DEPARTMENT OF PERSONNEL AND ADMINISTRATION

Division of Information Technologies

COLORADO RULES REGARDING THE USE OF ELECTRONIC SIGNATURES IN GOVERNMENTAL TRANSACTIONS

1 CCR 111-1

[Editor's Notes follow the text of the rules at the end of this CCR Document.]

PURPOSE

The purpose of these rules is to promote the development and the use of electronic transactions with Colorado public entities, by establishing acceptable technologies for the creation and use of electronic signatures in transactions that require high levels of authentication and security. Specifically, these rules identify the covered entities, define key terms, require digital signatures to be created by an acceptable technology in order to be presumed valid, set forth criteria for determining if a technology is acceptable, identify presently acceptable technologies, provide a mechanism for adding new technologies to be added to the list of acceptable technologies, establish a process for approving, monitoring and terminating certification authorities.

STATUTORY AUTHORITY

CRS 24-30-1604(1)

R1 Scope of Rules

These Rules apply to any Colorado public entity transaction where the use of electronic signatures has been expressly authorized by law and where the law mandates that the electronic signatures meet the five-fold criteria set out in CRS 24-71-101(2). These Rules also apply where an entity sending or receiving a transaction determines that the information contained therein needs to be protected by high levels of security. In addition, these Rules apply to governmental transactions with local public entities that have approved the use of electronic records or electronic signatures, unless the applicable governing body has adopted effective rules covering such transactions. These Rules do not apply to governmental transactions with the state judicial system.

R2 Definitions

A. "Approved Certification Authorities" means authorities that meet the requirements set out in these rules and have been placed on the List of Approved Certification Authorities.

B. "Asymmetric Cryptosystem" means a security system that uses an electronically processed algorithm, or series of algorithms, to generate a secure key pair that is attached to a digital signature. The key pair must be composed of two mathematically related but different keys that exhibit the following characteristics:

1. One key encrypts the data in a given message:

2. One key decrypts the data in a given message; and

3. The keys have the property that it is computationally infeasible to discover one of the key pairs merely by knowing the elements of the other key.

C. “CARAT Guidelines” means the CARAT Guidelines - Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates drafted by the Certification Authority Rating and Trust (CARAT) Task Force of the National Automated Clearing House Association (NACHA), Version 1 Draft, September 21, 1998, excluding later amendments or additions, incorporated by reference and on file with the Director. These guidelines provide prudent operational models for paired key infrastructure and shall serve as the guiding authority for implementing the use of asymmetric cryptosystem technology for electronic transactions with Colorado public entities. The guidelines are hereby incorporated by reference and are attached as Appendix A. This document may be examined at any state publications depository library. Questions about obtaining this material may be directed to the CITS Division Director, 690 Kipling Street, Lakewood, Colorado 80215.

D. “Certificate” means a computer based record generated by a Certification Authority that is affixed to or contained in a document with a digital signature. The certificate shall:

1. identify the Certification Authority issuing it;

2. identify the subscriber;

3. contain the subscriber's public key;

4. be digitally signed by the Certification Authority issuing;

5. identify the certificate's operational period and

6. conform to accepted industry standards, including, but not limited to ISO × 509.

E. “Certification Authority” means a person or entity that is approved by the Director to issue certificates to subscribers for the purpose of engaging in electronic transactions with Colorado public entities.

F. “Digital Signature” means a type of electronic signature that secures and transforms data through the use of an asymmetric cryptosystem.

G. “Director” shall mean the Executive Director of the Colorado State Department of Personnel.

H. “Electronic Record” is defined in CRS 24-71.1-103(4) as a record generated, communicated, received, or stored by electronic means.

I. “Electronic Signature” means an electronic or digital method of identification that is initiated, executed or adopted by a person or entity with the intent to be bound by the signature. It shall have the same force and effect as if a manual signature was used. If applicable, it must be unique to the entity using it, capable of verification, under the sole control of the entity using it and linked to the data in such a manner that the electronic or digital signature is invalidated if any of the data is changed.

