD PARTY BENEFICIARY

An entity claiming a right or benefit arising from a contract between other parties, in a case where the entity is not a party to the contract.

TIME STAMP

To create a notation that indicates, at least, the correct date and time of an action, and the identity of the person that created the notation; or such a notation appended, attached or referenced.

TIME-STAMPING SERVICE

A time-stamping service provides a strong and verifiable cryptographic statement that a specific digital record existed at a specific moment in time.

TARGET OF EVALUATION

The Common Criteria term for the information technology product or system (including its guidance documentation) for which security requirements are being specified in a Protection Profile (PP) or Security Target (ST).[478]

TORT

A civil wrong for which a remedy may be obtained, usually but not always in the form of damages.

TRANSACTIONAL CERTIFICATE

A certificate for a specific transaction incorporating by reference one or more digital signatures.

TRUSTWORTHY SYSTEM

Computer hardware, software, and procedures that:

- are reasonably secure from intrusion and misuse;
- provide a reasonably reliable level of availability, reliability, and correct operation;
- are reasonably suited to performing their intended functions; and

[478] *See* ISO Common Criteria, *supra* note 467.

- adhere to generally accepted security principles.

VALID CERTIFICATE

A certificate that (a) a certification authority has issued, and (b) has been accepted by the subscriber listed in it; or

- A transactional certificate that (a) a certification authority has issued, and (b) has been accepted by the subscriber listed in it, but limited to the digital signatures created pursuant to the specific transaction to which the transactional certificate relates.

VERIFY A DIGITAL SIGNATURE AND MESSAGE INTEGRITY

In relation to a given digital signature, message, and public key, to determine accurately:

- that the digital signature was created during the operational period of a valid certificate by the private key corresponding to the public key listed in the certificate; and
- the message has not been altered since its digital signature was created.

APP 1.2 ACRONYMS

ABA	American Bar Association
ACES	Access Certificates of Electronic Services
ACM	Association for Computing Machinery
AICPA	American Institute of Certified Public Accountants
ANSI	American National Standards Institute
ARL	Authority Revocation List
CA	Certification Authority
CA Trust	AICPA/CICS *WebTrust*$^{tm/sm}$ *Program for Certification Authorities*
CBK	Common Body of Knowledge
CC	Common Criteria for Information Technology Security Evaluation
CCF	Canadian Central Facility
CIA	Certified Internal Auditor (IIA)
CICA	Canadian Institute of Chartered Accountants
CISA	Certified Information Systems Auditor (ISACA)
CISSP	Certified Information Systems Security Professionals
CobIT	Control Objectives for Information and Related Technology (ISACA)
CP	Certificate Policy
CPA	Certified Public Accountant
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSE	Communications Security Establishment
DAP	Directory Access Protocol
DES	Data Encryption Standard
DN	Distinguished Name
DNS	Domain Name Services/Server
DSA/DSS	Digital Signature Algorithm / Digital Signature Standard
DSG	The ABA-ISC Digital Signature Guidelines
DSS	Digital Signature Standard
ECDSA	Elliptic Curve Digital Signature Algorithm
EDI	Electronic Data Interchange
ERC	Enhanced Reliability Check
FIPS	(US) Federal Information Processing Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
HTTP	Hypertext Transfer Protocol
ICSA	International Computer Security Association
IEC	International Electrotechnical Commission
IIA	Institute of Internal Auditors
ISACA	Information Systems Audit and Control Association
ISBN	International Standard Book Number
ISC	Information Security Committee of the ABA
ISO	International Organization for Standardization
I&A	Identification and Authentication
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSEC	IP Security
ISC	ABA's Information Security Committee
ITSEC	Information Technology Security
ITU	International Telecommunications Union
KDC	Key Distribution Center
KEA	Key Encryption Algorithm
KRA	Key Recovery Alliance

LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority – see also RA
NCSA	(U.S.) National Computer Security Association – see also ICSA
NIST	(U.S.) National Institute of Standards and Technology
NVLAP	(U.S.) National Voluntary Laboratory Accreditation Program
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
OS	Operating System (e.g., Windows 95/98/NT, Unix, etc.)
OSHA	Occupational Safety and Health Administration
PII	Personally Identifiable Information
PIN	Personal Identification Number
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PKCS	Public Key Cryptosystem
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority
PMO	Program Management Office
PP	Protection Profile
RA	Registration Authority
RFC	(IETF) Request For Comments
RSA	Rivest-Shimar-Adleman Algorithm
SEI-CMM	Software Engineering Institute's Capability Maturity Model
SEP	Secure Exchange Protocol
SHA-1	Secure Hash Algorithm
S-HTTP	Secure Hypertext Transfer Protocol
S/MIME	Secure Multi-part Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SSA	Serial Storage Architecture
SSL	Secure Sockets Layer
ST	Security Target
TCSEC	Trusted Computer System Evaluation Criteria, or Orange Book
TOE	Target of Evaluation
TRA	Threat and Risk Assessment
TSDM	Trusted Software Development Methodology
TTP	Trusted Third Party
UK	United Kingdom
UPS	Uninterruptable Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
US	United States of America
VA	Veteran's Administration (U.S.)

Appendix 2 (APP 2): Bibliography

SHORT TITLE	BIBLIOGRAPHY
	179 QUEBEC CIVIL CODE
	Department of Defense Interim External CA project;
1998 FTC Report	Privacy Online: A Report to Congress, FTC (1998), available at

SHORT TITLE	BIBLIOGRAPHY
	<http://www.ftc.gov/reports/privacy3/index.htm>.
2000 FTC Report	Privacy Online: Fair Information Practices in the Electronic Marketplace, FTC Report to Congress (May 2000), available at <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>.
3rd Party Guidelines	Guidelines for the Use and Management of Trusted Third Parties, ISO/IEC JTC 1/SC 27 PDTR 14516 (27 May 1997).
ABA Formal Op.	Attorney Ethics of Unencrypted E-mail, ABA Formal Opinion No. 99-413 (1999), available at <http://www.abanet.org/cpr/fo99-413.html>.
ACES	Access Certificates of Electronic Services (ACES), Draft, U.S. Gov't Services Administration (Mar. 1998), available at <http://hydra.gsa.gov/aces>.
ACSI 33	Security Guidelines for Australian Government IT Systems, § 2, Annex B, Australian Communications Security Instruction No. 33 (ACSI 33) (2000), available at <http://www.dsd.gov.au/infosec/acsi33/acsi_index.html>.
AICPA Standards	Statement of Auditing Standards, 70 AICPA (2000), available at <http://www.aicpa.org/>.
AICPA/CICA WebTrust	WebTrust Program for Certification Authorities, v. 1, AICPA/CICA (25 Aug. 2000), available at <http://ftp.webtrust.org/webtrust_public/certauth_fin.doc>.
ANSI Objectives	Certificate Management Objectives, ANSI Draft X9F5, available at <http://www.x9.org/committees_f.html> (members only).
ANSI X9.79	Public Key Infrastructure – Practices and Policy Framework, annex B, ANSI X9.79 (2001), available at <http://www.x9.org/docs.html>.
ANSI X9.84	Biometric Information Management and Security, ANSI X9.84 (2001), available at <http://www.x9.org/docs.html>.
APEC	Issues Relating to the Use of Electronic Authentication: Executive Summary, ¶¶ 111-114, APEC Telecomm. Working Group, available at <http://www.apii.or.kr/apecdata/telwg/eaTG/eaTG-2.htm>.
ASTM Cert. Policy	Standard Certificate Policy for Healthcare PKI, Committee 31.20, American Society for Testing & Materials (ASTM) *available at* <http://www.astm.org>.
Australian E-Commerce Rpt.	Electronic Commerce: Building the Legal Framework, Electronic Commerce Expert Group Report to the Attorney General, Australia (31 Mar. 1998), available at <http://www.law.gov.au/aghome/advisory/eceg/ecegreport.html>.
Australian Privacy Principles	Consumer Protection Principles in Electronic Commerce, Australian Competition and Consumer Commission (ACCC), 8 Oct. 1998, annex 2, *available at* <http://www.accc.gov.au/ecomm/principles.htm>.
Baker Presentation	Liability Presentation by Stewart Baker to the Copenhagen Hearing, European Commission, Directorate-General XIII (24 Apr. 1998).
Bank Act of 1956	Bank Holding Company Act of 1956, § 4(k)(4)(F), 12 U.S.C. § 1843(k) (1956).
Banking Certificates	Banking – Certificate Management Part 1: Public Key Certificates, ISO/CD-15782-1 (26 Feb. 1998).
Born	International Arbitration and Forum Selection Agreements: Planning Drafting and Enforcing, Dispute Toolkit, Born, G. (1999).
British Code	Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically, British Standards Institute Evidentiary Support for Electronic Information Committee, available at <http://www.bsi-global.com/Standards+Commercial/index.xhtml>.
British Standard pt. 1	Code of Practice for Information Security Management, pt. 1, BS 7799 - Information Security (1999), available at <http://bsonline.techindex.co.uk>.
British Standard pt. 2	The Requirements Specification for Information Security Management, (pt. 2), BS 7799 - Information Security (1999), available at <http://bsonline.techindex.co.uk>.
Brussels Regulation	Brussels Regulation on Jurisdiction and The Enforcement of Judgments in Civil and Commercial Matters, European Commission, 18 Int'l Legal Mat'ls 8 (1979), Brussels 1968 (Full Faith and Credit Convention), available at <http://europa.eu.int/eur-lex/en/lif/dat/1968/en_468A0927_01.html>.
Business Corp. Act Amendments	Changes in the Model Business Corporation Act—Amendments Pertaining to Electronic Filings/Standards of Conduct and Standards of Liability for Directors, 33

SHORT TITLE	BIBLIOGRAPHY
	Bus. Law. pg. # (Nov. 1997).
C.F.R. Definitions	Records Management, Electronic Records Management, 36 C.F.R. pt. 1234.2 (1995).
California Regulation	Digital Signature Regulations, CAL. CODE REGS. Tit. 2, § 22003, available at <http://www.ss.ca.gov/digsig/finalregs.htm>.
California Signature Law	Digital Signature Law, CAL. CODE § 16.5 (1997), available at <http://www.ss.ca.gov/digsig/digsig.htm>.
Canadian Accreditation Presentation	Government of Canada Public Key Infrastructure – Approach to Accreditation, William Dziadyk presentation to ABA Information Security Committee (31 Jul. 1997).
Canadian Algorithms	Cryptographic Algorithms for Use by CAs within the Gov't of Canada PKI, Gov't of Canada (2000), available at <http://www.cio-dpi.gc.ca/pki-icp/documents/documents_e.asp>.
Canadian Bill C-6	Personal Information Protection and Electronic Documents Act, Bill C-6, 2nd Sess., 36th Parliament, 48-49 Elizabeth II, 1999-2000, House of Commons of Canada (Royal Assent April 13, 2000), available at <http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html>.
Canadian Cert. Policies	Certificate Policies for the Government of Canada Public Key Infrastructure, Gov't of Canada (Apr. 1999), available at <http://www.cio-dpi.gc.ca/pki-icp/documents/documents_e.asp>.
Canadian Certification Guide	Guide to Certification and Accreditation of Information Technology Systems, Communications Security Establishment, Ottawa, Canada, available at <http://www.cse.dnd.ca/cse/english/Manuals/mg4int-e.htm>.
Canadian Certification Survey	Certification and Accreditation for PKIs and Certification Authorities – Survey of Standards, Trends and Identification of Potential Models, v. 2.0, William Dziadyk, Report to Industry Canada (7 Aug. 1998), available at <http://www.lgs.com/Services/adobe/m2svy_21.pdf>.
Canadian Confidentiality Policies	Digital Signature and Confidentiality, Certificate Policies for the Gov't of Canada Public Key Infrastructure, v. 3.02, Gov't of Canada (Apr. 1999), available at <http://www.cio-dpi.gc.ca/pki-cp/documents/Certificate_Policy/cp-pctb_e.asp>.
Canadian E-Commerce Act	Uniform Electronic Commerce Act, UNCITRAL Draft Uniform Rules on Electronic Signatures in Canada, Adopted by the Uniform Law Conference of Canada (30 Sept. 1999), available at <http://www.law.ualberta.ca/alri/ulc/current/euecafa.htm>.
Canadian Encryption Pamphlet	Email Encryption Made Simple, Ontario, Canada, available at <http://www.ipc.on.ca/english/pubpres/sum%5Fpap/papers/encrypt.htm>.
Canadian Evaluation Criteria	The Canadian Trusted Computer Product Evaluation Criteria, v. 3.0e, Communications Security Establishment (Jan. 1993), available at <ftp://ftp.cse.dnd.ca/pub/criteria>.
Canadian Interface Specs.	PKI Certificate and Key Management Interface Specification, v. 1, Gov't of Canada (Mar. 2000), available at <http://www.cio-dpi.gc.ca/pki-icp/documents/documents_e.asp>.
Canadian Land Title Act	Land Title Amendment Act of 1999, Bill 93, 3rd Sess., 36th Parliament, British Columbia, Canada (enacted 15 Jul. 1999), available at <http://www.legis.gov.bc.ca/proceedings/bills.htm>.
Canadian PKI Mgt. Policy	Policy for Public Key Infrastructure Management in the Gov't of Canada, Gov't of Canada (27 May 1999), available at <http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/PKI/pki_e.html>.
Canadian Policy Framework	A Cryptography Policy Framework for Electronic Commerce: Building Canada's Information Economy and Society, Industry Canada, Ottawa (Feb. 1998).
Canadian Practitioners Checklist	Digital Signatures: A Practitioners Checklist, 11th Annual Mtg., John T. Ramsay, Presentation to the Canadian Corporate Counsel Association, Edmonton Alberta (23 Aug.1999).
Canadian Privacy Act	Personal Information Protection and Electronic Documents Act, (2000), available at <http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html>.
Canadian Security Standards	Model PKI CA IT Security Guidance Document, Gov't of Canada (2000), available at <http://www.cio-dpi.gc.ca/pki-icp/documents/documents_e.asp>.

SHORT TITLE	BIBLIOGRAPHY
CARAT Guidelines	Certificate Authority Rating and Trust (CARAT), NACHA Internet Council (27 Oct. 1998), available at <http://www.internetcouncil.nacha.org/carat/>.
Carnegie Melon Model	Systems Security Engineering Capability Maturity Model, v. 1.1, Carnegie Melon University (16 Jun. 1997), available at <http://www.securityfocus.com/focus/ih/ipc/SSE-CMM.htm>.
CBA Policy Review	Report of Cryptography Policy, Comments from the Canadian Banker's Association (17 Apr. 1998).
Certification Approach	Approach to Certification: A Paradigm Shift for Information Security, Frederick G. Tompkins, Nat'l Computer Security Assoc. (22 Jul. 1997).
CIMCs Level 3	Certificate Issuing and Management System, Level 3, Protection Profile, v. 0.3, NIST (12 July 1999) § 3.2.1.6.
CIMCs Protection Profile	Certificate Issuing and Management Components (CIMCs) Protection Profile, v. 2.1, ISO/IEC 15408 (26 Jan. 2001), available at <http://csrc.nist.gov/pki/documents>.
Common Criteria Evaluation	Common Criteria Evaluation and Validation Scheme for IT Security, v. 1.0, NIST and NASA (Aug. 1998).
Computer Privacy Act	Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a (1994).
COPPA	Children's Online Privacy Protection Act of 1998 ("COPPA"), 15 U.S.C. §§ 6501-6505 (23 Jan. 2000).
COPPA Final Rule	Children's Online Privacy Protection Rule; Final Rule, Part III, Federal Trade Commission, 16 C.F.R. pt. 312 (3 Nov. 1999).
Cryptography Standards	Public Key Cryptography Standards, v.2.1, RSA Laboratories (5 Jan. 2001), available at <http://www.rsa.com>.
Danish Signature Bill	Draft Danish Bill for Act on Digital Signatures, Copenhagen Hearing on 23-24 Apr. 1998, European Commission, Directorate-General XIII, Telecommunications, Information Market and Exploitation of Research (16 Feb. 1998).
Dept. of Commerce Letter	Letter from the U.S. Dept. of Commerce to Tom Bliley, Chairman of the House Commerce Comm. (4 Aug. 1999), available at <http://www.ogc.doc.gov/ogc/legreg/letters.htm>.
DHHS Privacy Rule	Standards for Privacy of Individually Identifiable Health Information; Final Rule, Dept. of Health and Human Services, 45 C.F.R. pts 160, 164 et seq. (28 Dec. 2000)
DHHS Signature Rule	Security and Electronic Signature Standards, Proposed Rule, Dept. of Health and Human Services, 45 C.F.R. pt. 142 (1998).
Digital Signature Std.	Digital Signature Standard, FIPS 186-2 NIST (Jan. 2000), available at <http://nsi.org>.
DOD X.509	X.509 Certificate Policy, v. 0.5, U.S. Dept. of Defense, 239 Fed. Reg. 69,006 (1998)
DSG	Digital Signature Guidelines, ABA Information Security Committee (1996), available at <http://www.abanet.org/scitech/ec/isc/dsgfree.html>.
EC Convention	Jurisdiction and The Enforcement of Judgments in Civil and Commercial Matters, Brussels 1968 (Full Faith and Credit EC Convention).
EC Theme Paper	Theme Paper for the Copenhagen Hearing, European Commission, Directorate-General XIII, Telecommunications, Information Market and Exploitation of Research, 23-24 April 1998.
EESSI Final Report	European Electronic Signature Standardization Initiative (EESSI) Final Report to the European Commission, EESSI Expert Team (20 July 1999), available at <http://www.ict.etsi.fr/eessi/Final-Report.doc>.
Efficiency Act	Electronic Financial Services Efficiency Act, H.2937, 105th Cong. (1997), available at <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_bills&docid=f:h2937ih.txt.pdf>.
Enhancement Act	Electronic Commerce Enhancement Act, H.2991, 105th Cong. (1997), available at <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_bills&docid=f:h2991ih.txt.pdf>.
EPA Directive	Records Management Manual, Chapter 8 – Documentation and Preservation of Electronic Records, EPA Directive 2160 (17 Sept. 1997), available at <http://www.epa.gov/irmpoli8/recmgmt>.
E-SIGN Act	The Electronic Signatures in Global and National (E-SIGN) Commerce Act, 15 U.S.C. § 7001 et. seq., Pub. L. No. 106-229 (enacted 30 June 2000, effective 1 Oct. 2000).

SHORT TITLE	BIBLIOGRAPHY
ETSI Signature Standard	Policy requirements for certification authorities issuing qualified certificates, v.1.1.1, European Telecommunications Standards Institute (ETSI TS 101 456) (Dec. 2000) § 7.4.4(f), available at <http://www.etsi.org/sec/el-sign.htm>.
EU Data Privacy Directive	Protection of individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Council Directive 95/46/EC, 1995 O.J. (L 281), 31 (24 Oct. 1995), available at <http://europa.eu.int/eur lex/en/lif/dat/1995/en_395L0046.html>.
EU Lugano Convention	European Free Trade Association ("EFTA") Convention on Jurisdiction and Enforcement of Judgments in Civil and Commercial Matters, 1999 O.J. (L 319), 9 (1999), available at <http://www.curia.eu.int/common/recdoc/convention/en/c-textes/lug-idx.htm>.
EU Recommendation	Information Technology Security Evaluation Criteria (ITSEC), Council Recommendation 95/144/EC (7 April 1995), available at <http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/SecurityIssues.html#ITSEC>,
EU Resolution	Ensuring Security and Trust in Electronic Communication – Towards A European Framework for Digital Signatures and Encryption, Council Resolution, COM(97)0503 (20 May 1998), available at <http://europa.eu.int/ISPO/ecommerce/legal/documents/598IP0189/598IP0189_EN.pdf >.
EU Rome Convention	EU Rome Convention, European Commission (1980), available at <http://www.jus.uio.no/lm/ec.applicable.law.contracts.1980>
EU Signature Directive	Community Framework for Electronic Signatures, Council Directive 1999/93/EC, 2000 O.J. (L 013) 12-20 (13 Dec. 1999), available at <http://www.bmck.com/ecommerce/directivecomp1.htm>.
FDA Glossary	U.S. Food and Drug Administration, Electronic Records, 21 C.F.R. pt. 11, Subpart C, 62 Fed. Reg. 13,464 (20 Mar. 1997)
Fed. R. Evid. Reform	The Need for Reform of the Uniform Rules of Evidence to Accommodate the Admission into Evidence of Electronic Records, ABA Law of Commerce in Cyberspace Committee, available at <http://www.abanet.org/buslaw/cyber/archive/reform.html>.
Fed. Reserve Order	Federal Reserve Order to Identrus, LLC (10 Nov. 1999), summarized in GAO, Letter to the Chairman of the Board of Governors of the Federal Reserve System and to the Comptroller of the Currency, "Bank Regulators' Evaluation of Electronic Signature Systems" (8 Nov. 2000), available at <www.steptoe.com/webdoc.nsf/Files/GAObankpki/$file/GAObankpki.pdf>.
Fed. Reserve Standards	Uniform Standards for E-SIGN Act, Federal Reserve System, 66 Fed. Reg. 17,329 (Mar. 30, 2001).
Ford	Secure Electronic Commerce, Warwick Ford and Michael Baum (Prentice Hall, 2nd ed. 2001).
Fry	A Preliminary Analysis of Federal and State Electronic Commerce Laws, Patricia Brumfield Fry, available at <http://www.uetaonline.com/docs/pfry700.html>.
FTC Privacy Rule	Final Rule – Privacy of Consumer Financial Information, 65 Fed. Reg. 3,645, 16 C.F.R. pt. 313, Federal Trade Commission (2000).
Gamma article	The future of BS7799, Gamma Secure Systems Ltd., available at <http://www.gammassl.co.uk/bs7799/future.html>.
Gatekeeper Criteria	Gatekeeper Criteria for Accreditation of Certification Authorities, v. 9, Australia (Feb. 2001), available at <http://www.govonline.gov.au/projects/publickey/Gatekeeper.htm>
Gatekeeper Strategy	Gatekeeper, A Strategy for Public Key Technology Use in Government, Office of the Gov't Information Technology, Australia (1998), available at <http://www.govonline.gov.au/publications/GatekeeperStrategy.pdf>.
Georgia Signature Law	Electronic Records and Signatures Act, GA. CODE ANN. § 50 (1997), available at <http://www.cc.emory.edu/BUSINESS/gds.html>.
German Signature Act	Federal Act Establishing the General Conditions for Information and Communications Services – Information and Communications Services Act, art. 3, 1997 F.R.G. (enacted 8 Jan. 1997), available at <http://www.iid.de/iukdg/gesetz/sigve.html>
GLB Act	Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq. (1999), available at

SHORT TITLE	BIBLIOGRAPHY
	<http://www.senate.gov/~banking/conf/confrpt.htm>
GUIDEC	General Usage for International Digitally Ensured Commerce (GUIDEC), Section on Financial Resources (Information Security Committee-Electronic Commerce Project of the International Chamber of Commerce), (2000), available at <http://www.iccwbo.org/home/guidec/guidec.asp>.
GUIDeS	Guidelines, Methodologies and Standards to set up a CA for Digital Signatures (GUIDeS), v. 1.1, European Union Project, SPRITE-S2, available at <http://www.regione.emilia-romagna.it/guides>.
HCFA Bulletin	Internet Communications Security and Appropriate Use Policy and Guidelines for HCFA Privacy Act-protected and othe Sensitive HCFA Information, HCFA Internet Security Policy Bulletin, U.S. Health Care Financing Administration (24 Nov. 1998)
HIPAA	Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §§ 264, 1320d (1996).
Horwitz	Jurisdiction in the Internet Age, E. Horwitz & S. Fraser, The Metropolitan Corporate Counsel (February 2001), n. 8, available at <http://www.darbylaw.com/jurisdiction.html>.
Illinois Security Act	Electronic Commerce Security Act, 5 ILL. COMP. STAT. 175/1-101 (enacted Aug. 1998).
Illinois Signature Act	Illinois Secure Electronic Signature Act, 5 ILL. COMP. STAT. 175/10-120(b)(enacted 1997, effective July 1, 1999)
Imwinkelried	Evidentiary Foundations, Edward J. Imwinkelried (4th ed. 2000)
Int'l Digital Commerce	General Usage of Internationally Digitally Ensured Commerce, International Chamber of Commerce (1997), available at <http://www.iccwbo.org/home/guidec/guidec_living_document.asp>.
Irish Act	E-Commerce Act of 2000, Directive No. 27, Ireland, available at <http://www.ecommercegov.ie>.
ISBN	Preserving Digital Information, chap. 4, ISBN 1-55570-353-4 (2000), pp 53-60.
ISO Common Criteria	Common Criteria for Information Technology Security Evaluation, ISO 15408.
ISO X.5 Recommendation	Information Technology - Open Systems Interconnection: The Directory: Authentication Framework, ISO/IEC 9594-8/ITU-T Recommendation X.509, 1998.
Italian Signature Law	Digital Signature Law – The Bassanini Law, Italy (15 Mar.1997), available at <http://www.pkilaw.com/> (English Translation).
Japanese Guidelines	Certification Authority Guidelines, Electronic Commerce Promotion Council of Japan (Jun. 1998), available at <http://www.ecom.or.jp/ecom/ecom_e/guide/cag.pdf>.
Joint Privacy Rule	Joint Final Rule – Privacy of Consumer Financial Information, 65 Fed. Reg. 35,161, 12 C.F.R. pt. 40, Office of the Comptroller of the Currency; 12 C.F.R. pt. 216, Federal Reserve System; 12 C.F.R. pt. 332, Federal Deposit Insurance Corporation; 12 C.F.R. pt. 573, Office of Thrift Supervision (2000).
Joint Standards Rule	Joint Final Rule, Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8,616 (1 Feb. 2001).
Jueneman	Biometrics and Digital Signatures, R. R. Jueneman and R. J. Robertson, Jr., 38 JURIMETRICS 427 (1998), available at <http://www.mcg.org.br/mirrors/digsig.pdf>
Kersten Presentation	Minimum Requirements in German Law, Certification, Products and Procedures, presentation by Heinrich Kersten to the Copenhagen Hearing. European Commission, Directorate-General XIII (24 Apr. 1998).
Legislation	Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce, Thomas J. Smedinghoff and Ruth Hill Bro, John Marshall Journal of Computer and Information Law (vol. XVII, no. 3) page 723 Spr 99, available at <http://www.pkilaw.com/>.
Lugano Convention	Jurisdiction and Enforcement of Judgments in Civil and Commercial Matters, European Commission, 1999 O.J. (L 319), 9 (1999) (European Free Trade Association (EFTA) Convention), available at <http://www.curia.eu.int/common/recdoc/convention/en/c-textes/lug-idx.htm>.
Malaysia Signature	Malaysia's Digital Signature Act, (1997) available at

SHORT TITLE	BIBLIOGRAPHY
Act	<http://www.geocities.com/Tokyo/9239/digisign.html>
Malaysia Signature Bill	Malaysia Digital Signature Bill 1997, § 67(b), available at <http://www.geocities.com/Tokyo/9239/digi5.html>
Maryland UCITA	Uniform Computer Information Transactions Act, MD. CODE ANN., Commercial Law § 21 (implemented Oct. 1, 2000).
Mgt. of Digital Sign. Certs.	WD-xxxx The Management of Digital Signature Certificates, Part: Certificate Policy and Certification Practice Statement Framework ISO/TC68/SC 2 (18 Mar. 1997) cite
Minnesota Authentication Act	Minnesota Electronic Authentication Act, MINN. STAT. § 325K.24, Subd. 1.(c)(1)(enacted May 19, 1999), available at <http://www.revisor.leg.state.mn.us/cgi-bin/bldbill.pl?bill=H0056.2&session=ls80>.
Minnesota Cert. Practices	Certification Practice Statements, Minn. R. 8275.0045.E (2001).
NACHA Interoperability	Certification Authority Interoperability: from Concept to Reality, National Automated Clearing House Association (NACHA), (1999).
Nat'l Gov. Assoc.	What Governors Need to Know About E-SIGN: The Federal Law Authorizing Electronic Signatures and Records, National Governors Association, available at <http://www.nga.org/cda/files/000922ESIGN.pdf>.
NBS Special Publ.	Care and Handling of Computer Magnetic Storage Media, NBS Special Publ. No. 500-101, pp. 37 – 52.
NCUA Privacy Rule	Final Rule – Privacy of Consumer Financial Information, 65 Fed. Reg. 31,721, 12 C.F.R. pt. 716, National Credit Union Administration (2000).
Netherlands Project	Trusted Third Party Project, Ministry of Transport, Public Works, Water Management and Ministry of Economic Affairs, Netherlands (Mar. 1999).
Network of Trust	Authentication and Network of Trust Pilot Program: Certificate Policy. Contact: Jane E. Larimer, NACHA, available at <http://www.pkilaw.com/>.
Nimmer	Electronic Signatures in Global and National Commerce Act of 2000: Effect on State Laws, Raymond T. Nimmer, available at <http://www.bmck.com/ecommerce/ueta-esign-2.doc>.
NIST Guide	Risk Management Guide – Computer Security, NIST Special Publication 800-30 [1st Public Exposure DRAFT] June 2001, p. 1
NIST Presentation	National Time Standards Presentation, Judah Levine, Time and Frequency Division, NIST
NIST Principles	Generally Accepted Principles for Securing Information Technology Systems, Marianne Swanson and Barbara Guttman, SP 800-14 NIST (Sept. 1996), available at <http://nsi.org>.
NIST Security Practices	Good Security Practices for Electronic Commerce, Including Electronic Data Interchange, Roy Saltman, SP 800-9 NIST (Dec. 1993), available at <http://www.nsi.org>.
NIST Security Requirements	Security Requirements for the Design and Implementation of Cryptographic Algorithms, and Modules, FIPS 140-1 NIST (11 Jan. 1994), available at <http://csrc.nist.gov/publications/fips/fips1401.htm>.
NSTISSI Glossary	National Information Systems Security (INFOSEC) Glossary, rev. 1, NSA, National Security Telecommunications And Information Systems Security Committee, No. 4009 (Jan. 1999).
OCC News Release / OCC Statement	Operating Subsidiary Application, OCC Approval Statement, Zions First National Bank, Comptroller of the Currency, Administrator of National Banks, Treasury Dept. (12 Jan. 1998), available at <http://www.occ.treas.gov/ftp/release/98-4.txt>.
OECD Consumer Guidelines	Guidelines for Consumer Protection in the Electronic Marketplace DSTI/CP(98)13/FINAL, OECD, available at <http://www.oecd.org/dsti/sti/it/consumer/index.htm>
OECD Cryptography Guidelines	OECD Recommendation concerning Cryptography Policy Guidelines, C(97)188/FINAL, OECD (27 Mar. 1997), available at <http://www.oecd.org/dsti/sti/it/secur/index.htm>.
OECD Privacy Guidelines	Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, C(80)58/FINAL, OECD, (23 Sept. 1980).

SHORT TITLE	BIBLIOGRAPHY
OMB Guide	Guidance on Implementing the Electronic Signatures in Global and National Commerce Act, OMB, <http://www.whitehouse.gov/OMB/memoranda/m00-15.html>;
Open Group Doc.	The Open Group document on PKI
Orange Book	Trusted Computer System Evaluation Criteria (TCSEC), the "Orange Book", DOD 5200.28-STD, Nat'l Computer Security Center (Dec. 1985), available at <http://www.radium.ncsc.mil/tpep/library/tcsec/index.html>.
OSI Model	OSI Basic Reference Model – Security Architecture, ISO/IEC 7498-2 (date).
Presidential Paper	A Framework for Global Electronic Commerce, Whitehouse, Washington DC, USA (1 Jul. 1997), available at <http://www.ecommerce.gov/framewrk.htm>.
Privacy Act of 1974	Privacy Act of 1974, 5 U.S.C. § 552 (1974).
Quebec Agreement	Quebec Model Cross-Certification Agreement, Serge Parisien and Veronique Wattiez-Larose, Univ. of Montreal.
Quebec Code	
Radicati Study	Public Key Infrastructure Security: Products and Services 1999-2003, Radicati Group (11 Aug 1999), available at <http://www.radicati.com/>.
Redish	Of New Wind and Old bottles: Personal Jurisdiction, the Internet, and the Nature of Constitutional Evolution, Redish, M.H., 38 JURIMETRICS J. 575-610 (1998).
Reg. B	Regulation B – Implementations for the Equal Credit Opportunity Act, Board of Governors of the Federal Reserve System, 12 C.F.R. pt. 202.17(d)(2), 30 Mar. 2001, available at <http://www.federalreserve.gov/BoardDocs/Press/boardacts/2001/20010329>.
Reg. DD	Regulation DD - Truth in Savings, Board of Governors of the Federal Reserve System, 12 C.F.R. pt. 230.10(a), 30 Mar. 2001, available at <http://www.federalreserve.gov/BoardDocs/Press/boardacts/2001/20010329>.
Reg. E	Regulation E – Implementation for the Electronic Fund Transfers Act, Board of Governors of the Federal Reserve System, 12 C.F.R. pt. 205.17(c), 30 Mar. 2001, available at <http://www.federalreserve.gov/BoardDocs/Press/boardacts/2001/20010329>.
Reg. M	Regulation M – Implemenatations for the Consumer Leasing Act), Board of Governors of the Federal Reserve System, 12 C.F.R. pt. 213.6(d), 30 Mar. 2001, available at <http://www.federalreserve.gov/BoardDocs/Press/boardacts/2001/20010329>.
Reg. Z	Regulation Z - Truth in Lending, Board of Governors of the Federal Reserve System, 12 C.F.R. pt. 226.36(d), 30 Mar. 2001, available at <http://www.federalreserve.gov/BoardDocs/Press/boardacts/2001/20010329>.
Reporter's Memorandum	Reporter's Memorandum of D. Benjamin Beard (15 Aug. 1997), available at <http://www.law.upenn.edu/bll/ulc/uecicta/ect997.htm>.
RFC 2459	Internet Public Key Infrastructure - X.509 Certificate and CRL profile, RFC 2459, Housley, R., Ford, W., Polk, T, Solo, D., IETF, available at <http://www.ietf.org/rfc/rfc.2459.txt>.
RFC 2510	Internet X.509 Public Key Infrastructure, Certificate Management Protocols, RFC 2510, Internet Engineering Task Force (IETF) (Mar. 1999), available at <http://www.ietf.org/rfc/rfc2510.txt>.
RFC 2511	Internet X.509 Public Key Infrastructure, Certificate Request Message Format, RFC 2511, Internet Engineering Task Force (IETF) (Mar. 1999), available at <http://www.ietf.org/rfc/rfc2511.txt>.
RFC 2527	Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, RFC 2527, Internet Engineering Task Force (IETF) (Mar. 1999), available at <http://www.ietf.org/rfc/rfc2527.txt>.
RFC 2560	Internet X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP), RFC 2560, Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C., IETF, available at <http://www.ietf.org/rfc/rfc.2560.txt>.
Robertson	Summary of Electronic Commerce Security Act, R.J. Robertson and Thomas J. Smedinghoff, Ill. B.J. (June 1999), available at <http://www.pkilaw.com/>.
Rome II Green Paper	Jurisdiction and applicable law in cross-border consumer complaints, ECLG/157/98 (29 Apr. 1998) available at

SHORT TITLE	BIBLIOGRAPHY
	<http://europa.eu.int/comm/consumers/policy/eclg/rep01_en.html>.
Schlecter Presentation	Essential Requirements in the EU Directive, presentation by Richard Schlechter to the Copenhagen Hearing, European Commission, Directorate-General XIII (24 Apr. 1998).
SEAL Act	The Digital Signature and Electronic Authentication Law (SEAL) Act of 1998, S.1594, 105th Cong. (1998), available at <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_bills&docid=f:s1594is.txt.pdf>.
SEC Rule	Exemption of Transactions Pursuant to Certain Contracts, Investment Company Act of 1940, SEC Rule 17a-4, 17 C.F.R. pt. 270 (1947).
Security Guidelines	Information Technology – Guidelines for the Management of IT Security (GMITS), TR13335 through 13335-5.
Singapore Signature Act	Singapore Electronic Transactions Act, § 18(2)(a) (1998), available at <http://www.cca.gov.sg/eta/part5.html>.
Spitzer Press Release	Toysmart Bankruptcy Settlement Ensures Consumer Privacy Protection, Office of NY State Attorney General Eliot Spitzer, Press Release (11 Jan. 2001), *available at* <http://www.oag.state.ny.us/press/2001/jan/jan11a_01.html>.
Stoneburner	Guidance for COTS Security Protection Profiles (CSPP), Gary Stoneburner, NISTIR 6462 NIST (Dec. 1999), available at <http://csrs.nist.gov/cc/pp/pplist.htm>.
Survey of Legislative Inititatives	Survey of State Electronic and Digital Signature Legislative Initiatives, Internet Law and Policy Forum (date), available at <http://www.ilpf.org/digsig/digrep.htm> (members only).
Swedish Overview	Digital Signatures – A Technological and Legal Overview, Swedish Interministerial Working Group on Digital Signatures, Ministry of Transport and Communications, Sweden (Feb. 1998).
Swedish Signature Stds.	Digital Signature Standards, Secure Electronic Information in Society (SEIS) Sweden (16 May 2000), available at <http://www.pkilaw.com/>.
Techniques	Risk and Trust Management Techniques for an "Open But Bounded" Public Key Infrastructure, Daniel Greenwood, 38 JURIMETRICS 277 (1998), available at <http://www.state.ma.us/itd/legal/obb.htm>.
TG11	Authentication of Records and Media, TG11, Nuclear Information and Records Management Association (1998), available at <http://www.pkilaw.com/>.
Treitel	The Law of Contract, G.H. Treitel (8th ed. 1991)
TWG White Paper	CA-CA Interoperability White Paper, PKI Forum, Technical Work Group (TWG) (2001), available at <http://www.pkiforum.org/pdfs/ca-ca_interop.pdf>.
U.S. Antipiracy Act	U.S. House of Representatives passed H.R.2652, the Collections of Information Antipiracy Act, on May 19, 1998.
U.S. Internet Tax Freedom Act	Internet Tax Freedom Act, Title III – Government Paperwork Elimination Act, Senate Bill S.442, § 310.
U.S.C. Definitions	Definition of Records, Electronic Communications, 44 U.S.C. § 3301.3 (1991).
UCITA	Uniform Computer Information Transactions Act, (formerly UCC art. 2B) U.S. Nat'l Conf. of Commissioners on Uniform State Laws (23 Jul. 1999), available at <http://www.law.upenn.edu/bll/ulc/ulc.htm#ucita>.
UETA	Uniform Electronic Transaction Act (UETA), U.S. Nat'l Conf. of Commissioners on Uniform State Laws (NCCUSL) (4 Aug. 1999), available at <http://www.law.upenn.edu/bll/ulc/uecicta/eta1299.htm>.
UK E-Commerce Legislation	Promoting Electronic Commerce, Consultation on Draft Legislation, Department of Trade and Industry, United Kingdom (Jul. 1999).
UK Assurance Guidelines	Computer Assurance Guidelines, Department of Trade and Industry, United Kingdom (date), available at <http://www.dti.gov.uk/cag>.
UK E-Commerce Statement	"UK E-Commerce Strategy: Building Confidence In Electronic Commerce - A Consultation Document" <http://www.dti.gov.uk/cii/ecommerce/ukecommercestrategy/index.shtml>.
UN 2001 Model Law	Report of the Working Group on Electronic, UNCITRAL, 37th Sess., U.N. Doc. A/CN.9/483 (6 Oct. 2000), available at <http://www.uncitral.org/english/sessions/unc/unc-34/483e.pdf>.
UN Draft Guide	Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures,

SHORT TITLE	BIBLIOGRAPHY
	UNCITRAL, 38th Sess., U.N. Doc. A/CN.9/WG.IV/WP.88 (30 Jan. 2001), available at <http://www.uncitral.org/english/workinggroups/wg-ec/wp-88e.pdf>.
UN Draft Rules	Draft Uniform Rules on Electronic Signatures, UNCITRAL, 33rd Sess., U.N. Doc. A/CN.9/WG.IV/WP.82 (29 Jun. 1999), available at <http://www.uncitral.org/en-index.htm>.
UN Model Law	Model Law on Electronic Commerce, UNCITRAL, 30th Sess., U.N. Doc. A/CN.9/421 (1996), available at <http://www.uncitral.org/english/texts/index.htm>.
UN-1	UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996), with additional article 5 bis as adopted in 1998 available at <http://www.uncitral.org/english/texts/index.htm> [visited May 31, 2001].
UN-2	Draft UNCITRAL Model Law on Electronic Signatures, Report of the Working Group on Electronic Commerce, Oct. 5, 2000, on the work of its 37th Session, for consideration at 34th Session of UNCITRAL, Jun-July 2001 <http://www.uncitral.org/english/sessions/unc/unc-34/483e.pdf> [visited May 31, 2001].
US Assessment System	The ABCs of the U.S. Conformity Assessment System, Maureen Breitenberg, NISTIR 6014 NIST (Apr. 1997), available at <http://nvl.nist.gov/ts/htdocs/210/217/primer.htm>.
US Senate Hearing	The Digital Signature and Electronic Authentication Law: Hearing on S.1594 before the Senate Subcommittee on Financial Services and Technology, 105th Cong. (11 Mar. 1998), available at <http://www.senate.gov/~banking/98_03hrg/031198/witness/witness.htm>.
US Task Force Model	Model Certificate Policy, Part A: Introduction and Approach, Discussion Draft, US Gov't PKI Task Force, Business and Legal Work Group (25 Mar. 1998), available at <http://www.cio.gov/fpkisc/documents/cert_policyA.htm>.
Utah Signature Act	Uniform Electronic Transactions Act, UTAH CODE ANN. § 46-3 (2001), available at <http://www.le.state.ut.us/~code/TITLE46/htm/46_02025.htm>.
Van Eecke	The Legal Situation of Digital Signatures in Europe, Patrick Van Eecke, Univ. of Leuven, Belgium (Mar. 1998), available at <http://www.law.kuleuven.ac.be/icri/>.
Virginia UCITA	Uniform Computer Information Transactions Act, VA. CODE ANN. §§ 59.501.1 (Michie 2001), available at <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+TOC59010000043000000000000>.
Washington Authentication Act & Admin. Rules	Washington Electronic Authentication Act, WASH. REV. CODE § 19.34.010 et seq. (enacted 29 Mar. 1996, effective 1 Jan. 1998); Washington Authentication Administrative Rules, WASH. ADMIN. CODE § 434-180 (1997), both available at <http://www.secstate.wa.gov/ea/ealaws.htm>.
Wiley Tech Brief	PKI, A Wiley Tech Brief, Tom Austin, Wiley Computer Publishing (2000).
Winn	Law of E-Commerce, Winn, J., & Wright, B., (4th ed. 2001) Chap. 3
Wittie	E-Sign of the Times, Robert A. Wittie and Jane K. Winn, <http://www.cybersecuritieslaw.com/KL/wittie3.htm>.
Wu	Incorporation by Reference and Public Key Infrastructures: Moving Beyond the Paper-Based World, Steven Wu, 38 JURIMETRICS 317 (1998).
X.501	ISO/IEC 9594-2/ITU-T Recommendations X.501, Information technology – Open Systems Interconnection – The Directory: Models, Geneva, 1999.
X.509 Amendment	Final Text of Draft Amendment on Certificate Extensions, ISO/IEC 9594-8/ITU-T Recommendations X.509 (Jun. 1996).