J. “Expert” means a person with demonstrable skill and knowledge based on training and experience who would qualify as an expert pursuant to the Colorado Rules of Evidence.

K. “Governmental transaction” is defined in CRS 24-71.1-103 (6) as any activity by a public entity pursuant to which a record is created, amended, or retained, including a court order.

L. “Handwriting Measurements” means the metrics of the shapes, speeds and/or other distinguishing features of a signature as the person writes it by hand with a pen or stylus on a flat surface.

M. “Key Pair” means a private key and its corresponding public key in an asymmetric cryptosystem. The key pair must be unique in that the public key can verify the digital signature created by the private key.

N. “List of Approved Certification Authorities” means the list of Certification Authorities approved by the Director to issue certificates for electronic transactions involving persons doing business with public entities in Colorado. This list shall be maintained by the Department of Personnel and updated monthly. It may be obtained electronically via the World Wide Web, and at the Department's office located at 1525 Sherman Street, Denver, Colorado.

O. “Person” is defined in CRS 24-4-102 (12).

P. “Policy Authority” means, as referred to and as defined by the CARAT Guidelines, the authority that establishes the rules of procedure for the use of digital signatures. The Director shall serve as the Policy Authority for Colorado.

Q. “Private Key” means the key in an asymmetric cryptosystem key pair used to create a digital signature.

R. “Public Key” means the key in an asymmetric cryptosystem key pair used to verify a digital signature.

S. “Public Entity” as defined in CRS 24-71.1-103(8) means state agencies and every county, city and county, city, town, school district, special district, special improvement district, and every other kind of district, agency, instrumentality, political subdivision, or authority of the state organized pursuant to state law, whether or not it is subject to home rule.

T. “Record” as defined in CRS 24-71.1-103 (9) 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.

U. “S.A.S. 70” means the standards set out in the American Institute of Certified Public Accounts (AICPA) Statement on Auditing Standards No. 70. Should current S.A.S. 70 standards (or any succeeding version) be superceded, the Policy Authority, in consultation with the State Treasurer, shall establish a deadline for all affected parties to comply with the replacing standard. This deadline shall be no later than 2 years from the date of issuance of the new S.A.S. 70 standards.

V. “State agency” as defined in CRS 24-71.1-103, means this state or any department, institution, or other agency of this state, including institutions of higher education.

W. “Signature Digest” is the resulting bit-string produced when a signature is tied to a document using Signature Dynamics.

X. “Signature Dynamics” means measuring the way a person writes his or her signature by hand on a flat surface and binding the measurements to a message through the use of cryptographic techniques.

Y. “Subscriber” means a person or entity that:

1. Is the subject listed in the certificate.

2. Accepts the certificate, and

3. Holds a private key that corresponds to the public key listed in that certificate.

R3 Acceptable Technologies for Electronic Signatures

Electronic transactions with Colorado public entities as specified in Rule 1 must utilize electronic signatures that employ a technology identified in the list of acceptable technologies and that employ practices that are capable of creating signatures that conform to the requirements set forth in CRS 24-71-101(2) (a-d).

A. Public Key Infrastructure is an acceptable technology for use in transactions by Colorado pubic entities when an entity determines that the transaction requires a signature and a high level of security, provided that the electronic signature is created consistent with the requirements set forth in CRS 24-71-101(2)(a-d) and the provisions set out in these rules.

1. CRS 24-71-101(2)(a) requires that a digital signature be `unique to the person using it'. A public-key based digital signature may be considered unique to the person using it, if:

a) The private key used to create the signature on the document is known only to the signer, and

b) The digital signature is created when a person runs a message through a one-way function, creating a message digest, then encrypting the resulting message digest using an asymmetrical cryptosystem and the signer's private key, and

c) Although not all digitally signed communications will require the signer to obtain a certificate, the signer is capable of being issued a certificate to certify that he or she controls the key pair used to create the signature, and

d) It is computationally infeasible to derive the private key from knowledge of the public key.