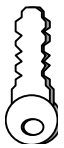
ORGANIZATION/ASSOCIATION	WEBSITES
AICPA/CICA WebTrust Program	http://webtrust.net/webtrust.html
American Institute of CPAs	http://www.aicpa.org/
Australian ICAA	http://www.icaa.org.au/
Canadian Institute Certified Accountants	http://www.cica.ca/
Certification Authority Accreditation Joint Project	http://www.magnet.state.ma.us/itd/legal/accred5.htm
Common Criteria and Protection Profiles	http://csrc.nist.gov/cc/index.html
Community Security Establishment (CC project status)	http://www.cse.dnd.ca/cse/english/cc.html
Computer Security Institute	http://www.gocsi.com/
Control Objectives for Information and Related Technology (CObIT)	http://www.isaca.org/cobit.htm
Critical Infrastructure Assurance Office (CIAO)	http://www.ciao.gov
Elec. Privacy Information Center	http://www.epic.org
Information System Audit and Control Assoc. (ISACA)	http://www.isaca.org/
Information Systems Security Org. (ISSO)	http://www.issa-intl.org/
International Computer Security Assoc. (ICSA)	http://www.trusecure.com/
NACHA	http://www.nacha.org
NASIRE	http://www.nasire.org
US Federal PKI Steering Committee	http://gits-sec.treas.gov./access/access_with_trust_contents.htm

Appendix 3 (APP 3): Tutorial

APP 3.1 TUTORIAL ON PUBLIC KEY TECHNOLOGY

This tutorial introduces the basic concepts underlying PKI technology. While there are many useful books that describe PKI technology in detail that you may wish to refer to for more details about PKI technology, this section will at least introduce the reader to certain foundational material to help in understanding of the remainder of this document. The *Digital Signature Guidelines* contain a tutorial concerning PKI technology, upon which this section is based. The *Digital Signature Guidelines* tutorial, however, concentrates on digital signature processes and technologies, while a full understanding of PKI requires additional understanding of confidentiality encryption, secure sockets layer ("SSL"), and access control functions of PKI technology.

APP 3.1.1 Public Key Cryptography

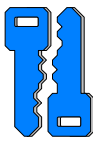


Cryptography is the branch of applied mathematics concerned with protecting information. Confidentiality is the protection of data against unauthorized access or disclosure through application of functions that transform messages into seemingly unintelligible forms and back again. These processes are called "encryption" and "decryption."[479] One kind of cryptography that can provide confidentiality, authentication, and integrity is called "symmetric key cryptography" in which an algorithm makes use of a single key used to encrypt data. The same key is also used to "decrypt" or return the encrypted data into its original form. This one key, called the "symmetric key," is very efficient in terms of processing speed and using minimal computing resources, but has two limiting security problems:

- First, how can two individuals who are interacting for the first time over an insecure network (such as the Internet) exchange a symmetric key securely? If the individuals tried to transmit the symmetric key over the insecure network, intending to encrypt information with it in subsequent communications, an attacker could intercept it key while in transit and use it to intercept and decrypt the later messages that the individuals hoped to keep confidential. Alternatively, an attacker could perform processes of his own with the symmetric key to make it appear as if a message written by the attacker had actually originated from the one of the individuals trying to communicate over the insecure network.

- Second, since both the "sender" and the "receiver" of a message share the same symmetric key, the authentication and integrity is not provable to a third party who does not also hold the key. Thus, while the authentication and integrity of a message may be sufficient between two trusted individuals, the sender could deny, or repudiate, the message. In general, symmetric cryptography cannot provide the additional security sever called nonrepudiation. The table *Mapping of Security Service to Cryptography Techniques* illustrates this point.

Another kind of cryptography, known as "public key cryptography," is an attempt to solve these particular shortcomings of symmetric key cryptography. Public key cryptography employs an algorithm using two



different but mathematically related keys, one for creating a digital signature or decrypting data, and another key for verifying a digital signature or encrypting data. Computer equipment and software utilizing such key pairs are often collectively termed an "asymmetric cryptosystem."

The complementary keys of an asymmetric cryptosystem for PKI technology are arbitrarily termed the private key, which is known only to the holder, and the public key, which is more widely known. If many people need the public key for various PKI applications, the public key must be available or distributed to all of them, perhaps by publication in an on-line repository or directory where it is easily accessible. Although the keys of the pair are mathematically related, if the asymmetric cryptosystem has been designed and implemented

[479] In a similar fashion, the integrity of a message can be verified using another technique called a Message Authentication Code (MAC).

securely it is "computationally infeasible" to derive the private key from knowledge of the public key. Thus, although many people may know the public key of a given holder, they cannot discover that holder's private key. This is sometimes referred to as the principle of "irreversibility."

Another fundamental process, termed a "hash function," is used in various PKI technologies. A hash function is an algorithm that creates from a message a digital representation or "fingerprint" in the form of a "hash value" or "hash result" of a fixed length. The hash result is usually much smaller than the message, but nevertheless substantially unique to it. Any change to the message produces a different hash result when the same hash function is used; i.e., the hash is unique to a given message for all practical purposes. In the case of a secure hash function, sometimes termed a "one-way hash function," it is computationally infeasible to derive the original message from knowledge of its hash value. Hash functions therefore enable the PKI application software to operate on smaller and predictable amounts of data, while still providing robust correlation to the original message content.

APP 3.1.2 Digital Signature Technology

Digital signatures are one application of public key cryptography, or more specifically, digital signatures are created and verified by public key cryptography. The signer has a key pair consisting of a private key and a public key. The signer holds a private key known only to the signer, which the signer uses to create the digital signature. The signer also has a public key, which is used by a relying party to verify the digital signature. Relying parties must obtain the signer's public key in order to verify the signer's digital signature. As applied here, the principle of irreversibility means that it is computationally infeasible to discover the signer's private key from knowledge of the public key and use it to forge digital signatures.

Software creating and verifying digital signatures makes use of hash functions. Any change to a digitally signed message produces a different hash result when the relying party uses the same hash function. These hash functions, when used with cryptography as described below, provide assurance that there has been no modification of the message since it was digitally signed.

Use of digital signatures usually involves two processes, one performed by the signer and the other by the receiver of the digital signature:

Digital signature creation uses a hash result derived from and unique to both the signed message and a given private key. For the hash result to be secure, there must be only a negligible possibility that the same digital signature could be created by the combination of any other message or private key.

Digital signature verification is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key.

To sign a document or any other item of information, the signer first delimits precisely the borders of what is to be signed. The delimited information to be signed is termed the "message." Then a hash function in the signer's software computes a hash result unique (for all practical purposes) to the message. The signer's software then transforms the hash result into a digital signature using the signer's private key. Commonly, this transformation process is encryption, although other processes may be used. In short, the resulting digital signature is unique to both the message and the private key used to create it.

Typically, a digital signature (the transformed hash result of the message) is attached to its message and stored or transmitted with its message. It may also be sent or stored as a separate data element, so long as it maintains a reliable association with its message. Since a digital signature is unique to its message, it is useless if wholly disassociated from its message.

Verification of a digital signature is accomplished by computing a new hash result of the original message by means of the same hash function used originally to create the digital signature. Then, using the public key and

the new hash result, the verifier checks: (1) whether the digital signature was created using the corresponding private key; and (2) whether the newly computed hash result matches the original hash result, which was transformed into the digital signature during the signing process. The verification software will confirm the digital signature as "verified" if: (1) the signer's private key was used to digitally sign the message, which is known to be the case if the signer's public key can be used to verify the signature; and (2) the message was not altered in transit, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the digital signature during the verification process.[480]

The processes of creating a digital signature and verifying it accomplish the essential effects desired of a signature for many legal purposes:

Signer authentication: If a public and private key pair is associated with an identified signer, the digital signature attributes the message to the signer. The digital signature cannot be forged, unless the signer loses control of the private key (a "compromise" of the private key), by divulging it or losing the media or device in which it is contained, or an attacker is, through the application of massive computing resources performing cryptographic analysis, able to derive the private key from the public key.[481]

Message authentication: The digital signature also identifies the signed message, typically with far greater certainty and precision than paper signatures. Verification reveals any tampering, since the comparison of the hash results (one made at signing and the other made at verifying) shows whether the message is the same as when signed.

Affirmative act: Creating a digital signature requires the signer to use the signer's private key. This act can perform the "ceremonial" function of alerting the signer to the fact that the signer is consummating a transaction with legal consequences.

Efficiency: The processes of creating and verifying a digital signature provide a high level of assurance that the digital signature is genuinely the signer's. As with the case of modern electronic data interchange ("EDI") the creation and verification processes are capable of complete automation (sometimes referred to as "machinable"), with human interaction required on an exception basis only. Compared to paper methods such as checking specimen signature cards -- methods so tedious and labor-intensive that they are rarely actually used in practice -- digital signatures yield a high degree of assurance without adding greatly to the resources required for processing.

The processes used for digital signatures have undergone thorough technological peer review for decades. Digital signatures have been accepted in several national and international standards developed in cooperation with and accepted by many corporations, banks, and government agencies. The likelihood of malfunction or a security problem in a digital signature cryptosystem designed and implemented as prescribed in the industry standards is extremely remote, and is far lower risk than that of a undetected forgery or an alteration on paper or of using other less secure electronic signature techniques.

Mapping of Security Services to Cryptographic Techniques

***Cryptography Techniques*: *Security Services*:**	**Encryption / Decryption**	**Message Authentication Codes / Keyed Hash**	**Digital Signature Generation / Verification**
Confidentiality	Symmetric or Asymmetric	-	-
Authentication	-	Symmetric or Asymmetric	Asymmetric only
Integrity	-	Symmetric or Asymmetric	Asymmetric only
Nonrepudiation	-	-	Asymmetric only

[480] Various asymmetric cryptosystems create and verify digital signatures using slightly different algorithms and procedures, but share this overall operational pattern.

[481] Where reliable cryptosystems and keys of sufficient length are used, however, it is infeasible for all practical purposes for an attacker to discover the private key using cryptographic analysis.

APP 3.1.3 Digital Certificates

The description of the use of digital signatures above leaves open one security question that must be resolved in an infrastructure for secure electronic commerce: how can the verifier obtain the alleged signer's public key in a way to assure that the public key is, in fact, that of the signer? Some mechanism is necessary to avoid the scenario of an attacker intercepting the message, rewrapping the plaintext of the message with his own digital signature, and giving the verifier his own public key. The attacker could pass off his own public key as if it were the public key of the intended signer. The verifier, using the attacker's public key, will find that the public key is able to process the digital signature on the message he received. Moreover, the verifier will think that the message originated with the signer, not the attacker. The verifier needs a mechanism to obtain the public key of the signer in a reliable way to avoid this kind of substitution.

Within a PKI, the method for preventing this kind of substitution attack is the "digital certificate" (also known as the "public key certificate" or simply a "certificate"). Different formats of certificates are available for use. Nonetheless, the most widely recognized format for certificates is the format defined in International Organization for Standardization/ International Electrotechnical Commission/International Telecommunications Union X.509 standard.

A certificate is a message stating that a public key belongs to or is associated with a given individual, organization, or device. The party issuing the certificate is a "certification authority" or "CA," and the party receiving it is called the "subscriber." A digital certificate is itself a digitally signed message. The issuing CA signs the message with its private key. The digital signature on the certificate itself provides assurances of the origin of the CA signing it, and the fact that the certificate has not been tampered with since issuance. Thus, the certificate is the CA's signed assertion that a particular public key belongs to a specific individual, organization, or device. To the extent the relying party trusts the CA, the relying party can trust in this binding and use the public key in the certificate with confidence to verify digital signatures of the subscriber.

Of course, if the certificate is a digitally signed message binding a subscriber to a public key, it is also necessary to obtain the CA's public key to verify the digital signature on the certificate. How can the relying party verify the CA's public key? Often, a PKI consists of a hierarchy of CAs, including high level issuers, called "roots" or "root CAs," as well as CAs subordinate to the root that issue certificates to end-user subscribers. The root CA issues certificates to the subordinate CAs with the public key of the subordinate CAs in them. Thus, to verify the public key of the CA issuing the certificate to the subscriber, the verifier can use the certificate issued by the root CA to the subordinate CA containing the CA's public key.

Again, however, it is necessary to have the root's public key in order to verify the digital signature on the certificate issued to the subordinate CA. How does the relying party verify this "root public key"? Again, the verifier obtains the root public key from a certificate, but since the root has no CA above it in the hierarchy, the root has to issue itself a certificate containing its own public key. This certificate is called a "self-signed" certificate because the root is attesting to the binding between it and its own public key. This self-signed certificate is also called a "root certificate" because it is the certificate containing the root public key.

Therefore, the certificate of the signer of a message, the certificate of the CA that issued the signer's certificate, and the certificates of the CAs above it in the hierarchy form a "certificate chain" starting with the end-user and terminating with the root. It is possible to obtain the public key of the signer of the message or certificate by obtaining the certificate issued by the next-higher entity in the PKI hierarchy. The software of the verifier of the original digitally signed message can process all of the digital signatures in the message and the certificate chain, and thus alert the verifier as to whether these digital signatures are all valid.

Ultimately, however, it is necessary to ensure that the verifier has the correct root certificate to prevent an attacker from substituting a phony public key. And since there is no certificate higher in the hierarchy, it is not possible to verify the digital signature on the root certificate with reference to a higher certificate. Some certificate must be trusted, and that certificate is the root certificate. How, then, can the root certificate be trusted?

The verifier should not depend upon obtaining the certificate via an insecure network due to the danger of the substitution attack. Consequently, other solutions are necessary to distribute the root certificate. If the verifiers that need the root certificate are small in number, it is possible to distribute the root in person. For example, a company having an internal PKI may arrange to have information systems personnel personally install the roots in all company computers. Root certificates may also be distributed on media using trustworthy non-Internet delivery mechanisms, such as reputable courier services or even postal mail.

All of these solutions, however, require the relying party or his agent to install the root in the computers that will use it. While this option may be satisfactory for small communities, it is difficult to scale this solution to large populations. As a result, many CAs have arranged with software manufacturers to embed their roots within the software itself. Under this solution, when a verifier needs to refer to a root certificate, the root certificate is already within the verifier's software and is available for use. To date, this solution has proved to be the most effective method of distributing roots widely.

In sum, the certificate is an assurance that a particular public key is bound to the identity of a particular person, organization, or device. This kind of certificate is called an "identity certificate." It is also possible to bind a public key to some other attribute of the subscriber besides the subscriber's identity. These certificates are known as "role-based certificates" or "attribute certificates." For example, it is possible to bind a public key to a role, such as "purchasing officer" or "CEO"; an authority or right, such as "right to see confidential financial data"; or a characteristic, such as a $3,000 credit limit. Therefore, a certificate may be a digitally signed assurance that a particular public key is bound to "a person with a $3,000 credit limit" without knowing whom that person is.

As of the time the PAG is published, however, the certificates in wide scale commercial and government deployment are mostly identity certificates. We have not yet seen a mature implementation of role-based or attribute certificates. Therefore, this version of the PAG is exclusively directed toward identity certificates.

APP 3.1.4 Confidentiality via Encryption

In addition to digital signatures, public key technology may be used to encrypt messages in order to protect the confidentiality of the information contained within them. In the encryption process, the sender of the data to be kept confidential uses the recipient's public key to encrypt the data. The recipient uses the recipient's private key to decrypt the data. The principle of irreversibility here means that it is computationally infeasible for anyone intercepting the message and having knowledge of the recipient's public key to derive the private key and decrypt the data. That is, the use of public key technology for encryption provides the sender with assurances that attackers intercepting the message will not be able to decrypt the data. Moreover, only the recipient, who holds that private key, will have the ability to decrypt the data.

Widely deployed encryption software, such as e-mail clients, can perform these encryption functions. This software, however, does not use the asymmetric key to encrypt the entire plaintext of the message. Asymmetric key operations tend to be costly in terms of time and computing power. Therefore, software commonly uses a symmetric key used only for this one operation (called a "session key") to encrypt the plaintext message and thenin turn uses the recipient's public key to encrypt the symmetric session key. The message sent to the recipient includes the encrypted message and the encrypted session key. The recipient then uses the recipient's private key to decrypt and recover the session key. The session key is then used to decrypt the message itself.

As with digital signatures, a sender of a confidential message can obtain the public key of the recipient using the recipient's certificate. The sender, therefore, becomes a relying party relying on the certificate of the subscriber recipient. Note that in the encryption scenario the message sender is the relying party and the recipient is the subscriber. By contrast, in the digital signature scenario, the signer who sends the message is the subscriber, and the recipient verifier is the relying party,

APP 3.1.5 Secure Sockets Layer

One of the best-known uses of public key technology is the protocol known as the Secure Sockets Layer ("SSL"), which protects the communications between a browser on a client machine and a server over an insecure network, such as the Internet. People every day access e-commerce sites to purchase goods and services over the Internet, and wish to secure their sessions with these sites to protect the confidentiality of information such as credit card numbers. The magnitude of this everyday use of SSL to protect these sites indicates that SSL is by far the most widespread commercially deployed PKI technology.

SSL is a session-based protocol. It protects the transient session that occurs when a user's browser communicates with a server. Following termination of the session, there are no residuals of the PKI processes. By contrast, if A sends B a digitally signed or encrypted message, the message may remain with B, and B can verify the digital signature or decrypt the message at a later time when B opens the message. The digitally signed or encrypted message remains after B has received the message.

An SSL session consists of the following procedures:

- A browser sends a request to connect to a site that has a server certificate. The user performs this request by clicking on a link indicating that it leads to a secure site, or the user types in a URL with an "https" protocol specifier, as in https://www.xyz.com.
- The server responds and provides the browser with the server's certificate.
- The browser verifies the digital signatures on the server certificate with reference to a certificate chain leading to a trusted root certificate. In older browsers, the browser may only determine whether a trusted CA issued the certificate based on the presence of the CA's root public key in the browser. The browser also compares the server's domain with the domain listed in the certificate to ensure that they match. If these steps are successful, the server has been authenticated to the user, providing assurances to the user that the user is accessing a real site whose identity was validated by a CA. This process is called "server authentication."
- Optionally, the server may request the user's certificate. The server can use the user's certificate to identify the user, a process called "client authentication."
- The browser generates a symmetric session key for use by the browser and server in encrypting communications between the two.
- The browser encrypts the session key with the server's public key obtained from the server certificate and sends the encrypted key to the server.
- The server decrypts the session key using its private key.
- The browser and server use the session key to encrypt all subsequent communications.

Following these procedures, the user may notice a padlock symbol appearing on the screen. In addition, the user will be able to inspect the certificate on the site using the browser.

With respect to server authentication and the confidentiality encryption inherent in the SSL session, the user is the relying party who relies on the server's certificate. If the server is performing client authentication, the web site is also a relying party who relies on the client certificate of the user.

APP 3.1.6 Access Control

Public key technology, and digital certificates in particular, may also be used to enable a web site to control access to information the site is attempting to keep confidential. For example, the site may require users wishing to access to the site to first obtain a certificate. The browser then requests a connection with the site's server. The server then requests that the user provide the server an appropriate certificate to obtain access to the site. The server then checks the certificate to ensure that it is in fact appropriate and, if so, allows the user access to the site.

The server can be configured to consider all certificates issued by a certain CA to be appropriate certificates. Such a configuration would correspond to a validation policy whereby the CA issues certificate to all those persons, and only those persons, entitled to have access to the site. For example, if the site contained a company's accounting data, a special-purpose CA may be created for the company's accountants, and all the accountants are issued certificates from that CA. After receiving their certificates, all accountants could use these certificates to access the site. The server, however, would not allow persons without such a certificate, even employees of the same company with other company certificates, to access the site. The server could be configured to accept only the accounting CA's certificates.

Less common is an application that must extract the information from the certificate and compare the information against a database. An example would be an application that parses the certificate, extracts the common name from it, and compares the common name against a list of persons permitted access to the site. In these applications, it is not sufficient to have a certificate from a given CA or set of CAs. Rather, the application requires more granular control and allows only some subscribers to have access.

In either case, the entity establishing the web site acts as a relying party in this scenario. The person seeking access to the site is the subscriber.

APP 3.1.7 Biometrics

Biometrics is a term referring to the measurement of one or more biological characteristics of an individual, such as fingerprints, voice recognition, eye imaging, hand geometry, and the like. Primarily a form of identification and authentication, biometrics can enhance PKI and can be enhanced by PKI.

- A biometric can augment or replace the access control placed over a subscriber's private key.
- The integrity and authenticity of the biometric template can be ensured via digital signature and can even be enveloped within a digital certificate.
- The biometric reader device can be authenticated via PKI (similar to existing mechanisms used for point-of-sale (POS) and automated teller machines (ATM).

The ANSI standard X9.84-2000 *Biometric Information Management and Security* addresses the use of PKI with biometrics for the financial industry.

APP 3.1.8 Key Management

Because cryptographic keys are very special pieces of data that require extraordinary handling, the subject warrants particular attention. Symmetric and asymmetric algorithms and their cryptographic keys all have different strengths, weaknesses, and properties that require distinct policy and practices to protect them.

Secret symmetric keys are called secret because nobody must know the value of the key. The algorithms that take the key and the data as cleartext input, and output the ciphertext are public information. Unlike passwords

where at least the owner of the password knows its value, the security of the cryptography relies upon the underlying sophistication of the publicly known algorithm and the secrecy of these strings of random binary bits called symmetric keys.

Assuming that the underlying symmetric algorithm (e.g., DES, RC6, MARS, AES) is of equal strength, then all things being equal, the longer the key the stronger the key. Each bit of a key doubles the key space that an attacker must search to determine the key. A 40-bit key gives 2^{40} = 1,099,511,627,776 possible keys or approximately one trillion keys. A 56-bit key yields2^{56} or approximately 72 quadrillion keys.

In 1999 at the RSA Security Conference it was announced that a group of researchers using approximately 100,000 workstations and a specialized computer called Deep Crack, successfully searched 90% of the 72 quadrillion keys to find the correct DES key in 22¼ hours. This unprecedented achievement has forced most systems to begin migrating to double length DES keys, increasing the relative strength to 112-bit keys, or stronger algorithms, such as the Advanced Encryption Standard (AES) which supports 128-bit, 192-bit, and 256-bit keys and offers unparalleled cryptographic security.[482]

Private keys are the secret part of an asymmetric key pair. Similar to symmetric keys, no one must know their values. Unlike symmetric keys, private keys are not random, but rather large numbers expressed as binary strings that are mathematically related to their counterparts, the public asymmetric keys. Each private key has one and only one corresponding public key.

In most implementations, the sheer size of the private key space is so large that finding the private key by exhaustive determination (as is typically done for symmetric keys) is considered to be infeasible. The strength of an asymmetric cipher is therefore measured by the difficulty of determining the private key from the public key.

The controls over the asymmetric private and public keys inherent in a properly deployed PKI ensure its reliability. For the public key, a digital certificate ensures the integrity and authentication of the subscriber's public key and provides the cryptographic binding between the subscriber's identity (and/or other attributes) and public key. The validation of the certificate applicant during enrollment is of paramount importance since the overall security of the PKI can be undermined if the wrong person is fraudulently or erroneously registered.

The relative strength of a public key is very dependent upon the characteristics of the specific algorithm and is a topic of research and debate. On February 2, 1999, a group of researchers completed the factorization of the 140 digit RSA modulus (approximately 490 bits). The work was accomplished with the General Number Field Sieve. The amount of CPU time closely matched what would be expected based upon the prior effort to factor the 130 digit RSA Challenge. A 155 digit number (512 bits) should be about 7.2 times harder in terms of time and 2.7 times harder in terms of memory requirements. A 1024-bit number should be about 40 million times harder in terms of time, and 6,300 times harder in terms of space.[483]

In some cases, such as hardware failure, employment termination, or even death, keys must be recovered. Key recovery is the ability to reconstitute a decryption key for the purposes of recovering encrypted data. This may be necessary in the event of a hardware failure, where the key has been lost, the untimely death of an employee where the password guarding access to the key is no longer available, or other circumstances where encrypted data must be recovered. There are several techniques available to enable key recovery, and these techniques are largely dependent upon the key management scheme employed. Special attention is needed to establish policies and implement procedures to ensure proper controls over key recovery.[484]

[482] *Available at* <http://csrc.nist.gov/encryption/aes/>.

[483] The RSA-140 Challenge information was provided by RSA Laboratories, *available at* <http://www.rsalabs.com>.

[484] General security practices disallow key recovery for the asymmetric private key used for signature generation.

APP 3.1.9 Assurance

A public key infrastructure (PKI) is an integration of hardware, software, and cryptographic components, combined with policies and procedures to enable business applications to operate securely. Adherence to an objective review of such policies and procedures can provide assurance of prudent business practices and due diligence. A more detailed discussion is provided in Appendix 4: *PKI Audit Methodology and Guidelines*. This section presents a framework in which to address the various roles that exist within a PKI and an overview of the assurance process. Nonetheless, as a practical matter, frameworks, roles, names of PKI components and assurance processes necessarily vary. Thus, the following is presented as an example.

The role of the **Policy Management Authority** is to create, approve and maintain the Certificate Policy (CP) and related policies (e.g., key management) and to manage or provide oversight of the PKI. The Policy Authority may be required to interpret and assure adherence to the applicable policies, determine when updates are necessary, and oversee change control management procedures. Policy Authorities are typically composed of the PKI stakeholders, including management, operations group, internal audit group, security officers, and risk management group. In some instances, the users and other "communities of interest" may also be involved.

The role of the **Issuer** (often, in practice, consolidated into the roles of and term "certification authority") is to issue certificates in response to authenticated certificate requests received from the Registration Authority. The Issuer can undertake or delegate the generation (creation) of such certificates to a *Certificate Manufacturer*. The scope of the Issuer role typically includes the issuance and revocation of public key certificates. The Issuer's name (or brand) may appear in the public key certificate. Sometimes certificates are "co-branded" where the co-branding party is certificate manufacturer or other party participating in the provision of PKI-related services.

The role of the **Certificate Manufacturer** is to generate and (typically) distribute digital certificates. The Certificate Manufacturer typically generates and protects its private key and manages the public/private key pair. Depending upon the implementation, the Certificate Manufacturer's public key (typically under the brand name of the Issuer) is distributed or otherwise made available to the End-Entities and/or the Relying Parties.

The role of the **Registration Authority** ("RA") is to serve as the primary interface with the User. The RA validates the identity and/or other attributes of the certificate applicant together with the applicable enrollment information prior to approving and submitting certificate requests to the Issuer. End-Entities may check on the status of certificate applications with the RA and may submit to the RA requests for certificate revocation. In order to maintain secure communications with the Issuer, the RA frequently also generates and maintains its own keys used for digital signatures or access control.

The role of the **Repository** is to manage and maintain public key certificates, certificate revocation lists, and other PKI-related information. In some regulated environments, the Issuer publishes any certification licenses within the Repository, typically located at its website. Furthermore, the Repository may act as a directory for relying parties to locate a User's digital certificate. The Repository may have diverse legal relationships with the other parties/components of a PKI.

The role of a **User** (a.k.a., subscriber) is typically to generate its asymmetric key pair(s), securely manage its private key(s), and register its public key(s) with the RA. The User is an entity that uses the PKI services to conduct business securely. Typically, most Users who have public key certificate are also Relying Parties.

The role of the **Relying Party** is that of the recipient of a User's public key and/or digital signature that relies on the trustworthiness of the certified public key.

The assurance that any system (or component thereof) is reliable and trustworthy is a function of three parameters and can be expressed as:

Trustworthy = ***f*** (technology, practices, audit).[485]

Each of these trust parameters is a distinct discipline and must be addressed independently. As a practical matter, the technologies and techniques used in a PKI include asymmetric cryptography, symmetric cryptography, key management, and cryptographic protocols. Practices include many of the operational aspects of managing the technology, such as company policies, automatic controls, and manual procedures, which, as a whole, enhance or provide for a trustworthy system. Policies include guiding principles addressing general security issues, privacy, cryptography, public key certificates, physical security, and standards etc. Automatic controls are those imposed and performed by the system hardware and/or software, whereas manual controls are manifested by the execution of written procedures.

The goal of any organization is best achieved by exercising due diligence in the deployment and assessment of technology via appropriate controls. Compliance with policies, standards, and procedures can only be assured by verification of the controls via an audit or other assessment. There are two primary types of security reviews, internal audits (or assessments) and external audits (or assessments). Internal audits are undertaken by employees of the audited entity, whereas external audits are undertaken by an independent third party, such as an audit firm. Internal security reviews are sometimes assisted by external audit firms or other assessors. The results of an internal audit are typically confidential within the company. External security reviews are performed by independent third parties. The purpose of the external audit can be for use limited to within the company, or may be issued to customers. The criteria used for internal or external security reviews may be internally generated or originate from recognized standards.[486]

APP 3.2 TUTORIAL ON PKI BUSINESS MODELS

This tutorial describes some of the different business models that assessors may encounter in performing their assessments. "Business models" refer to the various ways in which a PKI is organized, the purpose for the PKI, who is permitted to participate in the PKI, who performs the various functions of the PKI participants, and what relationships the parties have with each other. For instance, a PKI may have a "business model" of company-owned certification authorities that outsource front-end functions to registration authorities and that have the right to outsource back-end functions to certificate manufacturing authorities, where the CAs issue certificates to employees of the companies for the purpose of facilitating business-to-business transactions among the companies who contracted to create the PKI. This section, however, is not intended as an exhaustive listing of possible business models, and new models or variations on existing models are inevitable. Moreover, a PKI may contain elements from more than one business model, or imperfectly implement one. Nonetheless, as a practical matter, assessors will benefit from an understanding of the theory behind these models when assessing PKIs.

One type of PKI business model presented is the "open" PKI model. The open model typically involves one or more certification authorities issuing certificates that can be used (*i.e.*, relied upon) by anyone in the general public. In other words, anyone can be a relying party. In addition, this model assumes that the CA is a third party with respect to the relationship between the subscriber and relying party. That is, the CA is not directly involved in contractual or other relationships between the subscriber and relying party.

Because of this detached relationship, the open PKI model often involves one or more certification authorities that issue certificates to subscribers who may use the certificates for general purposes. For example, a region may have several CAs, all of whom issue certificates to individuals for use in secure e-mail and electronic commerce. The CA provides a general service of confirming the identity or other attributes of subscribers, and

[485] It is important to distinguish trustworthy from trust. The former is a property of the system, while the latter is a subjective judgment about the system.

[486] *See* PAG APP 2 (*Public Key Infrastructure – Practices and Policy Framework*, annex B, ANSI X9.79 (2001), *available at* <http://www.x9.org/docs.html>, hereinafter "ANSI X.9.79"); *see also* PAG APP 2 (*Statement of Auditing Standards*, 70 AICPA (2000), *available at* <http://www.aicpa.org/>, hereinafter "AICPA Standards").

anyone in the public can benefit from the assurances provided by the CA. Legislation that assumes the open PKI model is directed generally towards assuring the quality of these third party CAs to protect the subscriber and relying party communities from CAs falling below minimum quality standards. Examples of such legislation include the digital signature laws of Utah, Washington, and the Federal Republic of Germany.

In some literature, however, the notion of "open PKI" is defined in an even more extensive sense. In this more extensive notion of "open PKI," there is not only no direct CA involvement in the relationship between the subscriber and relying party, there is also no contractual relationship at all between the CA and the relying party. This view of" open PKI" also assumes that the act of reliance itself does not create a contract with the CA. Therefore, the relying party under this view is never bound by contract to the CA, and any legal implications of the relationship between the CA and the relying party arise from tort law, rather than contract law. This extensive view of "open PKI," however, is largely theoretical and, in hindsight, an outdated perspective; no major CAs avoid or disclaim privity with relying parties, or even admit the lack of privity. To the contrary, the major CAs that are the most "open" within the marketplace purport to have a contractual relationship with relying parties. To be more accurate, therefore, even the most "open" significant PKIs in existence are technically "contractual" PKIs as described below.

Another kind of PKI is the "closed" PKI model. In the closed model, the CA is itself the relying party (or the employer of the relying party). In one alternative, the relying party may outsource PKI services to a CA that will issue certificates to subscribers on behalf of the relying party.

Examples of a closed PKI model include a bank operating a CA and issuing certificates to its customers. This model may or may not involve a separate PKI-related contract between a company acting as CA and its customers. This model is frequently used by "enterprise" deployments of PKI to establish PKI services and issue certificates to the employees and possibly customers, suppliers, or other extranet members of an enterprise.

The liabilities and obligations contained in the closed model are usually a function of the business relationship (including bargaining position) between the parties. This may be the employer-employee relationship or a contractual relationship with a customer or supplier.

An additional PKI business model is the "contractual" model. In the contractual model, the provider of PKI service is bound by contract with its subscribers and relying parties. No party outside the contractual relationship is permitted to participate in the PKI. The contracts may create a contractual relationship between the subscriber and the CA or among many parties, including other subscribers. The advantage of this model is that risk, responsibility, and recourse can be clearly defined and managed. Thus, there is less reliance on tort law. Depending upon the implementation, the execution of a contract (and thus, creation of privity) between the parties may happen at anytime including immediately prior to reliance on a certificate.

APP 3.3 TUTORIAL ON PKI DOCUMENTATION

This tutorial describes the legal, business, and technical documentation that assessors may encounter in performing their assessments. These documents fall into three categories. First, policy documents can convey at a high level the requirements to which a PKI adheres and the practices the PKI employs to meet these requirements. The two most commonly used policy documents are the "certificate policy" and the "certification practice statement." Second, PKIs may utilize agreements to bind participants to the requirements of the PKI. The most common PKI agreements are the "subscriber agreement" and the "relying party agreement." Third, PKIs may utilize documents that set forth security, operational, and auditing practices. These documents set forth policies and procedures in a detailed fashion. This tutorial discusses each of these categories of documents in turn.

APP 3.3.1 Policy Documents

APP 3.3.1.1 Certificate Policy

A certificate policy ("CP") is defined in the X.509 standard as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements."[487] For example, a particular CP might indicate that a particular type of certificate may be used to verify digital signatures on e-mails requiring a high level of assurances and security. Alternatively, a CP may set forth rules for certificates used to authenticate parties engaging in transactions for the sale of goods or services within a given price range.

The X.509 definition of "certificate policy" points to two kinds of CPs, one directed to defining a type of certificate applicable to a "particular community" for which the PKI was designed and one directed to a type of certificate for a "class of application with common security requirements." A community of interest may create a PKI to allow interoperation among the members of that community. The community may be a group of participants within a certain vertical market, such as a group of banks hoping to create an authentication and payment system to support business-to-consumer transactions over the Internet. In this example, the banks can agree on the parameters for a single class of certificates to be issued to consumers and embody their policies in a certificate policy.[488]

An example of CPs covering a class of applications with common security requirements would be the Government of Canada Certificate Policies. Canada established four assurance levels for certificates, Rudimentary, Basic, Medium, and High, and wrote a certificate policy for each level reflecting the common security requirements for four sets of applications corresponding to these assurance levels. For instance, the CP for certificates having a high level of assurance describes a class of high-security applications. These applications have common security requirements, and the High assurance CP sets forth requirements for these certificates.

A CP is also said to be a "requirements" document. That is, it sets forth requirements that different participants within the PKI have to meet in order to operate within the PKI. The CP, however, leaves for other documents the details of the methods used to meet these requirements.

A CP may or may not be a public document, depending upon the nature of the applications and the business model of the PKI. For example, if the certificates issued in the PKI are used by a large, diverse population of relying parties, the CP must be available and accessible by the general public. The CP, therefore, may require participating CAs to post the CP on their web sites.

Other PKIs, however, may wish to keep their CPs private. A PKI may wish to place requirements in the document that it may wish to keep confidential for security reasons. In addition, a PKI not dealing with a large, diverse community of relying parties may simply consider the CP to be a private matter that does not need to be disclosed to the public.

Notice of an applicable CP may also appear in the certificate itself. The X.509 format defines a field within a certificate extension, called the Certificate Policies extension, which is intended to contain a registered number called an "object identifier" ("OID")[489] that identifies the relevant CP. By issuing a certificate containing a CP's

[487] Note that a CP may do more than "indicate the applicability" of the certificate to the community/class of application. Namely, it may set forth the rules governing the use of or reliance upon the certificate for that community/class of application, and it may serve as the foundation for interoperability, as described below. *See* RFC 2527, *supra* note 193.

[488] *See* PAG APP 2 (*Certification Authority Interoperability: from Concept to Reality*, National Automated Clearing House Association (NACHA), (1999), hereinafter "NACHA Interoperability").

[489] An OID is a unique alphanumeric or numeric identifier registered under the ISO registration standard (*see* RFC 2527, *supra* note 193) to reference a specific object or object class. OIDs are also used to uniquely identify a particular CP. The registration process of OIDs follows applicable procedures, such as those specified in ISO/IEC and ITU standards.

OID in its Certificate Policies extension, the CA in essence is asserting to potential relying parties that a certificate is appropriate for use in the applications described in the referenced CP. Thus, relying parties can configure their machines to look for the presence of a certain OID, knowing that they are using the certificates for the applications set forth in the CP corresponding to the OID. The CA is also asserting that the certificate and its practices and procedures meet the requirements of the CP.

CPs are useful to the assessment process in many possible ways. For example, the PKI may be bound by contract to abide by the CP, and its compliance may be determined by audit. Thus, the PKI may have an obligation to undergo an audit to compare the PKI's performance with the requirements set forth in the CP. Another example would be facilitating interoperation. CAs or PKIs that are more complex may agree to certify each other to establish a PKI that is the union of their individual PKIs. This process is known as "interdomain certification" or "cross-certification." It involves one CA issuing a certificate to another CA that certifies the second CA's public key and vice versa. The actual issuance of cross-certificates in a peer-to-peer fashion, however, may not be necessary, for instance if both PKIs establish a common root that certifies the public keys of CAs in both PKIs. In any case, before two PKIs agree to cross-certify each other or interoperate, they would probably wish to examine the CPs governing each other's PKI to ensure that they are largely compatible. After beginning to interoperate, CPs are also useful for evaluation and auditing.

APP 3.3.1.2 Certification Practice Statement

The term "certification practice statement" ("CPS") is commonly defined as: "[a] statement of the practices that a Certification Authority employs in issuing certificates." A CPS typically is a comprehensive statement of practices and procedures relating to the same kinds of subjects set out in a CP and is intended to describe what a CA does from a technical, business, and legal perspective, for instance to show how the CA implements its service offerings. A CPS is typically more detailed than a CP.

As with a CP, a CPS may or may not be a public document. Again, publication depends upon the nature of the applications and the business model of the PKI. A PKI used by a large, diverse population of relying parties often requires that the CPS be available and accessible for consultation by all concerned parties. The CA writing such a CPS may therefore post the CPS on its web sites and provide paper and electronic copies by other means. The CA may also wish to provide notice of its CPS in the certificates it issues. The X.509 specification for the Certificate Policies extension includes a field called the CPS Pointer Qualifier, which is intended to contain a URL of the CPS governing the certificate. By issuing a certificate containing a CPS's URL in the CPS Pointer Qualifier, the CA in essence is asserting to potential relying parties that its CPS at that URL governs the use and reliance upon the certificate.

By contrast, a CA that has written a CPS containing significant details may want to keep its CPS a private document. The CA may wish to keep its operational and security practices private in order to maintain security. Moreover, a CA dealing with a small, limited community may also feel no need to disclose the terms of its CPS.

CPSs, like CPs, can be an integral part of the assessment process. A CA, for instance, may on its own accord, or under requirement by law or contract, obtain a periodic compliance audit. In that case, the auditors may assess the CA's PKI against the benchmark set in the CPS. In addition, a PKI having a CP may require a CA to undergo an audit. In that case, auditors may have a two-fold function. First, they may need to ensure that the CA's CPS terms provide for a PKI that meets the requirements of the CP. That is, they study the CPS to ensure that if a CA follows its CPS, it will comply with the requirements in the CP, regardless of whether or not the CA actually does what it says it does in the CPS. Second, assuming the CPS complies with the CP, the auditors would ensure that the CA's practices actually adhere to the disclosures in the CPS.

In other instances, CPSs may be the basis for cross-certification among two CAs. The CAs may inspect each other's CPSs, determine that the assurance levels are equivalent, and issue cross-certificates to each other. Moreover, after cross-certifying each other, the CAs may look to the other CA's CPS on an evaluation or auditing basis to ensure that assurance levels remain equivalent.

APP 3.3.1.3 Relationship between a CP and CPS

CPs and CPSs are not the same thing. They fulfill different purposes. A CP is sometimes viewed as a statement of requirements (i.e., what needs to be achieved), whereas a CPS is viewed as a statement of procedures (i.e., how those requirements are to be satisfied).[490] Consequently, under most business models, the CP and CPS, if they exist at all, exist as two separate and distinct documents.

It is possible, however, for a PKI to have a CPS and not have a CP. For example, in a private PKI of a single CA having a single application, there is no need for a CP. The PKI may have a CPS to disclose to its customers or to the world what its practices and procedures are, but it may have no need to claim that its certificates satisfy any CP.

Moreover, even if a PKI that has both a CP and a CPS, the relationship between them may not be a one-to-one relationship. For example, a CA, having a single CPS, may issue certificates that satisfy more than one CP. That CA may use its CPS to disclose all of the CPs that the certificates satisfy. Likewise, a PKI may have a single CP and recruit multiple CAs to issue certificates satisfying that CP. Each CA may have its own CPS. Consequently, the number of CPs and CPSs that exist within a given PKI will depend upon the business model.