2. CRS 24-71-101(2)(b) requires that a digital signature be `capable of verification'. A public key-based digital signature is capable of verification if

a) The acceptor of the digitally signed document can verify the document was signed by using the signer's public key to decrypt the message: and

b) If a certificate is a required component of a transaction, the issuing Certification Authority, either through a certification practice statement or through the content of the certificate itself, must identify the form(s) of identification it required of the signer prior to issuing the certificate.

3. CRS 24-71-101 (2) (c) requires that the digital signature remain `under the sole control of the person using it'. Whether a signature is accompanied by a certificate or not, the person who holds the key pair, or the subscriber identified in the certificate, assumed a duty to exercise reasonable care to retain control of the private key and prevent its disclosure to any person not authorized to create the subscriber's digital signature.

4. CRS 24-71-101 requires that the digital signature must be linked to the data in the document in such a way that if the data are changed the digital signature is automatically invalidated.

B. Signature dynamics is an acceptable technology for use by Colorado public entities in governmental transactions, so long as the electronic signature meets the requirements set forth in CRS 24-71-101(2)(a-d) and the provisions set forth in these rules.

1. “Unique” CRS 24-71-101 (2) (a) requires that an electronic signature be unique to the person signing the document. A signature digest produced by Signature Dynamics technology may be considered unique to the person using it, if:

    a) the signature digest records the handwriting measurements of the person signing the document using signature dynamics technology, and

    b) the signature digest is simultaneously cryptographically bound to the handwriting measurements, and

    c) after the signature digest is bound to the handwriting measurements, it is computationally infeasible to separate the handwriting measurements and bind them to a different signature digest.

2. “Verification” CRS 24- 71-101(2)(b) requires that a digital signature be capable of independent verification. A signature digest produced by Signature Dynamics technology is capable of independent verification if:

    a) the acceptor of the digitally signed message obtains the handwriting measurements for purposes of comparison, and

    b) if signature verification is a required component of a transaction with a public entity, the handwriting measurements are sufficient to allow an expert handwriting and document examiner to assess the authenticity of a signature.

3. “Sole Control” CRS 24-71-101 (2) (c) requires that a digital signature remain `under the sole control of the person using it'. A signature digest is under the sole control of the person using it if:

    a) the signature digest captures the handwriting measurements and cryptographically binds them to the message directed by the signer and to no other message, and

    b) the signature digest makes it computationally infeasible for the handwriting measurements to be bound to any other message.

4. “Linked” CRS 24-71-101 (2) (d) requires that the signature digest produced by the Signature Dynamics technology be linked to the message in such a way that if the data in the message are changed, the signature digest is invalidated.

R4 Identification of Additional Acceptable Technologies

A. The Director shall review and approve the use of all technologies for electronic transactions with Colorado public entities. All such transactions must use a technology identified on the List of Approved Technologies and must meet the standards set forth in CRS 24-71.1-106(2), if applicable.

B. Provisions for Adding Approved Technologies to the List

1. Any person or public entity may petition the Director to review a technology for use in electronic transactions with Colorado public entities by providing a written request for review. This request shall include a full explanation of the technology and shall show that it meets the requirements established in CRS 24-71.1-106(2), if applicable, and that it meets any additional applicable requirements then in effect.

2. The Director has **120** days from the date of the request to review the petition and to accept or reject it.

3. If the Director finds that the criteria established in CRS 24-71.1-106 (2)(a-d) is applicable and that petitioner's proposed technology meets those requirements and any additional applicable requirements then in effect, the Director shall adopt any necessary regulations pursuant to the Administrative Procedure Act and add the new technology to the list of approved technologies for use with electronic signatures by public entities in Colorado.

4. If the proposed technology is rejected, the petitioner may appeal the decision through the Administrative Procedure Act. CRS 24-4-101. et seq.

R5 Certification Authority Application, Approval, Suspension, Revocation and Renewal

A. Applications and Approval of Certification Authorities

1. Applicants may obtain an application to be an approved Certification Authority from the office of the Department of Personnel. Applicants shall file a complete application in the office of the Department of Personnel. The application is available via the World Wide Web and at 1525 Sherman Street. Denver, Colorado.

2. Applicants shall provide one of the following:

   a) A certified copy of an unqualified performance audit performed in accordance with standards set forth in S.A.S. 70 to ensure that the Certification Authorities practices and policies are consistent with the requirements of CRS 24-71.106.

   b) Certification Authorities in operation in other jurisdictions for one (1) year or less shall undergo a S.A.S. 70 type 1 audit — A report of Policies and Procedures placed in operation. The applicant must receive an unqualified opinion and provide a certified copy of that opinion with the application.

   c) Certification Authorities in operation in other jurisdictions for longer than one (1) year shall undergo a S.A.S. 70 type 2 audit — A report of Policies and Procedures placed in operation and test of operating effectiveness. The applicant must receive an unqualified opinion and provide a certified copy of that opinion with the application.

3. The Director shall place Certification Authorities on the “Approved List of Certification Authorities” within thirty days after the applicant provides the Director with a complete application.

4. A Certification Authority shall remain on the “Approved List of Certification Authorities”, if the Certification Authority provides proof of compliance every two (2) years after initially being placed on the list and meets any additional applicable requirements of the Policy Authority in effect at that time.

5. The Director shall maintain the “List of Approved Certification Authorities” authorized to issue certificates for electronic transactions with public entities in Colorado.

6. In sending or receiving governmental transactions that require a signature and a high level of security. Colorado public entities shall accept certificates only from Certification Authorities that appear on the “List of Approved Certification Authorities”.

B. Suspension of Certification Authorities

1. A Certification Authority must notify the Director immediately if its accreditation, license or approval is revoked by another jurisdiction or if its authority lapses or terminates for any reason in another jurisdiction. Failure to notify the Director is cause for revocation.

2. If the Director becomes aware that a Certification Authority has had its accreditation, licensing or approval revoked in another jurisdiction, the Director shall notify the Certification Authority in writing of its intent to revoke. The Certification Authority may contest the intent to revoke within thirty days after receipt of notice pursuant to the applicable provisions of the Administrative Procedure Act. If the Certification Authority does not contest the intent to revoke within thirty days the Executive Director shall remove the Certification Authority from the List of Approved Certification Authorities.

C. Removal of Certification Authorities

1. Certification Authorities shall be removed automatically from the "Approved List of Certification Authorities" on the two year anniversary date of its approval unless within thirty days if its expiration date, it provides the Director with proof of a successful S.A.S. 70 audit (as required by R4 A(4)) and shows that is operating in compliance with any additional applicable requirements then in effect.

    2. The expiration date shall be determined from the date that the Executive Director signs the approval.

D. Reinstatement of Certification Authorities

Certification Authorities shall be reinstated to the "Approved List of Certification Authorities" once it submits an acceptable S.A.S. 70 audit pursuant to R4 A(4) to the Director and shows that it is in compliance with any other applicable requirements in effect at that time.

R6 Presumption of Validity and Burden of Proof

If a digital signature is received by a public entity from a subscriber using an approved Certification Authority, the signature shall be presumed valid. If a digital signature is sent by a public entity using an approved Certification Authority, the signature shall be presumed valid. It shall be the burden of the party contesting the validity of the signature to overcome the presumption.

CARAT Guidelines

Guidelines for -Constructing Policies Governing the Use of Identity-Based Public Key Certificates

v. 1.0 (DRAFT: September 21, 1998)

National Automated Clearing House Association (NACHA)

The Internet Council

Certificatione Authority Rating and Trust (CARAT) Task Force

EXECUTIVE SUMMARY

Background

The bright promise of electronic commerce is shaded by concerns about security. The very openness of the Internet that has led to its explosive growth has also given rise to an awareness of its security limitations. Government entities and private businesses that are obvious candidates for participating in

electronic commerce are understandably cautious. To be able to rely on the electronic messages they receive, such organizations need assurance that those messages are authentic and have not been altered.

Technical means of establishing message authenticity and integrity have existed for some time. For example, public key technology, which has long been known in technical circles, seems to hold extraordinary promise but its implementation is only beginning. What is presently lacking are public key infrastructures, or PKIs, that define the business and legal expectations and requirements of the parties.