A CPS is by definition a document written or adopted by a CA, and a CA may also wish to write a CP. For example, a CA providing multiple classes of certificates may write a document embodying high-level requirements for these different classes and write a CPS document showing how the CA complies with the requirements of each class. In addition, a consortium of CAs may wish to agree among themselves to interoperate and establish a CP to govern this interoperation. Each CA within the consortium may also agree to have a CPS. In these cases, CAs adopt both a CP and a CPS as a complete document set providing for requirements and the practices meeting these requirements.[491]

Nonetheless, other parties besides CAs may have reason to adopt a CP. For instance, a large organization seeking to use certificates for secure e-mail or access control may write a CP. The organization may intend the PKI to be a vehicle by which it receives bids and responses to RFPs. It may wish to set up relationships with a network of CAs to provide certificates to sales representatives of bidding companies. In this case, the organization is essentially the relying party, or perhaps a sponsoring organization for an entire community of interest whose members are relying parties. The organization may wish to set standards for certificates to ensure that it or its members will be relying on trustworthy certification services. Therefore, the organization may want to write a CP and impose it upon its PKI vendors by contract.[492]

Not only may a CP be a vehicle for relying parties, a relying party community, or a relying party sponsor to assure obtaining trustworthy certification services, a subscriber, subscriber community, or subscriber sponsor may also want to have a CP. For example, an organization may wish to obtain certificates from a number of sources for use by its own employees or members. In order to ensure uniform quality among these certificates, it may draft a CP and impose it upon the CA vendors. Other scenarios besides CA-, relying party-, or subscriber-driven CPs are possible. For example, a CA and a relying party or subscriber community may wish to utilize a third party CP issued by a quality assuring entity to govern their PKI. For example, an industry consortium may wish to write a CP in order to record the industry's "best practices." The consortium itself may not wish to establish a PKI, but its members may independently use the CP to contract with CA vendors to ensure interoperability with the PKIs of the other consortium members. The consortium's CP then serves as a benchmark that others adopt. In coming years, yet other CP scenarios may become apparent.

[490] Subprocess documents, such as those describing operational procedures, are generally developed and deployed to further detail the actual processes and controls used to facilitate day-to-day operations and to ensure compliance with the CPS and CP.

[491] *See* NACHA Interoperability, *supra* note 488.

[492] *Id*., s*ee also,* DoD Interim External CA project *available at* <http://www.disa.mil/infosec/pkieca>.

In the situation where a subscriber or relying party community permits multiple CAs to function under a CP not issued by the CAs themselves, the CP may contemplate each CA authoring its own CPS. In that case, it may require these CPSs to conform to the CP, or to meet minimum requirements stated in the CP.

APP 3.3.2 Agreements

APP 3.3.2.1 Subscriber Agreements

A subscriber agreement is an agreement entered into by a subscriber obtaining a certificate that may contain the terms and conditions of the use of the subscriber's certificate and the private key corresponding to the public key in the certificate. In addition, a subscriber agreement may specify the rights and responsibilities of the respective parties. In addition to the subscriber, the other party to a subscriber agreement may be a CA or an RA. A subscriber agreement may be as simple as a brief statement of rights and obligations akin to a shrink-wrap license agreement for software. A more extensive subscriber agreement, however, may be appropriate for certificates having higher levels of assurances.

Like CPs and CPSs, a subscriber agreement may or may not be a public document, depending on the business model of the PKI. If the PKI allows members of the general public or large populations to obtain certificates, the subscriber agreement is typically shown upon enrollment and made available on the CA's web site or by other means for consultation later. If, however, the CA issues certificates to a small or limited group of subscribers, the CA may wish to keep the subscriber agreement private, or at least limit distribution to the group of potential certificate applicants.

Those assessing a PKI will likely find the subscriber agreement relevant if it functions to flow down requirements from a CP or implement terms of a CPS. During the assessment process, for example, the assessor may compare the subscriber agreement to the CPS to ensure that the CPS's subscriber obligations appear in the subscriber agreement. The assessor may also wish to determine if subscribers are, in fact, performing their obligations under the subscriber agreement.

The relationship between a subscriber agreement and the CPS will also differ by the business model of the PKI. In rudimentary PKIs, a CA may wish to state the practices under which it issues certificates in a single subscriber agreement. Such a document essentially would double as a CPS. Thus, a PKI may have no CPS separate from a subscriber agreement. Thus, in a rudimentary PKI, the distinction between a subscriber agreement and CPS may be a matter only of terminology. In more complicated PKIs, however, the CA will have both a CPS and a subscriber agreement. CPSs in these PKIs may be book-length documents in comparison with considerably shorter subscriber agreements.

APP 3.3.2.2 Relying Party Agreements

A relying party agreement is an agreement entered into by a party wishing to rely on a certificate and the information contained in it. In addition to the relying party, the other party to the relying party agreement is typically the CA that issued the certificate, but in theory could also be the RA that approved the certificate application. A relying party agreement governs the terms and conditions under which the relying party is permitted to rely upon the certificate. Most commonly, the agreement requires the relying party to check the status of the certificates in the chain of certificates upon which the relying party wishes to rely.

As with subscriber agreements, the nature of a PKI's relying party agreement will depend upon the PKI business model. A rudimentary PKI may not wish to have a relying party agreement because the low-assurance nature of the certificates may not, in the judgment of the CA, create much exposure to liability. Therefore, the CA may not think that a relying party agreement is worth the time and expense necessary to draft and implement it. Also, in some PKIs, the CA itself may be the relying party. For example, a bank may issue certificates to its customers as access control mechanisms for its customers to access account information at the bank. The bank would be relying upon certificates that the bank itself issued. Since CA and relying party are the same in this model, there is no reason to have a relying party agreement.

Similarly, the business model will dictate whether it is necessary to publish a relying party agreement. A PKI having a large, diverse population of relying parties would likely wish to publish the relying party agreement and show it to potential relying parties for consultation. Therefore, the CA may publish the relying party agreement electronically or by other means. In addition, the CA may also wish to point to its relying party agreement in the certificates it issues. Although the X.509 specification for the Certificate Policies extension does not include a special field for a pointer to the CA's relying party agreement, a CA may wish to populate the CPS Pointer Qualifier with the URL of the relying party agreement. Although the X.509 specification originally intended the CPS Pointer Qualifier to contain the URL of the CA's CPS, from a legal perspective, it may be more desirable to display for relying parties the relatively short relying party agreement rather than a long CPS. By issuing a certificate containing a relying party agreement's URL in the CPS Pointer Qualifier, the CA is asserting to potential relying parties that the referenced relying party agreement at that URL governs the use and reliance upon the certificate.

APP 3.3.2.3 Other Documents

CPs, CPSs, subscriber agreements, and relying party agreements are the core documents within a PKI. From a legal perspective, the subscriber agreements and relying party agreements are the fundamental building blocks within the PKI. However, the PKI may require other agreements as well. The following are some examples of other agreements that a PKI may employ:

- Agreements to facilitate interoperability. For example, a number of entities, possibly CAs, may enter into an interoperability agreement setting forth the terms and conditions under which interoperation will occur. More specific interoperation may occur when one CA certifies the public key of another. A unilateral certification may be governed by a Certification Agreement, while CAs cross-certifying each other may enter into a cross-certification agreements.

- Vendor agreements. An organization's PKI may be based on the technology obtained from a PKI vendor. If the vendor provides PKI software used by the organization to create its own PKI, it may enter into a software license agreement with the software vendor. If, by contrast, the organization uses a managed service, it would enter into a service agreement or outsourcing agreement with its vendor.

- Agreements aiding certificate distribution. An organization having a PKI may wish to extend the PKI to new geographical and vertical markets. Thus, it may enter into distribution or reseller agreements with entities already in these markets. Alternatively, a PKI may use RAs to extend its capabilities to validate certificate applications in new markets with a registration authority agreement.

- Internal agreements related to the trustworthiness of a PKI. Organizations operating a PKI may have internal agreements to ensure that personnel entering into trusted roles are contractually bound to security and personnel practices. Examples would include nondisclosure agreements and employment agreements authorizing background checks in accordance with personnel policies of the organization.

Documents other than agreements may also be relevant to any assessment. A review of these other documents is likely necessary to gain an in-depth view of the PKI being assessed, as well as a firm understanding of its trustworthiness. Often, the CP and CPS are at too high a level to provide an assessor with the technical, security, and operational details concerning the PKI. These details may be found in ancillary documents. Examples include:

- Security policies and manuals. If a PKI has a public CPS, it may offload some of the security sensitive details or voluminous minutiae about a PKI in security policy or manual.

- PKI Disclosure Statement ("PDS"). A PDS is a supplementary document instrument that provides a concise, "clear and conspicuous" framework to disclose and emphasize critical information about

the policies and practices of a certification authority, or an entire PKI, that is normally addressed in much greater detail by an associated CP or CPS. (See PAG Appendix 6 for more detailed information).

- Training, operational, installation, and user manuals. Manuals may explain operational procedures for performing PKI operations. For example, RA personnel may learn validation procedures from a manual given to them in a training process.

- Key management plans. A key management plan may contain critical detail about the protections used for hardware cryptographic modules and procedures for the secure generation, activation, deactivation, and destruction of CA private keys.

- Human resources guides and employee handbooks. These documents may be important supplements to an organization's trusted personnel policies. They may, for instance, describe background check procedures, procedures for periodic rechecking, and employee discipline in the event of untrustworthy behavior.

- E-mail policies. An organization may have an e-mail policy by which it imposes subscriber and relying party obligations on its personnel. It may also communicate standards for the protection of end-user private keys and data needed to activate private keys (such as passwords).

Appendix 4 (APP4): PKI Audit Methodology and Guidelines[493]

APP 4.1 PURPOSE

The purpose of this appendix is to define a framework of the standards for independent audits of PKI participants for the purpose of the accreditation of those PKI participant by accrediting bodies. Most commonly, the participants that have a business need to undergo an audit are CAs, although RAs, CMAs, repository services, and other participants may also have a need to be audited.

When digital signatures are used in a business transaction, the subscriber may be required to demonstrate to other parties in the transaction that techniques and associated operations used in the transaction satisfy certain due diligence and/or operational security requirements. An effective means of showing compliance with these requirements is through a third party audit report that addresses appropriate audit criteria. This Appendix 4 suggests a compliance audit framework that builds upon industry standards for CA controls.

APP 4.2 USERS OF THE AUDIT REPORT

The users of the audit report include, relying parties, subscribers, policy-adopting bodies, competent authorities, policy authorities, and operational authorities. The form of the audit report will depend upon the scope and purpose of the audit or other assessment, as discussed in the following sections.

APP 4.3 SCOPE OF AUDIT

The scope of the assessment is the review of the design and operational effectiveness of the controls of a PKI participant covering a specified period of time. The audit should be performed using appropriate audit criteria covering certification environmental, key management, and certificate life cycle management controls.[494] Such an audit is intended to assess whether the participant's implemented controls are effective and in accordance with the participant's defined business practices as articulated in one or more CPs, a CPS, and/or other supported policies and procedures.

The audit scope includes the certification practices and related controls that support a particular implementation of a given Certificate Policy and jurisdictional requirements. The focus of the report is on a participant's compliance with the CP, CPS, or other criteria. While there is a population of controls within a target participant that contributes to the overall reliability of a certificate, the users for a given certificate class may want to know whether a particular CP or CPS is being implemented as intended and functioning with sufficient effectiveness.

The scope of the compliance audit is defined by the requirements within the target CP or CPS. Thus, the compliance audit may apply to any participant or component in a PKI if addressed in the CP. In some cases, the focus may be solely on requirements imposed on the audited participant itself, and in others it may extend to

[493] The PKI Audit Methodology and Guidelines portion of the PAG is a work-in-progress product of the audit workgroup within the Information Security Committee. The principal authors of these DRAFT PKI Audit Methodology and Guidelines are Kevin Coleman (KPMG), Bill Dziadyk (DOMUS Security, LGS Group Inc.), Gene Ozgar (KPMG), Mark Lundin (KPMG) and Pat Cain (Genuity).

[494] *See* AICPA/CICA WebTrust, *supra* note 4, (provide a comprehensive set of control objectives (criteria) and recommended control procedures covering CA environmental controls, key management, and certificate life cycle management). *See* ANSI X9.79, *supra* note 486. The X9.79 control objectives and control procedures were developed using the existing body of domestic and international standards for information security, key management, and certificate management as inputs. The text of the PAG was also one of these inputs.

other participants in the PKI, such as subscribers and relying parties. The audit criteria would be customized to the scope of the audit.

Control areas typically covered in an auditof a CA include the following (customized to the particular circumstance):

CA Environmental Controls	Key Management	Certificate Life Cycle Management
CPS and Certificate Policy Management Security Management Asset Classification and Management Personnel Security Physical and Environment Security Operations Management System Access Management Systems Development and Maintenance Business Continuity Management Monitoring and Compliance Event Journaling	CA Key Generation CA Key Storage, Backup and Recovery CA Public Key Distribution CA Key Escrow (if applicable) CA Key Usage CA Key Destruction CA Key Archival CA Cryptographic Hardware Life Cycle Management CA-Provided Subscriber Key Management Services (if applicable)	Subscriber Registration Certificate Renewal (if applicable) Certificate Rekey Certificate Issuance Certificate Distribution Certificate Revocation Certificate Suspension (if applicable) Certificate Status Information Processing Integrated Circuit Life Cycle Management

The scope of the CA audit does not include directly assessing the degree of compliance of a Certification Authority's operations to rules and regulations that may have been issued by a governing jurisdiction (or Competent Authority). The CA Policy Authority is responsible for ensuring such rules and regulations are reflected in the selected or developed CP. The audit is then conducted to assess compliance to the CP.

APP 4.4 PHASES OF THE AUDIT

The typical phases in a CA compliance audit, in which a CA and its CPS will be audited for compliance with the requirements in a Certificate Policy, are as follows:

- **Planning Phase**.
- **Policy Assessment Phase**. Review of the written Certificate Policy relative to the RFC 2527 framework and the assessor's understanding of the intended Certificate Policy requirements in the context of the business and operational environment.
- **Certification Practice Statement (CPS) Review Phase**. Review of the suitability of design of certification practices to satisfy Certificate Policy requirements and generally accepted CA control standards.
- **Operational Effectiveness Verification Phase**. Testing of the operational effectiveness of the implemented certification practices.
- **Reporting Phase**.

Prerequisites for the CA assessment are:

- A threat and risk assessment (TRA) should be conducted by the CA.
- A documented Certificate Policy or equivalent document is required. Adherence of the Certificate Policy to the IETF RFC 2527 framework is recommended.
- A supporting Certification Practice Statement or equivalent document is required. Adherence of the Certification Practice Statement to the IETF RFC 2527 framework is recommended.

- A written assertion, by the operational authority is required, asserting that it has appropriately designed and implemented certification practices to reasonably achieve the requirements of the Certificate Policy and that such certification practices have operated with sufficient effectiveness, during some defined period of time.

APP 4.4.1 Planning Phase

During the Planning Phase, the assessor gains an understanding of the business model under which the CA domain operates. Other objectives of this phase are to:

- establish communication with the staff within the CA's operational and policy organizations and
- refine the scope of the assessment.

APP 4.4.2 Policy Assessment Phase

During the Policy Assessment Phase, the assessor will assess whether the target Certificate Policy itself is suitable for its intended purposes. The assessor, in carrying this prefatory phase, will base the analysis on the stated purposes of the Certificate Policy. The Certificate Policy will provide the assessor with an understanding of the business environment, the intended use and the related reliance on the certificates issued. The objective is to develop an understanding that is sufficient for the assessor to apply judgment about the appropriateness of the controls for satisfying the Certificate Policy requirements. The assessor should establish risk-based priorities for significant areas to be addressed during the following phases. Such risks may have been identified in a Threat and Risk Assessment (TRA). This can be accomplished by assessment of how specific Certificate Policy elements impact risks with respect to intended certificate use. (See Policy Assessment Phase audit program template in PAG APP 4, § 4.7.1 for a sample approach to applying IETF RFC 2527 framework considerations to this phase.)

APP 4.4.3 CPS Review Phase

During the CPS Review Phase, the assessor determines the degree of compliance of the operational authority's CPS with the target CPs. In addition, the assessor verifies that there are independent ratings of cryptographic modules or trusted products, if required by the CP. It is not intended that the CA's assessor would be required to have the skills and knowledge for rating trusted CA components. If required, cryptographic module ratings should precede the audit of the CA. The presumption is that the absence of a FIPS 140-1 (or equivalent) certification is cause for a qualified opinion from the assessor with respect to the functional accuracy of the cryptographic module. In such cases, the assessor will seek additional qualified assistance. (See CPS Review Phase audit program template in PAG APP 4, § 4.7.2 for mapping certification practices to policy requirements.)

APP 4.4.4 PKI Operational Effectiveness Verification Phase

During the Operational Effectiveness Verification Phase, the assessor confirms that the parties obligated to certain conduct under the target Certificate Policies and the Certificate Practice Statement are in fact in compliance with those obligations. Procedures to confirm compliance include:

- inquiry of management,
- inspection of documents and logs, and
- other confirmation of performance of controls.

The assessor derives suitable testing techniques to determine whether the target CP and CPS are adequately supported by operations, technology, and/or documentation with respect to requirements that are considered relevant to the audit (i.e. pass or failure of this point has bearing on the assessment report). These derived test requirements (DTR) use a combination of the following techniques:

- obvious (i.e., self-evident);
- validated by an inspection, as in documentation;
- validated by analysis, for those points that cannot be reasonably tested;
- validated by positive testing, the objective of which is to determine if a particular function works properly; and
- validated by negative testing, the objective of which is to attempt to create failures.

As some Operational Authorities or jurisdictions may require specific techniques for a DTR, it is suggested that the independent assessor maintain a table which notes which specific techniques are used to validate each DTR. (See PKI Operational Effectiveness Verification Phase audit program template in PAG APP 4, § 4.7.3.)

APP 4.4.5 Reporting Phase

During this final phase, the assessor prepares an Independent Assessor's Report and briefings to PKI operational and policy authorities.

APP 4.5 AUDIT CONSIDERATIONS

APP 4.5.1 Form of Audit Report

The form of the audit report is one of attestation to third parties.

The CA Operational Authority asserts to its Policy Authority, subscribers, and relying parties that:

- it has appropriately designed and implemented certification practices to reasonably achieve the requirements of the Certificate Policy; and
- such certification practices have operated with sufficient effectiveness, during some defined period of time, to achieve the requirement of the CP.

The assertions of the operational authority of the CA, supported by the CPS, are made in writing to the independent assessor and to any higher-level policy authorities, regulatory bodies, etc. An assertion by management is important because it establishes that the operational authority is solely responsible for the operation of its certification practices in such a manner that the requirements of the CP are achieved.

The assessor will typically express a conclusion about the reasonableness of the assertions made by the Certification Authority. Said another way, the assessor expresses an opinion regarding the design, implementation, and operational effectiveness of the controls and practices supporting the CP. (See example report below.)

Other Communications with the Operating Authority or Policy Authority. In addition to supporting the audit opinion, the assessor's observations about policy assessment, practice design, and operational effectiveness can provide valuable feedback to operational or policy authorities for enhancing service quality.

The assessor may wish to communicate such significant observations about control deficiencies or other opportunities for process improvement. This communication should be separate from the audit report. It may be in the form of a letter for sole use of the operational authority or policy authority, stating finding and recommendations. It also might be in the form of a presentation describing findings, potential impact and recommendations.

APP 4.5.2 Timing of the Audit and the Report

Audits may be performed when an operational authority commences use of a Certificate Policy, or may be performed at some other point during the life cycle. Generally the frequency of the audit is established by the Certificate Policy. If the frequency of the audit is not established by the Certificate Policy:

- the frequency could be based upon the frequency of a threat and risk assessment (TRA) lifecycle; or
- the users of the audit report may determine the audit frequency.

To be useful, reports should cover a meaningful period of time and be issued at some reasonable interval during the policy life cycle. The policy authority is responsible for ensuring that the length of reporting period and frequency of assessment are in accordance with contractual, regulatory, and other higher level requirements. These audit requirements would be incorporated into the CP.

Relationship to other audits such as regulatory, financial or internal. As public key infrastructures develop, the audit requirements and process will take into account and define how regulatory, financial, and internal audit reports may be related. As the specific definitions of these reports are created and accepted by industry, the impact of these reports on the nature, timing, and scope of the independent audit should be assessed.

The assessor should consider the extent to which internal audit activities may be relied upon to modify the nature, timing and extent of test work performed by the assessor. If reliance on internal audit is planned, the assessor should determine:

- the competence and objectivity of internal audit; and
- the extent to which the internal audit activities cover the specific certification practices of interest.

APP 4.6 REFERENCES AND AUTHORITATIVE BODIES

In determining the suitability of certification practices and the effectiveness of the operation of those certification practices in achieving the Certificate Policy, the assessor shall consider generally accepted control principles, which may apply to certification authority operations. The related body of knowledge may include:

- AICPA/CICA WebTrust Program for Certification Authorities;
- ANSI X9.79 PKI Practices and Policy Framework;
- Institute of Internal Auditors' Systems Auditability and Control Report;
- Information Systems Audit and Control Association's Control Objectives for Information and Related Technology (CObIT);
- Common Criteria;
- Other NIST or equivalent publications; and

- IETF PKIX Standards.