Many states have sought to provide a measure of predictability in this arena by enacting laws regarding digital or electronic signatures. A few of these laws go so far as to construct major elements of a PKI within their jurisdictions. State laws are far from uniform, however and it is unclear whether this lack of uniformity is itself an impediment to the further growth of electronic commerce. Nonetheless, in response to a perceived need for a more integrated approach, several national associations of state officials embarked on a collaborative effort to address their shared security concerns. In May 1997, the National Association of State Information Resource Executives (NASIRE), along with the National Association of State Purchasing Officers (NASPO), the National Association of State Auditors. Comptrollers and Treasurers (NASACT) and several individual states, sought to create a forum to explore this issue in collaboration with private sector participants. Following a competitive solicitation of proposals, the National Automated Clearing House Association (NACHA) was selected to facilitate this effort. These Guidelines are a product of that effort.

Introduction to the Guidelines

These Guidelines are intended to help organizations create closed but interoperable PKIs that may then be used to facilitate pilot projects employing public key technology. Such organizations, here called Policy Authorities, can use the Guidelines to analyze their particular needs and construct a PKI that will meet those needs. One important product of that analysis is likely to be a Certificate Policy, which may be thought of as a charter for a particular PKI. Briefly, a Certificate Policy defines who the parties are, what uses are acceptable within the PKI, and the relationships and obligations of the parties to each other. The last part of these Guidelines includes high-level drafting instructions for Certificate Policy writers. The Guidelines suggest that Policy Authorities use contracts to make the provisions of a Certificate Policy legally binding among the parties.

The Guidelines are a publication of NACHA and were developed under the auspices of The Internet Council, a NACHA-sponsored council. They were drafted by the Certification Authority Rating and Trust (CARAT) Task Force of The Internet Council's Authentication and Network of Trust Work Group. Please note that the release of these Guidelines does not necessarily indicate approval or disapproval of its contents by any particular member of NACHA or the CARAT Task Force. The Guidelines are still in draft form and should not be regarded as a finished document. For this work to advance, it is critical that interested parties provide comments to NACHA regarding the usefulness of this document. To that end, NACHA encourages interested parties to use these Guidelines to draft Certificate Policies that pertain to their particular pilot needs. It is envisioned that the cumulative experience of interested parties and their feedback to NACHA will lead to a revised and improved version of these draft Guidelines. NACHA welcomes all comments. Comments will be accepted until December 31, 1998.

Summary of the Guidelines

The first major part of the Guidelines (Part B. “Organization and Governance - Getting Started”) explains the concept of a Policy Authority and its role in imparting structure, form and organization to a PKI. The Policy Authority is distinguished from other stakeholders, who may be End Entities and/or PKI Service Providers. End entities include the parties to the underlying transactions - for example, buyers and sellers in a procurement setting. PKI Service Providers include parties that perform enabling functions that support the underlying transactions. Even though a PKI is created to enable certain transactions it should not be confused with the substance of the business being conducted by the End Entities.

Because public key technology is an enabling technology, any attempt to use it must start by looking at the business drivers: *i.e.*, the transactions that bring stakeholders together. This should include taking into account the general business and legal environment surrounding the transactions. A deliberate look at the parties' needs is a critical first step in determining whether and how a PKI can help. The next step is to learn more about the functions that public key technology can perform and consider how they may be applied to the parties' needs.

In Part C. “Building a Business and Legal Model,” the Guidelines describe a suite of *functions* derived from public key technology that might be performed in a PKI. The list, which is not exhaustive, includes: key generation and safekeeping; information acquisition and confirmation; certificate creation: certificate signing; certificate distribution: certificate revocation: resolving claims and disputes; and risk management. These functions can be thought of as building blocks with which to construct a PKI. Once the relevant functions are identified, they must be associated with roles. The Guidelines refer to this as *allocating functions to roles*.