As technology and practice in this area is still maturing, the common body of knowledge is still growing and the reader is encouraged to forward comments, additions, and suggestions to the authors.

APP 4.7 CONDUCT OF THE AUDIT

The audit should be performed in accordance with generally accepted auditing standards as defined by such documents as the American Institute of Certified Public Accountants' Statements on Auditing Standards and the Institute of Internal Auditors' Standards for the Professional Practice of Internal Auditing.

The assessor should consider the community and the applicability of the Certificate Policy in considering the nature, timing, and extent of testing procedures to be performed during the audit.

Audit program considerations vary with the requirements of the underlying Certificate Policy and community of trust. The following are examples of templates for the substantive phases of the compliance assessment.

APP 4.7.1 Policy Assessment Phase – Sample Audit Program Template

PKIX Policy / Practice Definition	Certificate Policy Element	Observations
4.3……	……	
4.4.1 Certificate Application Used to state requirements regarding subject enrollment and request for certificate issuance.	4.1 Certificate Application Applicants for a certificate shall complete the following procedures for each certificate application: ▪ Determine a proposed distinguished name; ▪ Generate a key pair; ▪ Protect the private signature key of this key pair from compromise; ▪ Submit a certificate application to the CA or LRA; and, ▪ Demonstrate to the CA or LRA that they have a functioning key pair.	[It may be necessary to communicate observations on policy in case of: ▪ Misalignment with RFC 2527 framework and definitions ▪ Inappropriateness of the Certificate Policy, given the assessor's understanding of the PKI's trust requirements This column is also used for highlighting of inherent risks to be addressed in subsequent audit phases.]
4.4.2…….	…….	

APP 4.7.2 CPS Review Phase – Sample Audit Program Template

Certificate Policy Element	Related Certification Practice Element	Observations
2.6.1……	……	
2.6.2 General Provisions/ Publication and Repositories/ Frequency of Publication Certificates shall be published promptly upon issuance. CRL publication shall be in accordance with Section 4.4.6. Newly approved versions of this Certificate Policy and the CA's Certification Practice Statement shall be published promptly.	2.6.2 General Provisions/ Publication and Repositories/ Frequency of Publication Certificates issued by the XYZ CA are published immediately upon issuance. When revoked, certificates are published in CRLs, which are created and published in the X.500 directory every twenty-four (24) hours. New versions of the supported Certificate Policies and this Certification Practice Statement are loaded promptly to the XYZ CA's Web site as per secure update procedures and in accordance with the practices described in Section 8.	[Describe whether the certification practices are suitably designed to meet the Certificate Policy requirements.]
2.6.3…….	……	

APP 4.7.3 Operational Effectiveness Verification Phase – Sample Audit Program Template

Certification Practice Element	Test Work and Observations
2.6.1……	
2.6.2 General Provisions/ Publication and Repositories/ Frequency of Publication Certificates issued by the XYZ CA are published immediately upon issuance. When revoked, certificates are published in CRLs, which are created and published in the X.500 directory every twenty-four (24) hours. New versions of the supported Certificate Policies and this Certification Practice Statement are loaded promptly to the XYZ CA's Web site as per secure update procedures and in accordance with the practices described in Section 8.	[Documentation should be adequate to describe the nature, timing and extent of test work and the results. Observations are about whether the certification practices are operating effectively.] Auditor selected log entries from 15 days throughout the period and noted that CRLs were created and published at least every 24 hours in each case.
2.6.3……	

The assessor would consider any exceptions or deficiencies, along with other test work and results from other audit areas, in determining the overall opinion about the compliance audit. In addition to the audit report opinion, significant findings may be communicated to the operational or policy authority in separate correspondence to facilitate process improvement.

APP 4.8 EXAMPLE AUDITOR'S REPORT AND MANAGEMENT ASSERTION

The following are examples of a management assertion and independent auditor's report where the CA audit is performed using the WebTrust Principles and Criteria for Certification Authorities. The format and contents of the assertion and report are based on the AICPA's attestation standards. In this example, the report is intended for broad distribution (e.g., through posting on the CA's web site).

The sample report and assertion could be modified for particular circumstances such as:

- to reflect a different or limited scope (e.g., external RA operations);
- to indicate that its distribution is limited to certain parties (e.g., the Policy Authority and CA management);
- to indicate compliance with the relevant criteria without broadly disclosing the CA's CPS;
- to indicate compliance with other criteria (e.g., specific CP requirements); or
- to reflect local reporting requirements and standards.

APP 4.8.1 Example Audit Report

Report of Independent Certified Public Accountant

To the Management of ABC Certification Authority, Inc.:

We have examined the assertion by the management of ABC Certification Authority, Inc. (ABC-CA) that in providing its Certification Authority (CA) services at LOCATION, ABC-CA, during the period from DATE through DATE— [495]

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly authenticated (for the registration activities performed by ABC-CA); and
  - The integrity of keys and certificates it managed was established and protected throughout their life cycles.
- Maintained effective controls to provide reasonable assurance that:
  - Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;

[495] The bullet points represent the WebTrust for Certification Authorities Principles - CA Business Practices Disclosure, Service Integrity (including key and certificate life cycle management), and CA Environmental Controls. These high level principles are supported by the detailed WebTrust for Certification Authorities Criteria and the CA's disclosed business practices (CP and CPS).

- The continuity of key and certificate life cycle management operations was maintained; and

- CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities Criteria.[496]

ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly, included (1) obtaining an understanding of ABC-CA's key and certificate life cycle management business and information privacy practices and its controls over key and certificate integrity, over the authenticity and privacy of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over development, maintenance and operation of systems integrity; (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business and information privacy practices; (3) testing and assessing the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, for the period DATE through DATE, ABC-CA management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the AICPA/CICA WebTrust for Certification Authorities Criteria.

Because of inherent limitations in controls, errors, or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to assess the effectiveness of controls at individual subscriber and relying party locations.

The WebTrust seal of assurance for Certification Authorities on ABC-CA's Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.[497]

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust for Certification Authorities Criteria, nor the suitability of any of ABC-CA's services for any customer's intended purpose

[Name of CPA firm]
Certified Public Accountants
[City, State]
[Date]

[496] *See* AICPA/CICA WebTrust, *supra* note 4; *see also* ANSI X9.79, *supra* note 486. The WebTrust for Certification Authorities Criteria are based on ANSI X9.79 and address the CA environmental, key management, and certificate life cycle management control topics listed in the assertion that follows and Section C - Scope of Audit.

[497] This and the following paragraph are only applicable if the CA desires to display the "WebTrust Seal" on its web site after successfully completing the audit with an unqualified opinion.

APP 4.8.2 Example Management Assertion

Assertion of Management as to its Disclosure of its Business Practices and its Controls Over its Certification Authority Operations during the period from DATE through DATE

[Date]

ABC Certification Authority, Inc. operates as a Certification Authority (CA) known as ABC-CA. ABC-CA provides the following certification authority services:

- Subscriber key management services (if applicable)
- Subscriber registration
- Certificate renewal (if applicable)
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate suspension (if applicable)
- Certificate status information processing
- Integrated circuit card life cycle management

Management of ABC-CA is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls can provide only reasonable assurance with respect to ABC-CA's Certification Authority operations. Furthermore because of changes in conditions, the effectiveness of controls may vary over time.

Management has assessed the controls over its CA operations. Based on that assessment, in ABC Certification Authority, Inc. (ABC-CA) Management's opinion, in providing its Certification Authority (CA) services at LOCATION, ABC-CA, during the period from DATE through DATE—

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly authenticated (for the registration activities performed by ABC-CA) and
  - The integrity of keys and certificates it managed was established and protected throughout their life cycles

- Maintained effective controls to provide reasonable assurance that:
    - Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
    - The continuity of key and certificate life cycle management operations was maintained; and
    - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

based on the AICPA/CICA WebTrust for Certification Authorities Criteria including the following:

CA Business Practices Disclosure

Service Integrity

Key Life Cycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Escrow (if applicable)
- CA Key Usage
- CA Key Destruction
- CA Key Archival
- CA Cryptographic Hardware Life Cycle Management
- CA-Provided Subscriber Key Management Services (if applicable)

Certificate Life Cycle Management Controls

- Subscriber Registration
- Certificate Renewal (if applicable)
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension (if applicable)
- Certificate Status Information Processing

- Integrated Circuit Card Life Cycle Management

CA Environmental Controls

- Certification Practice Statement and Certificate Policy Management
- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- Systems Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Event Journaling

[Name]

[Title]

Appendix 5 (APP5): Proposed Guidance for Development of Compatible End-User Product

APP 5.1 SCOPE

Technical standards-makers and regulators have focused great attention on articulating PKI service and product requirements. Nonetheless, as a practical matter, end-user software utilizing PKI may present substantially greater risks to end-users, and yet it largely has not benefited from widely recognized guidance or requirements. Consequently, this appendix has been developed to respond to this lack of guidance.

This section provides guidance to developers and deployers of browsers, "plug-ins," and other end-user ("client") software utilizing PKI, to allow them to satisfy guidelines and policies described in the PAG. It also provides a checklist for the assessment of such end-products. Although this guidance is focused on end-user/client software, the guidance is also applicable to server implementations.

Please keep in mind that this guidance must be considered in the context of reasonableness and appropriateness based on the requirements of the particular transaction or communication. In practice, security of PKI-enabled software should reflect the attendant risks of the transactions for which it is deployed. Finally, please note that because this is a particularly new area of consideration, it will invariably evolve rapidly. Thus, this appendix will be updated from time-to-time.

APP 5.2 INTRODUCTION

Browsers and other end-user software utilizing PKIs shall be robust enough to provide for secure transactions, and for the secure management and operation of those transactions, including, as appropriate, security policy specifications for its use.

Essential to the secure management of a public-key infrastructure is ease-of-use and clarity of obligations for all participants. To achieve them, this appendix considers three areas of concern: management, functionality, and standards conformance.

APP 5.3. MANAGEMENT

The management area is defined to cover enrollment, configuration, training, documentation, and maintenance.

APP 5.3.1 Policy regime

Definition. A policy regime is defined to be the collection of operational configurable options that allow the pre-setting of such things as selection of acceptable algorithms and key sizes, certificate policies, acceptable authority public keys (e.g., pre-loaded or embedded root certificates) appropriate business applications,requirements for the protection ofend-user subscriber private keys, acceptable key storage provisions, etc. In some applications, it may be necessary to specify these parameters on an application-by-application, or even transaction-by-transaction basis, depending on the risk.[498]

[498] For example, honoring a purchase requisition for a box of pencils may involve such comparatively little risk that no constraints on acceptable key sizes, certificate issuers or roots, etc. may be required. On the other hand, a purchase order for a $1 billion dollar supertanker would presumably require the most stringent of policy controls, yet conceivably both requisitions could be processed by the same software.

If required by the policy regime, the software shall be capable of supporting separation of duties between different end-users, between management and end-users (and classes of management and end-users). When the software permits a user to hold more than one certificate, it shall permit the designation of a default certificate for appropriate usages, e.g., for encryption, digital signatures, and/or authentication.

If policy regimes are enforced by the software and the end-user attempts to obtain or use a key pair or certificate (either by enrollment or by importation) that would be inconsistent with the policy regime, then the certificate request shall be rejected.

The software shall make available, or provide links to acceptable certificate policies or CPSs of CAs which are included (or subsequently authorized) in an approved list supplied with the software or otherwise provided by the community of interest.

The software shall permit the removal and addition of authority certificates from the approved certificate authority list in a trustworthy fashion.

APP 5.3.2 Key generation, storage, and use

Where the end-user is responsible for generating key pairs or data encryption keys, either in software or hardware, the software or hardware shall do so in a trustworthy fashion in accordance with applicable standards and policy. In the event the private key is generated outside of, or can potentially be extracted from, a suitable tamper-resistant device, appropriate mechanisms must be provided to ensure that the key is not compromised while in storage. These mechanisms may include the use of Personal Identification Numbers (PINs), passwords, biometric devices, etc. In order to ensure that such access does not remain "live" when the authorized user is not in attendance and control, timeout mechanisms may be required.

Because both hardware devices and software routines are invariably invoked and controlled by higher level routines that may not be under the direct control of the user, there is the possibility that a device or routine could be used to sign something other than what the user intended, e.g., to sign two items when only one was requested, etc. For this reason, it may be desirable that the actual usage of private keys for signature or decryption be audited at the lowest possible level, e.g., by a hardware device such as a smart card itself, so that what was requested can be compared to what was actually signed. Alternative approaches, such as only performing one signature operation per manual insertion or activation of the card or token, enforced by the card or token itself, may be required. This may be particularly important in an unknown or potentially hostile environment, such as a point of sale terminal, publicly-accessible kiosk, or other application not directly controlled by the end-user.

End-user applications shall implement and enforce restrictions imposed on private key usages in a trustworthy manner, in accordance with relevant standards and policies.

APP 5.3.3 Transportability

Where the software provides a facility for private key portability, it shall be done in a secure and straightforward fashion (because users are otherwise unlikely to perform the function correctly).

Systems importing or exporting private keys shall ensure that the protective measures of the source are at least as secure as the destination, and vice versa.

APP 5.3.4 Revocation

The software shall allow a user (or delegated authority) to request revocation of an end-user's certificate in a secure manner. Upon revocation of the certificate, the software shall remove the revoked certificate from active use in accordance with applicable policy.

Independent of any certificate revocation, the software should allow a user to reliably destroy (zeroize) any private keys under his or her control, for example to ensure that no further signature operations are carried out with that key, or to prevent data encrypted with that key from ever being read, following expiration of the key usage period.

APP 5.3.5 Multi-user systems

If the software accommodates the private keys of multiple users, then it shall provide secure storage, isolation, and access controls for each user's information.

APP 5.3.6 Documentation

Available product documentation shall disclose and discuss the security implications of the use of all configurable options.

APP 5.3.7 Audit trail

The software shall be capable of maintaining an audit trail evidencing transactions, certificates, and revocation information in accordance with applicable policy. Such information may be of particular use to internal auditors within the end-user subscriber's organization or external auditors assessing the trustworthiness of a PKI that includes the subscriber.

APP 5.4 FUNCTIONALITY

APP 5.4.1 Functional correctness

- The software shall accurately do what it purports to do, and only that, and be verifiable in its conformance with this guidance.[499]
- The software shall be designed to assure a reasonably secure state commensurate with the attendant risk.
- In the event of software failure, the software's failure routines should minimize data loss, minimize disruption to the operating system and other applications running concurrently, and maximize the ability to recover control following the failure.

APP 5.4.2 User authentication

The software shall be capable of providing trustworthy user authentication for secured PKI functions. For example, this may include strong password selection, multi-factor authentication, and trusted path.

[499] Consider who is presenting the threat or risk? Is it the user himself? The administrator who installed the software? The vendor? And who is going to perform the verification, and ensure that the system was installed properly?

The software shall support the secure administration of PKI-related user authentication functions.

APP 5.4.3 Incomplete transactions

The software shall be capable of displaying and recording the cause, date, and time of incomplete transactions, such as rejected transactions, sender/certificate name mismatch, and non-conformance with the applicable policy.

APP 5.4.4 Policy regimes

Where policy regimes are configurable, the software shall assure that the security to be applied to a transaction is consistent with the policy regime. For example, the software shall be capable of informing an end-user that a received certificate does not conform to the selected policy regime.

APP 5.4.5 Operational information

APP 5.4.5.1 Message status

The software shall be capable of indicating whether messages have been digitally signed and/or encrypted or whether communication channels are authentic and confidential, in accordance with applicable policy regime.

The software shall be capable of displaying the validation status (e.g., not performed, signature verified, certificate valid) for an end-user certificate before its use by a relying party.

The software must be capable of identifying which information in the transaction is required to be signed or verified. The software shall be capable of indicating which algorithm and which certificate (if any) is associated with each signed and/or encrypted communication.

APP 5.4.5.2 Certificate content

The software shall be capable of displaying certificate content, including X.509 version 3 extensions. The names of fields shall be in readily understandable language.

APP 5.4.5.3 Certificate status

The software shall be capable of displaying, in readily understandable language, the precise terms and conditions for the use of any selected certificate. (e.g., if any limitations on liability, allowed/prohibited uses, etc.).

APP 5.5 STANDARDS CONFORMANCE

The software should adhere to the guidance of this PAG and other applicable standards, and assure that policy declarations cannot be bypassed.

It is strongly recommended that certificate processing systems adhere to ITU X.509 and IETF/PKIX 2459 because if processing (e.g., certificate path processing) is performed incorrectly, the finest certificates in the world can do no good.

As systems mature, the use of ancillary services, such as date-stamping, key recovery, etc. will need to be reflected in this section.

Appendix 6 (APP 6): PKI Disclosure Statement (PDS)

Certificate policies (CPs) and certification practice statements (CPSs) are generally very detailed documents containing complex legal and technical information. Although such a large amount of complex terms and expressions may be essential to ensure the proper operation, legal certainty, and full disclosure within a public key infrastructure (PKI), many PKI users, especially consumers, are likely to find these documents difficult to read, let alone comprehend. Consequently, there is often a need for a supplemental and simplified instrument to assist PKI users in making informed trust decisions. In response, members of the International Chamber of Commerce (ICC), in an informal cooperative effort with the Information Security Committee of the American Bar Association and other groups, developed a draft PKI Disclosure Statement (PDS). A PDS is a supplementary document that provides a concise, "clear and conspicuous" framework to disclose and emphasize critical information about the policies and practices of a certification authority, or a PKI, that is normally addressed in much greater detail by an associated CP or CPS.[500]

A PDS is not meant to substitute for a fully detailed CP, although, strictly speaking, a PDS may satisfy the strict X.509 requirements in order to qualify as a certificate policy.[501] As such, a PDS may function as a substitute for a larger CP in some limited situations, for example, when a relying party needs to decide quickly if it will rely on a previously unfamiliar CA's certificates, or when a CA wishes to conform simultaneously with more than one CP (*e.g.*, when a CA wishes to participate in more than one "community of interest" by having its certificates accepted by the relying parties of one or more other CAs, and the CAs have not previously coordinated their CPs, and the CA in question does not necessarily want to (or cannot) amend its larger CP to resolve minor differences with the other CA's CPs).

The model PDS below provides structure and categories (but not substantive provisions) defining a harmonized set of statement types that would be contained in a deployed PDS. Each CA or PKI would draft substantive provisions to appear in its implementation of the PDS.

The following table represents the PDS categories, listing a section for each defined *statement type* (category) and a corresponding *descriptive statement* that may include hyperlinks or computer references to the relevant CP or CPS sections.

Table 1 - Contents of the PDS

STATEMENT TYPES	STATEMENT DESCRIPTIONS
CA contact information:	**The name, location and relevant contact information for the CA.**
Certificate type, validation procedures, and usage:	**A description[502] of each class/type of certificate issued by the CA[503,] corresponding validation procedures,[504] and any restrictions on certificate usage.[505]**

[500] *See* ETSI Signature Standard, *supra* note 317 at 38-39. (The PDS has also been included as a formal annex.)

[501] X.509 defines a certificate policy as: "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements." *See* RFC 2527, *supra* note 193.

[502] This description can include the corresponding certificate policy object identifier that must also be included in the certificates.

[503] Alternatively, there can be separate PDSs for each type or class of certificate.

[504] This statement may simply reference the X.509 certificate processing rules.

[505] This statement may include the requirements to qualify as a subscriber or relying party and any restrictions on the applications for which the certificates are approved to be used.

Reliance limits:	**The reliance limits, if any.**
Obligations of subscribers:	**The description of, or reference to, the critical subscriber obligations.**[506]
Certificate status checking obligations of relying parties:	**The extent to which relying parties are obligated to check certificate status, and references to further explanation.**[507]
Limited warranty & disclaimer/Limitation of liability:	**Summary of the warranty,**[508] **disclaimers, limitations of liability, and any applicable warranty or insurance programs.**
Applicable agreements, Certification Practice Statement, Certificate Policy:	**Identification and references to applicable agreements, CPS, or CP.**[509]
Privacy policy:	**A description of and reference to the applicable privacy policy, if any.**
Refund policy:	**A description of and reference to the applicable refund policy, if any.**
Applicable law and dispute resolution:	**Statement of the choice of law and dispute resolution mechanism.**
CA and repository licenses, trust marks, and audit:	**Summary of any governmental licenses, seal programs, a description of the audit process**[510] **and, if applicable, the audit firm.**

[506] This statement may include the requirement to protect the confidentiality of the subscriber's private key and report actual or suspected compromise or change of material circumstances.

[507] This statement may include the requirement to protect the integrity of the CA's public key, and, optionally, including instructions for retrieving certificates issued by the CA.

[508] This statement may include whether the CA warrants the accuracy of the information contained in the certificate.

[509] A disclosure of the applicable CP is appropriate particularly if the PDS is simply a subset of the terms from the CP.

[510] This statement may include a reference to the current specific audit report.

Appendix 7 (APP 7): PKI and XML

One of the challenges of a PKI is the exchange of information among systems and individuals inside and outside that PKI. XML was developed to provide a structural methodology for the exchange of this type of information. More specifically, XML was designed to provide a simplified method for creating base vocabularies that have particular use in their industry or domain. The set of terms that are defined in the vocabulary, collectively called a syntax or grammar, allow the exchange of information without having prior knowledge of the format of the stored information. For example, an XML document that requests the first name of a user may flag the field "FirstName." Thereafter, a page that receives this XML information could merely include the command to display "FirstName" and the value entered in that field would be displayed. Thus, the information could be reformatted, altered, changed, searched, or hidden depending on the context, purpose, user authorization, or other variables.

In this regard, XML has much to offer in the creation, exchange, and assessment of PKI-related documents, such as subscriber agreements, disclosure statements, CPs, CPSs, and the host of other documents that must be exchanged among the actors in a PKI. There are two primary reasons why XML is advantageous in this setting. First, XML recognizes the concept of a "document." In other words, XML provides more than just a "stream of bits," but rather it provides for a structured package of information that can be exchanged as a whole, or in its logical sections. This structure provides opportunities for reformatting information for a particular audience depending on its needs or interests. For example, a user may only want to see those portion of the CPS related to their particular certificate or certificate service. The ability to focus on information of interest insures that the information is formatted in a manner that promoted clarity and relevance in communications.

Second, although XML is useful for structuring documents that are intended to be read by human beings, its real value is found in the structuring of documents for "reading" by computers. Consequently, XML provides a standardized method for exchanging PKI-related documents in one format that can be universally understood by both humans and computers. For example, the portion of the CPS related to verification procedures could have separate defined terms for different aspects of the verification description in a CPS. If both parties have previously agreed upon shared grammar, the parties could exchange information using the terms of the grammar rather than requiring prior knowledge of the specific layout or location of that information. This greatly enhances the opportunities for automation and interoperability between PKI providers.

In sum, XML creates a number of possibilities for facilitating PKI interoperation and assessment, such as:

- using software tools that automatically compare the CPSs of different PKIs section by section, and flag important sections for review by an assessor in accordance with the priorities and preferences of the reviewer,
- preparing different "views" of a PKI policy document "on-the-fly" for different assessment needs,
- facilitating agreement on contractual terms among PKI actors,
- integrating PKI-related policies and agreements into the certificate enrollment process, while maintaining separation between software and policy, and
- automating the creation and review of PKI-related documents.

In the implementation of digital signatures for XML, the working group of the W3C has encountered difficulties in the representation of certificate chains, because most PKI standards work predated XML and consequently PKI standards do not share a common syntax with XML. Thus, the next step in successfully implementing XML in this setting is the creation and support for a syntax that can be adopted by other PKI providers. As a result, it is not yet clear whether XML can successfully provide an adequate level of support for applications that employ certificates equal to the usefulness demonstrated today for encryption and hash algorithms involved

in digital signatures. It is recommended that assessors familiarize themselves with XML, to the extent that the assessed PKI incorporates XML, and also that assessors investigate opportunities for the use of XML to facilitate PKI assessment.

Appendix 8 (APP 8): PKI Assessment Examples

This appendix provides examples of current assessment schemes for PKI systems. The following schemes are described:

1. State of Washington PKI licensing
2. United Kingdom (UK) tScheme initiative
3. Australia's Government PKI Initiative (GPKI), or Gatekeeper strategy

APP 8.1 STATE OF WASHINGTON PKI LICENSING

This information is derived from the Washington State website on Electronic Authentication, located at <http://www.secstate.wa.gov/ea/default.htm>.

Under Washington State's Electronic Authentication Act (EAA), the state of Washington licenses private businesses to issue and verify digital signatures. The Office of the Secretary of State administers the certification and operating standards set forth in the law and issues licenses to the following two types of entities:

- Certification Authorities. A certification authority, or CA, is the person or company who issues digital certificates to subscribers. CAs act as a "trusted third party" certifying the identity (and/or other attributes) of the subscriber to anyone who receives a digitally signed message or who other relies on the binding between the subscriber and the public key contained in the certificate. In order to obtain a license, a CA must submit the following:

    1. A completed application, along with the required application fee;
    2. A copy of the applicant's CPS;
    3. An audit report, from a qualified auditor, stating that the applicant's computer systems comply with Washington's standards for trustworthy systems (currently this means being in agreement with the recommendations contained in NIST publication NISTIR 6462);
    4. A list of current, certified operative personnel; and
    5. A surety bond, or other appropriate suitable guarantee, in the amount of $50,000.00.

- Operative Personnel. Operative personnel are people employed by certification authorities who perform sensitive duties for a certification authority or repository. Typically, these are people who maintain the systems, issue certificates, or establish certification policies. In order to be licensed, individuals must submit:

    6. A completed application, along with the required application fee;
    7. Satisfactory completion of the required operative personnel exam;
    8. A background check report from the Washington State patrol; and
    9. A background check report compiled by a private provider.

Additionally, the state 'recognizes,' as opposed to licenses, repositories of digital certificates. Recognition of repositories is done in connection with licensure as a CA. The materials submitted for the CA license are reviewed in order to provide repository recognition. If recognition of a repository is desired, the CA sends a cover letter stating that fact and includes the appropriate recognition fee.

APP 8.2 TSCHEME

tScheme is a UK initiative that is an example of a stakeholder-led, self-regulatory scheme. Such schemes are non-statutory and aim to provide credible and effective systems and procedures for the approval of electronic trust services. tScheme is an independent not-for-profit company, limited by guarantee, with its own staff. The following section provides a brief overview of tScheme.[511]

tScheme approves services. These services will be approved against pre-defined profiles. Profiles define the service type (e.g., registration, certificate issuance, key generation), and set minimum criteria for organizational fitness, appropriate technology and procedures, and other elements.

A service provider wishing to have a service approved by tScheme goes through the following steps:

1. Submits a "Self Declaration" to tScheme,
2. Provides supporting evidence,
3. Provides information on other applicable approvals (e.g., FSA, Oftel, BS7799),
4. Submits to an independent audit against the profile,
5. If successful, submits the audit report to tScheme for approval, and
6. Enters into a contractual commitment regarding the approval and use of the tScheme mark.

A tScheme Approval covers a specific service operated by an organization. Not all services the organization offers must be approved, but separate approvals must be sought for individual services. Figure 8-2, below, illustrates the tScheme Approvals process:

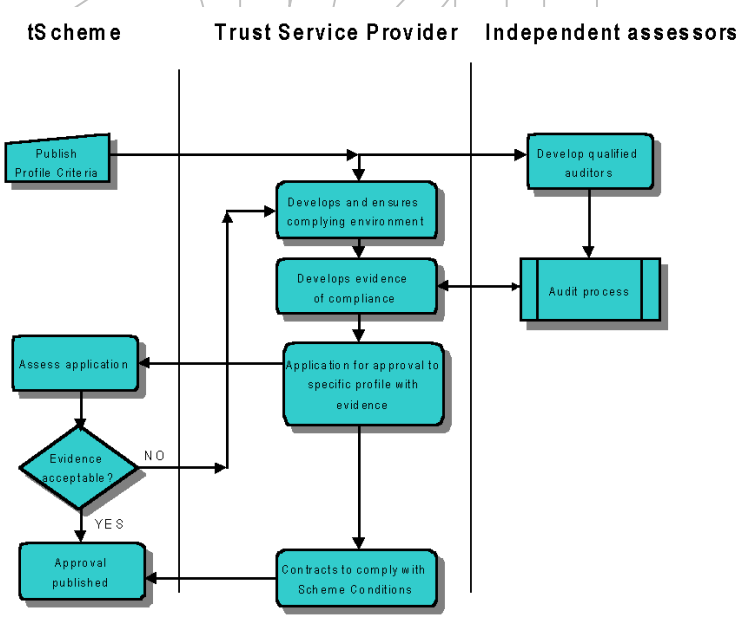


Figure 8-2: tScheme Approval Process

[511] A complete explanation of tScheme and its approach to PKI assessment is *available at* <http://www.tscheme.org.uk>.

APP 8.3 GATEKEEPER

In May 1998 the Australian Government issued a report GATEKEEPER A strategy for public key technology use in the Government.[512]

The scope of the Government Public Key Infrastructure (GPKI), or Gatekeeper, and how agencies may use public key technology in providing services to their customers is limited to an Australian national infrastructure, specifically:

- Commonwealth government intra- and inter-agency use; and
- interaction between agencies and the Australian public.

Three major groups are identified within the GPKI:

- CAs;
- agencies delivering applications online; and
- users.

Gatekeeper allows for a number of classes of certificates that are based on the purpose for which they are to be used. The classes are:

Type 1 - Individual certificates

- Grade 1 Non sensitive information with no financial implications;
- Grade 2 IN CONFIDENCE information, individual transactions up to $1,000; and
- Grade 3 PROTECTED/RESTRICTED information, individual transactions up to $10,000.

Type 2 - Non-individual certificates

- Grade 1 Non sensitive information, individual transactions up to $10,000;
- Grade 2 IN CONFIDENCE information, individual transactions up to $10,000 maximum $100,000; and
- Grade 3 PROTECTED/RESTRICTED information, individual transactions up to $10,000 maximum $100,000.

The Gatekeeper Accreditation Certificate (GAC) Accreditation criteria for certification authorities were released in December 1998.[513] The criteria include:

- compliance with Commonwealth Government procurement policy;

[512] *See* PAG APP 2 (*Gatekeeper: A Strategy for Public Key Technology Use in Government*, Office of the Gov't Information Technology, Australia (1998), *available at* <http://www.govonline.gov.au/publications/GatekeeperStrategy.pdf> hereinafter "Gatekeeper Strategy").

[513] *See* Gatekeeper Criteria, *supra* note 33.

- security policy and planning;
- physical security;
- technology evaluation;
- Certification Authority policy and administration;
- personnel vetting;
- legal issues; and
- privacy considerations.

The criteria are evaluated by organizations approved by the National Office for the Information Economy.

Interoperability within the Australian Government Certificate Infrastructure (AGCMI) is to be achieved via the Gatekeeper Accreditation Certificate (GAC).[514] The GAC is intended to be a central "trust point" for the Commonwealth and other jurisdictions or PKI schemes that may wish to accept it, but is NOT intended to be a national root certificate.

A recent initiative is the ABN-DSC (Australian Business Number - Digital Signature Certificate), which is being developed by the Australian government, in partnership with States/ Territories and in co-operation with the private sector, to facilitate the development of e-commerce in Australia; speed the evolution of government online services to business; and help cut the "red-tape" compliance cost burden small business often have to face in dealing with government.

[514] *Id*.

Appendix 9 (APP 9): Industry-Specific Supplements to the PAG

The subsections of this appendix provide industry-specific resources as supplements to the PAG for the following sectors: Financial Services and Healthcare.

APP 9.1 PKI AND INFORMATION SECURITY ISSUES FOR FINANCIAL SERVICES

Preface

Financial service regulators have long warned of the threats to electronic information, but have been especially prolific in recent months, issuing dozens of guidelines and risk analyses relating to information security. In addition, 1999's Gramm Leach Bliley Financial Service Modernization Act spawned a slew of privacy and security regulations. This appendix provides references that assessors, accreditors, or evaluators in the financial service industry may find useful when crating, designing, implementing or examining public key infrastructure systems. The references in this appendix include: short letters adequately described by their titles as well as some summaries of more substantive releases including statements from the International Committee on Banking Supervision, the Federal Financial Institutions Examination Council's (FFIEC) Risk Management Statements, which that arose from financial modernization, and policy statements from the major United States federal financial services regulators.

1. Standards bodies and standards (existing and proposed)

American National Standards Institute

Standards for the financial services industries, including the American Bankers Association, developed by the American National Standards Institute, Accredited Standards Committee, X9 (ANSI ASC X9). ASC X9 is the national standards-setting body for the financial services industry and is accredited by the American National Standards Institute (ANSI). ASC X9 is the only industry-wide forum that brings together bankers, securities professionals, manufacturers, regulators, associations, consultants and others in the financial services arena to address technical problems, find the best solutions and codify them as nationally accepted standards. ANSI accredited ASC X9 in 1984. The American Bankers Association serves as ASC X9 secretariat, providing administrative support.[515] Numerous PKI-related standards documents are available at the following URL <http://webstore.ansi.org/ansidocstore/dept.asp?dept_id=80>, including:

ANSI X9.24, X9.30, X9.31, X9.42, X9.45, X9.52, X9.55, X9.57, X9.62, X9.69, X9.71 (discussing key generation, digital signature and encryption algorithms; key and certificate management; certificate and key management extensions);

X9.68-2xxx WD, Digital Certificates for Mobile/Wireless and High Transaction Volume Financial Systems: Part 2: Domain Certificate Syntax; and

X9.79, Public Key Infrastructure (PKI) Practices and Policy Framework, Date of Publication: September 2000

ANSI x9.79, PKI Practices and Policy Framework, defines the components of a financial services PKI and sets a framework of practices and policy requirements. It defines the operational practices relative to industry-accepted information systems control objectives and supporting control procedures. PKI users implementing this standard can support multiple policies that incorporate the use of digital signature technology (cost, $40).
<http://webstore.ansi.org/ansidocstore/product.asp?sku=ANSI+X9%2E79%2D2001>

[515] *See* <http://www.x9.org>.

2. International Organizations

2.1 Basel Committee on Banking Supervision

The Basel Committee was comprised in 1974 by the central-bank Governors of the Group of Ten countries with the charge of reporting "best practices" to the central bank governors). <http://www.bis.org/bcbs/aboutbcbs.htm>.

May 2001 - Risk Management Principles for Electronic Banking

> This document recommends tailoring standard bank risk practices to suit electronic banking. The Committee discusses bank board and management oversight, security controls and legal and reputational risk management. *See* <http://www.bis.org/publ/bcbs82.htm>.

January 2001 - Customer Due Diligence for Banks

> This document sets forth guidance for banking supervisors to use in reviewing the controls and procedures of banks to ensure they are not used for criminal or fraudulent purposes. <http://www.bis.org/publ/bcbs77.pdf>.

October 2000 - Electronic Banking Group Initiatives and White Papers

> The Committee explores risk issues arising from the geographical and political reach of electronic delivery channels. *See* <http://www.bis.org/publ/bcbs76.htm>.

March 1998 - Risk Management for Electronic Banking and Electronic Money Activities

> The Committee's first step in reviewing risk provided by electronic money transfers. This publication provides a framework to develop methods for identifying, assessing, managing and controlling the risks associated with electronic banking. *See* <http://www.bis.org/publ/bcbs35.htm>.

2.2 Identrus

November 10, 1999 - The Board of Governors of the Federal Reserve System approved foreign bank and bank holding company ownership in Identrus.

> Board of Governors approved Bayerische Hypo- und Vereinsbank, Deutsche Bank AG, Stichting Prioriteit ABN AMRO Holding, Stichting Administratiekantoor ABN AMRO Holding, ABN AMRO Holding N.V. and ABN AMRO Bank N.V., to partially own Identrus, a new Certification Authority. <http://www.federalreserve.gov/boarddocs/press/bhc/1999/19991110/19991110.pdf>.

3. United States - Regulatory

3.1 Department of the Treasury Interagency Regulations

Joint Final Rule: Interagency Guidelines Establishing Standards for Safeguarding Customer Information Final Rule: 66 Fed. Reg. 8,616 (Feb. 1, 2001)

Effective Date: July 1, 2001

Available at the following URLs:

PDF format

<http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=01-1114-filed.pdf>
<http://www.cbanet.org/issues/privacy/documents/Information_Safeguard_Guidelines.pdf>
<http://www.ots.treas.gov/docs/73112.pdf>

HTML/TXT format
<http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=01-1114-filed>
<http://www.fdic.gov/news/news/financial/2001/fil0122a.html>
<http://www.bankersonline.com/topstory/fedreg/66FR8615.txt>

The Guidelines are issued pursuant to sections 501 and 505(b) of the Gramm-Leach-Bliley Act, and include a section-by-section analysis of the following regulations:

- Office of the Comptroller of the Currency - 12 C.F.R. pt.30, (OCC resources are also reviewed below);
- Board of Governors of the Federal Reserve System - 12 C.F.R. pts. 208, 211, 225 and 263, (Federal Reserve resources are also reviewed below);
- Federal Deposit Insurance Corporation - 12 C.F.R. pts. 308 and 364, (FDIC resources are also reviewed below); and
- Office of Thrift Supervision - 12 C.F.R. pts. 568 and 570, (OTS resources are also reviewed below).

December 22, 2000 - Electronic Authentication Policy, for Federal payment, collection, and collateral transactions conducted over open networks such as the Internet

The Office of Management and Budget, as part of its procedures to implement the Government paperwork Elimination Act, directed the Department of the Treasury to develop, in consultation with Federal Agencies and the OMB, policies and practices for the use of electronic transactions and authentication techniques in Federal financial transactions, including in payment and collections. Digital signatures, as part of a public key infrastructure, appear to be required for transactions deemed high-risk.
<http://www.fms.treas.gov/eauth/index.html>.

3.2 Office of the Comptroller of the Currency <www.occ.treas.gov>

April 24, 2001 - OCC Alert 2001-4: Network Security Vulnerabilities

Response to recent hacker attacks and advisories issued by National Infrastructure Protection Center. Advises financial services companies to identify systems vulnerabilities, apply vendor-provided security patches, disable exploitable files and services, conduct penetration testing, review security provisions of service contracts, and establish controls as an indicator of security breaches. <http://www.occ.treas.gov/ftp/alert/2001-4.txt>.

February 28, 2001 - Release 2001-12: Risk Assessment for bank-provided aggregation services, with suggested control mechanisms.

Discusses new technologies and business models encouraging electronic aggregation of access to bank and brokerage accounts (gathering information from many secure web sites and presenting the information in a consolidated fashion to the customer). Recommends controls involving security, compliance, vendor management, data gathering and customer education. Regulation E (Electronic Funds transfer Act) may be triggered for the aggregating party offering transfers between accounts. Covers authentication and verification issues. <http://www.occ.treas.gov/ftp/bulletin/2001-12.txt>.

February 15, 2001- Release 2001-8: Guidelines Establishing Standards for Safeguarding Customer Information

Pursuant to Gramm-Leach-Bliley Section 501, the OCC issued these guidelines for the administrative, technical and physical safeguards for customers' "nonpublic personal information." Addresses threats to security or

integrity of customer information and unauthorized access to such information. Emphasizes responsibility of bank directors for security concerns and management of risk in electronic environment. All service provider contracts must meet the guidelines within two years. <http://www.occ.treas.gov/ftp/bulletin/2001-8.txt>. (*See supra* Section 3.1, *Department of the Treasury Interagency Regulations*).

January 2001 - Comptroller's Corporate Manual – The Internet and the National Bank Charter Handbook

Document created to address the risk questions surrounding creation of a bank on the Internet or with a large Internet access component. This manual is not as detailed on encryption and security issues as earlier Comptroller's Manual. <http://www.occ.treas.gov/corpbook/group4/public/pdf/internetnbc.pdf>.

January 29, 2001 - Advisory Letter 2001-3: Internet-Initiated ACH Risks

Automated Clearing House (ACH) and other electronic payment risks have grown with the rise of the Internet. This OCC Advisory discusses changes to NACHA's operating rules with respect to Internet-initiated payments. Merchant customers of national banks are required to employ fraudulent-transaction detection systems and procedures. *See* <http://www.occ.treas.gov/ftp/advisory/2001-3.txt>; *see also* <http://www.nacha.org> for operating rules).

January 17, 2001 - Release 2001-4: Interagency Guidelines Establishing Standards For Safeguarding Customer Information (issued jointly with Federal Reserve, FDIC and OTS)

The guidelines require financial institutions to establish an information security program to: (1) identify and assess the risks that may threaten customer information; (2) develop a written plan containing policies and procedures to manage and control these risks; (3) implement and test the plan; and (4) adjust the plan on a continuing basis to account for changes in technology, the sensitivity of customer information, and internal or external threats to information security. Each institution may implement a security program appropriate to its size and complexity and the nature and scope of its operations. <http://www.occ.treas.gov/ftp/release/2001-4.txt> (*See supra* Section 3.1, *Department of the Treasury Interagency Regulations*).

November 28, 2000 - OCC Advisory Letter 2000-12: FFIEC Guidance on Risk Management of Outsourced Technology Services

See <http://www.occ.treas.gov/ftp/advisory/2000-12.doc>; discussed *infra* in Section 3.6, Federal Financial Institutions Examination Council.

July 7, 2000 - Release 2000-53 and Alert 2000-9: Protecting Internet Addresses of National Banks

Discusses risk of confusion with similar domain names and risk of loss for bank's domain names. Recommends banks establish trademark in their domain names. <http://www.occ.treas.gov/ftp/release/2000-53.txt> and <http://www.occ.treas.gov/ftp/alert/2000-9.txt>.

May 15, 2000 - OCC 2000-14: Infrastructure Threats – Intrusion Risks

Thorough discussion of preventing, detecting, and responding to intrusions into bank computer systems. Concentrates on intrusions originating inside or outside of the bank and resulting in a range of damaging outcomes, including the theft of confidential information, unauthorized transfer of funds, and damage to an institution's reputation. Discusses security strategies, various controls to detect and prevent intrusion (including encryption), intrusion responses and information sharing. <http://www.occ.treas.gov/ftp/bulletin/2000-14.txt>.

November 16, 1999 - OCC Conditional Approval #339: Operating Subsidiary Applications by Bank of America, N.A., and Citibank, N.A. to expand activities of Identrus, LLC

OCC approval for Bank of America and Citibank to partially own and expand the activities of Identrus, a new Certification Authority. <http://www.occ.treas.gov/interp/dec99/ca339.pdf>.

October 1999 - Comptroller's Handbook – Internet Banking

Detailed discussion of Internet Banking risks and the controls needed to minimize those risks. Analysis of outsourcing risks. Includes cryptography appendix, as well appendices on firewalls and associated controls and types on online attacks. *See supra* January 2001 - Comptroller's Corporate Manual – The Internet and the National Bank Charter Handbook. <http://www.occ.treas.gov/handbook/intbank.pdf>.

May 4, 1999 - OCC 99-20: Certification Authority Systems

Bulletin for bankers, bank examiners and bank management interested in bank-owned/bank-operated CA systems. Bulletin explains certification authority systems, describes the roles of banks in emerging systems, and identifies the risks of such systems (i.e., issuing digital certificates, verifying identity, certificate creation, distribution and acceptance, internal security concerns, managing certificates, revoking certificates, and processing relying party requests) using the OCC supervision-by-risk framework. By outlining risks, bulletin intended to enable bankers to make informed decisions about whether and how to become involved in CA systems. This regulatory statement also includes a tutorial appendix on digital signatures and public key cryptography. <http://www.occ.treas.gov/ftp/bulletin/99-20.txt>

March 5, 1999 - OCC 99-9: Infrastructure Threats from Cyber-Terrorists

Cyber-terrorism is the use of computing resources against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. These can be operations to disrupt, deny, corrupt, or destroy information resident in computers or available via computer networks. This letter discusses the risks and vulnerabilities of cyber-terrorism and recommends certain controls to prevent or recover from infrastructure attacks. <http://www.occ.treas.gov/ftp/bulletin/99-9.txt>.

August 24, 1998 - OCC 98-38: Technology Risk Management: PC Banking

Substantial text on PC Banking risks. Provides guidance on how to identify, measure, monitor, and control risks arising from the use of retail personal computer banking. Discusses access authentication and other security controls including password systems, firewalls, and encryption. Also discusses intrusion detection and penetration testing. <http://www.occ.treas.gov/ftp/bulletin/98-38.txt>.

February 4, 1998 - OCC 98-3: Technology Risk Management

Long advisory memo explaining the OCC's risk categorization for technology driven banking activities, emphasizing transaction, strategic, reputation and compliance risks. Sets forth recommended methods to plan, implement and monitor technologies as they are chosen and used in banks. <http://www.occ.treas.gov/ftp/bulletin/98-3.txt>.

January 12, 1998 – OCC Conditional Approval #267: Zions First National Bank's application to own and operate a Certification Authority as an operating subsidiary

OCC approval to operate a Certification Authority as an operating subsidiary of a national bank. <http://www.occ.treas.gov/interp/jan98/ca267.pdf>.

3.3 Board of Governors of the Federal Reserve System <www.federalreserve.gov>

April 26, 2001 - SR-01-11 (SUP) Identity Theft and Pretext Calling

Reviews regulations and criminal laws applicable to identity theft in a financial services context. Recommends steps to protect customer information including verification procedures, fraud prevention and customer education. <http://www.federalreserve.gov/boarddocs/SRLETTERS/2001/sr0111.htm>.

March 29, 2001 - Interim Rules for Electronic Delivery of Disclosures under E-SIGN

Interim Rule(s) to establish uniform standards under five consumer protection regulations as required by the Equal Credit Opportunity Act,
<http://www.federalreserve.gov/BoardDocs/Press/boardacts/2001/20010329>, as follows:
Reg. B (Equal Credit Opportunity; Docket No. R-1040),
<http://www.federalreserve.gov/BoardDocs/Press/boardacts/2001/20010329/attachment.pdf>;
Reg. E (Electronic Fund Transfers; Docket No. R-1041),
<http://www.federalreserve.gov/BoardDocs/Press/boardacts/2001/20010329/attachment1.pdf>;
Reg. M (Consumer Leasing; Docket No. R-1042),
<http://www.federalreserve.gov/BoardDocs/Press/boardacts/2001/20010329/attachment2.pdf>;
Reg. Z (Truth in Lending; Docket. No. R-1043),
<http://www.federalreserve.gov/BoardDocs/Press/boardacts/2001/20010329/attachment3.pdf>; and
Reg. DD (Truth in Savings; Docket No. R-1044),
<http://www.federalreserve.gov/BoardDocs/Press/boardacts/2001/20010329/attachment4.pdf>.

November 30, 2000 - SR 00-17 (SPE): Guidance on the Risk Management of Outsourced Technology Services

This is the Federal Reserve Board's introduction of the FFIEC's outsourcing rules described in Section 3.6 below. <http://www.federalreserve.gov/boarddocs/SRLETTERS/2000/sr0017.htm>.

February 29, 2000 - SR 00-4 (SUP): Outsourcing of Information and Transaction Processing

More detailed discussion of risk management, international considerations and oversight of outsourcing in banks. <http://www.federalreserve.gov/boarddocs/SRLETTERS/2000/sr0004.htm>.

March 31, 1999 - SR 99-8 (SUP): Uniform Rating System for Information Technology (with attached FFIEC January 20, 1999 release)

Highlights revisions to the FFIEC technology rating system (*see infra* Section 3.6) including renewed emphasis on the quality of risk management processes. The Uniform Rating System for Information Technology is a tool used by regulators to compare the risks in different banks arising from chosen computing systems. <http://www.federalreserve.gov/boarddocs/SRLETTERS/1999/SR9908.HTM>.

April 20, 1998 - SR 98-9 (SUP): Assessment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations

This document provides a framework for evaluating a bank's information technology, including management processes, architecture, integrity, security and availability. Attachment includes an IT risk chart. <http://www.federalreserve.gov/boarddocs/SRLETTERS/1998/SR9809.HTM>.

December 4, 1997 - SR 97-32 (SUP): Sound Practices Guidance for Information Security for Networks

Basic short overview of sound information security practices in banking. Includes references to encryption, employee background checks and internal network vulnerabilities.
<http://www.federalreserve.gov/boarddocs/SRLETTERS/1997/SR9732.HTM>.

3.4 Federal Deposit Insurance Corporation <www.fdic.gov>

May 17, 2001 - Compliance Examination Procedures for Part 332 - "Privacy of Consumer Financial Information"

> Summarizes the basic requirements of the regulation; identifies examination objectives; establishes procedures for examining for compliance with the regulation; and provides an examination checklist for use in verifying compliance. <http://www.fdic.gov/news/news/financial/2001/fil0146.html>.

May 9, 2001 - Financial Institution Letter (FIL) FIL-39-2001: Identity Theft and Pretext Calling;

> Reviews regulations and criminal laws applicable to identity theft in a financial services context. Recommends steps to protect customer information including verification procedures, fraud prevention and customer education. <http://www.fdic.gov/news/news/financial/2001/fil0139.html>.

March 14, 2001 - FIL-22-2001: Security Standards For Customer Information (as required by the Gramm-Leach-Bliley Act).

> Joint guidelines with Federal Reserve Board, Office of the Comptroller of the Currency and Office of Thrift Supervision to establish standards for safeguarding customer information as required by the Gramm-Leach-Bliley Act (GLBA). <http://www.fdic.gov/news/news/financial/2001/fil0122.html>. (*See supra* Section 3.1, *Department of the Treasury Interagency Regulations*).

November 9, 2000 FIL-77-2000: Bank Technology Bulletin

> Letter addresses risks associated with Internet domain names. <http://www.fdic.gov/news/news/financial/2000/fil0077.html>.

October 3, 2000 FIL-67-2000: Security Monitoring of Computer Networks

> FDIC suggests practices for maintaining security and analyzes risks from external threats, internal threats and outsourcing. <http://www.fdic.gov/news/news/financial/2000/fil0067.html>.

September 21, 2000 FIL-63-2000: Online Banking

> Announcing “Tips for Safe banking over the Internet” brochure from the FDIC. <http://www.fdic.gov/news/news/financial/2000/fil0063.html>.

December 20, 1999 FIL-113-99: Financial Institution Web Site Privacy Survey

> Announcing and reviewing results of bank privacy policy survey. <http://www.fdic.gov/news/news/financial/1999/fil99113.html>.

July 7, 1999 - FIL-68-99: Risk Assessment Tools and Practices for Information System Security

> Detailed analysis of information security tools and practices. This letter describes a “prevention, detection, response” security system and risk assessment procedures. The FDIC discusses common pitfalls that may arise in implementing security tools. Then it explores various threats including denial of service attacks, social engineering, Trojan horses, viruses and Internet protocol spoofing. An appendix explores intrusion detection tools and other vulnerability analysis. <http://www.fdic.gov/news/news/financial/1999/fil9968.html>.

3.5 Office of Thrift Supervision <www.ots.treas.gov>

May 4, 2001 - Release OTS 01-32 - Identity Theft and Pretext Calling

Announcement of guidance to address identity theft in a financial services context. Recommends steps to protect and address customer information including verification procedures, fraud prevention and customer education. <http://www.ots.treas.gov/docs/77132.html>.

January 17, 2001 - Release OTS 01-04 - Interagency Guidelines Establishing Standards For Safeguarding Customer Information

See <http://www.ots.treas.gov/docs/77104.html>; *also see supra* Section 3.1, *Department of the Treasury Interagency Regulations*.

June 10, 1999 - CEO Memorandum 99-109: Transactional Web Sites

This memorandum discusses regulatory requirements for financial web sites, and includes a portion on information security. <http://www.ots.treas.gov/docs/25109.pdf>.

November 30, 1998 - Final Rule on Electronic Operations

Rule permits Federal savings associations to use, or participate with others to use, emerging technology to electronically perform functions and provide products and services as part of an authorized activity. <http://www.ots.treas.gov/docs/73058.html>.

December 23, 1997 - CEO Letter 75: Guidance Concerning the Reporting of Computer-Related Crimes by Financial Institutions

The memorandum describes criminal law relating to computer fraud and abuse, and proposed thrift reporting standards for computer crimes. <http://www.ots.treas.gov/docs/25075.pdf>.

October 15, 1997 - OTS Thrift Activities Handbook, Section 341: Information Technology

The OTS issued this information as Regulatory Bulletin 32-6. This document provides an analysis of regulatory and supervisory requirements for implementing information technology and an examination guideline for reviewing a thrift operation of such technology. It includes a discussion of examination ratings. <http://www.ots.treas.gov/docs/74028.pdf>.

3.6 Federal Financial Institutions Examination Council <www.ffiec.gov>

November 28, 2000 - Risk Management of Outsourced Technology Services

The document demands the boards of directors and senior management of financial institutions oversee and manage outsourcing relationships. The FFIEC requires financial institutions to institute an outsourcing process that includes: a risk assessment to identify the institution's needs and requirements; proper due diligence to identify and select a provider; written contracts that clearly outline duties, obligations and responsibilities of the parties involved; and ongoing oversight of outsourcing technology services. Primary focus on institutional oversight of outsource providers.
<http://www.federalreserve.gov/boarddocs/SRLETTERS/2000/sr0017a1.pdf>

January 20, 1999 - Uniform Rating System for Information Technology (64 Fed. Reg. 3109)

Federal Register announcement of FFIEC's revisions to the Uniform Interagency Rating System for Data Processing Operations, Information Systems (IS) rating system.
<http://www.federalreserve.gov/boarddocs/SRLETTERS/1999/sr9908a1.pdf>.

July 15, 1998 - Interagency Guidance on Electronic Financial Services and Consumer Compliance

Provides guidance on the consumer regulatory implications of laws and regulations relating to electronic financial services. <http://www.ffiec.gov/press/pr071598.htm>.

3.7 Securities Exchange Commission <www.sec.gov>

March 13, 2001 - Proposed Electronic Recordkeeping rule for Investment Companies and Investment Advisers

Proposes standard rules for treatment of the electronic storage of records kept by funds and advisers regardless of how they originated. <http://www.sec.gov/rules/proposed/ic-24890.htm>.

February 28, 2001 - Advanced Notice of Proposed Rulemaking

Notice of Delayed Effective Date for changes to recordkeeping provisions for broker-dealers, transfer agents, investment companies, investment advisers as a result of the Electronic Signatures in Global and National Commerce Act of 2000. <http://www.sec.gov/rules/proposed/33-7955.htm>.

January 25, 2001 - Office of Compliance Inspections and Examinations: Examinations of Broker-Dealers Offering Online Trading: Summary of Findings and Recommendations

Reviews implementation of security measures for online trading, including encryption, firewalls and passwords. <http://www.sec.gov/news/studies/online.htm>.

June 22, 2000 - Regulation S-P - Privacy Rules for Brokers, Dealers, Investment Companies, and Investment Advisers (65 Fed. Reg. 40,333)

Requires that firms registered with the SEC adopt policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. <http://www.sec.gov/rules/final/34-42974.htm>.

4. Other Resources

4.1 Financial Services Information Sharing and Analysis Center <http://www.fsisac.com>

January 2001 - Report of the President to Congress on the Status of Federal Critical Infrastructure Protection Activities

Discusses efforts to reduce vulnerability through encryption and other network security mechanisms. <http://www.fas.org/irp/offdocs/pdd/CIP_2001_CongRept.pdf>.

May 18, 2000 - Treasury Assistant Secretary Gregory A. Baer's Statements to the House Banking Subcommittee on Financial Institutions

Provides an update of activities of the FS/ISAC. <http://www.treas.gov/press/releases/ps637.htm>.

October 1, 1999 - Financial Services Information Sharing and Analysis Center (FS/ISAC) Opens

Department of the Treasury announces the opening of the banking and financial services information security facility, the Financial Services Information Sharing and Analysis Center (FS/ISAC). <http://www.treas.gov/press/releases/ps135.htm>

May 22, 1998 - Presidential Decision Directive 63 (PDD-63)

PDD 63 directed the development of a national plan to defend the critical information infrastructure of the United States, including that portion of the infrastructure related to financial services. <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>.

4.2 BITS <www.bitsinfo.org>

BITS is the Technology Group for the Financial Services Roundtable <http://www.fsround.org>. BITS maintains a Security and Risk Assessment (SRA) Steering Committee to address issues of security, safety and soundness in electronic payment technologies and e-commerce, as well as an accreditation program for security evaluation of products used in the financial services industry. <http://www.bitsinfo.org/sra.html>.

APP 9.2 HEALTHCARE PKI ASSESSMENT ISSUES (OUTLINE)

DRAFT VERSION 4-19-01

1. Purpose of this Appendix
   - 1.1. U.S. healthcare is a unique environment: it is structured, organized, paid for, governed, and regulated and deploys information in unique ways. A healthcare PKI therefore must be different from PKIs established in other business sectors.
   - 1.2. PKI will be an essential component of HIPAA compliance for healthcare organizations
   - 1.3. The purpose of this Appendix is therefore:
     - 1.3.1. To identify those legal issues and business processes peculiar to healthcare that are materially different from those which are assumed for assessments under the PAG;
     - 1.3.2. To augment the PAG regarding these identified healthcare issues and processes;
     - 1.3.3. To provide legal guidance to the healthcare field in the establishment and operation of PKIs

2. Scope of Appendix
   - 2.1. This appendix is intended to be an introduction to the industry-specific considerations, guidelines, and requirements of the U.S. healthcare industry for assessing public key cryptography combined with associated infrastructure
   - 2.2. This appendix should provide an intellectual framework for PKI assessment in managing the creation, maintenance, and transfer of healthcare information from the perspective of existing and emerging business, legal, and regulatory requirements as best understood at the time of publication.
   - 2.3. What the appendix is not:
     - 2.3.1. Legal advice
     - 2.3.2. ABA Official Policy

3. Audience
   - 3.1. This Appendix should be useful to healthcare providers, health plans and payers, consumers of healthcare services and their counsel and others who do business with them.

4. Interoperability/Accreditation
   - 4.1. Bridge CAs
     - 4.1.1. Federal Healthcare CP
     - 4.1.2. Other
   - 4.2. ASTM E31.20

5. Assurance
   - 5.1. Purpose of I&A
   - 5.2. I&A processes
   - 5.3. Levels of assurance
   - 5.4. Technical and administrative controls

6. Certificate Profile
   - 6.1. Content
     - 6.1.1. Necessary information
     - 6.1.2. Unique healthcare issues
   - 6.2. Confidentiality of information

7. PKI Business Model
   - 7.1. Scope of Community
   - 7.2. “Open” vs “closed” PKIs in healthcare
   - 7.3. Regulatory Requirements
     - 7.3.1. Legal obligations for protection of healthcare info

- 7.3.1.1. HIPAA regulations
- 7.3.1.2. HCFA Internet Policy
- 7.3.1.3. DEA interim rules
- 7.3.1.4. FDA rules
- 7.3.1.5. State laws
- 7.3.1.6. JCAHO & NCQA
- 7.3.2. Assessment of a CA's practices in promotion of "HIPAA Compliance"
- 7.3.3. Use of digital signatures
  - 7.3.3.1. Assurance level of the CP
  - 7.3.3.2. Duty of Relying Party to assess
  - 7.3.3.3. Evidentiary basis for signature
    - 7.3.3.3.1. State law
    - 7.3.3.3.2. Federal regulations
    - 7.3.3.3.3. Effect of eSign Law

7.4. Physical Procedural and Personnel Security Controls

7.5. Access Control

- 7.5.1. Ability of the party's system to accept certificates determined as reliable and reject others
- 7.5.2. Duty of relying party to make determination
- 7.5.3. Audit trials for access control

7.6. Subscriber key protection

7.7. Contractual relationships

- 7.7.1. Business Partners
  - 7.7.1.1. Business Associate agreements
  - 7.7.1.2. Chain of Trust agreements
  - 7.7.1.3. Trading Partner agreements
- 7.7.2. Subscriber Agreement
  - 7.7.2.1. Parties (CA & Subscriber)
  - 7.7.2.2. Relationship of Subscriber & Certificate Subject
  - 7.7.2.3. Relying party as a third party beneficiary
  - 7.7.2.4. Applicable scope
  - 7.7.2.5. Recommended provisions
- 7.7.3. Relying Parties
  - 7.7.3.1. Contract with CA
  - 7.7.3.2. Review of CPS and mapping to CP
- 7.7.4. Other PKI relationships
  - 7.7.4.1. Role of Registration Authority
    - 7.7.4.1.1. RA that has a customer relationship with CA
  - 7.7.4.2. Role of other ancillary service providers
  - 7.7.4.3. Responsibilities of CA for acts of agents
  - 7.7.4.4. Liability protections for Relying Parties and Subscribers
- 7.7.5. Assertion of a specific CP the CA's CPS
  - 7.7.5.1. Legal and business expectations
    - 7.7.5.1.1. Consequences of an inaccurate assertion
  - 7.7.5.2. Assessment parameters for validating the assertion of a specific CP OID
- 7.7.6. Audits
- 7.7.7. Liability
  - 7.7.7.1. General Discussion
    - 7.7.7.1.1. Compromise of CA
    - 7.7.7.1.2. Unique healthcare issues
      - 7.7.7.1.2.1. "Many to many" document/information flow
      - 7.7.7.1.2.2. Need for appropriate documentation which is consistent (CP, CPS, Subscriber Agreement, Relying Party Agreement
      - 7.7.7.1.2.3. Effect of inconsistency or unavailability of terms and risk of disclosure of protected information

7.7.7.1.2.4. Liability for long lived records (digital certificates and medical records)
7.7.7.2. Representations & warranties
7.7.7.3. Certificate assurance level
7.7.7.3.1. Assessment of sensitivity of information
7.7.7.3.2. Levels of assurance provided by CA in certificate
7.7.7.3.2.1. I&A (Personal appearance & other out of band assurance)
7.7.7.3.3. Exclusive use of hardware token storage
7.7.7.3.4. Other assurances concerning HIPAA security regulations
7.7.7.3.5. Nomenclature (ASTM & Federal Bridge)
7.7.7.4. Applicable law
7.7.7.4.1. Effect of HIPAA preemption
7.7.7.4.2. Consistency of provisions concerning state law applicability in relevant documents

8. Effect of Federal and State Laws on Electronic Healthcare Transactions
   8.1. The Effect of Federal and State Laws on Electronic Healthcare Transactions and Records
      8.1.1. Scope of issue
      8.1.2. eSign law generally
      8.1.3. Evaluating Consumer Protections under UETA and Other State Laws, Against eSign's Consumer Protection Exemptions and Preemption Provisions
      8.1.4. Relevance is whether to use PKI or any eSign at all?
      8.1.5. eSign's Preemption of Paper Records Retention Requirements, and Relevance for PKI Assessors
      8.1.6. Measures against degradation of certificates; certificate archival method allows access to and revision of PHI under HIPAA and state laws and JCAHO accreditation requirements, for required/desirable periods
   8.2. Privacy and security laws
   8.3. Medical records retention laws
   8.4. Fraud & Abuse and Office of Inspector General Implications
   8.5. Evidentiary standards

9. Digital Signature Use Protocol
   9.1. Authentication vs. nonrepudiation
   9.2. Federal Bridge position

10. Referenced Documents
   10.1. ASTM E31.20 version 4D
   10.2. Federal Bridge CA CP
   10.3. Applicable ISO Documents

F. INDEX

100293 v1/RE
25DX01!.DOC