A number of possible *roles* are identified and named. They include PKI Service Provider roles such as *Issuer, Certificate Manufacturer, Registrar* and *Repository*. End entity roles include *Subscribers* and *Relying Parties*. Not all these roles will be appropriate in every business model and there may be other roles not here identified that a Policy Authority may wish to specify. Nevertheless, parties within a PKI must agree to perform certain roles and those agreements should be embodied in legally enforceable contracts. It may well be that one party may assume several roles within a given PKI, depending on the business and legal model employed.

Various models for structuring the parties' relationships have been constructed over time. These Guidelines use a four-cornered model (Subscriber, Issuer, Repository and Relying Party) as a point of departure from which to consider how the functions and obligations of the parties might be allocated in a closed but scalable and interoperable PKI. The four-cornered model is not a recommended or preferred model: it is included because it is helpful in illustrating how to allocate functions and obligations among the parties in a PKI.

The four-cornered model is then analyzed in some detail by looking at the functions and obligations of each party to the other parties. For example, the functions assigned to the Issuer (*e.g.*, issue certificates, state information accurately, revoke certificates on request, publish certificates, confirm accuracy of information in the certificates: etc.) are analyzed in light of the Issuer's obligations to the Subscriber. Repository and Relying Party. A similar analysis is performed for each of the other three roles occupying the four corners. In addition, other roles such as Certificate Manufacturer and Registrar are addressed. This section also foreshadows certain themes such as implementing contracts that are explored more fully in the next section.

In Part D. “Implementing a Business and Legal Model.” the Guidelines address PKI governance issues, including the documents that may be used to organize and implement a particular PKI. This section discusses some of the factors that may affect whether or not a Certificate Policy is needed. It reiterates and elaborates upon the need to bind parties to their respective roles through implementing contracts.

Assuming a Certificate Policy is to be drafted, this section of the Guidelines reminds Policy Authorities that there are a number of additional things to consider beyond the underlying transactions and the available suite of PKI functions. They include a consideration of noncontractual governance structures such as existing legal and regulatory conditions that may apply to certain transactions. Different business and legal models, such as the three-party “certificate authority” model (Subscriber, certificate authority and Relying Party) envisioned by the American Bar Association's Digital Signature Guidelines, are briefly introduced. Readers are reminded that the Guidelines were written with certain overarching assumptions, including reference to a general business environment in which public sector buyers engage in online interactions with private sector sellers. It is necessary for Policy Authorities to draft Certificate Policies that are tailored to their particular needs and business requirements, and to view these Guidelines as informational but not prescriptive.

The final part of the Guidelines (Part E. “Drafting a Certificate Policy”) is intended to provide practical suggestions to Policy Authorities as they begin the task of drafting their own Certificate Policies. This part, unlike the previous parts of the Guidelines, is organized with reference to the Internet Engineering Task Force (IETF) PKIX 4 Framework. It is numbered to track the numbering used in that Framework except where noted. Parts 5. 6 and 7 of the PKIX 4 Framework are not incorporated in these Guidelines due to their technical nature, which is inappropriate for Guidelines of this type.

Part 1, Part 2, Part 3, Part 4 and Part 8 of the PKIX 4 Framework serve to organize the correspondingly numbered sections of these Guidelines. In each such section, the reader will find “drafting instructions” followed by a “discussion.” The drafting instructions include high-level suggestions regarding what ought to be included in a Certificate Policy. They use the terms “should” and “may” in recognition of the fact that these are guidelines and should not be regarded as prescriptive.

In part 1 of Drafting a Certificate Policy (“Introduction”), the Guidelines provide assistance to drafters in describing the scope and purpose of a Certificate Policy. Of central importance here is the description of community and applicability; *i.e.*, the parties to whom the Certificate Policy will apply and the uses that will be permitted within the PKI.

In part 2 (“General Provisions”), drafters are instructed to address the obligations of the various parties to one another. The content of the provisions in this section will vary widely from one Certificate Policy to another depending on the business and legal model constructed by the Policy Authority. This part also addresses matters related to enforcement of the parties' obligations, and issues such as the fees that may be charged by PKI Service Providers, publication requirements, compliance audit requirements, and so forth.

Part 3 (“Identification and Authentication”) addresses the central issue of the confirmation of individual identity. This part of the Guidelines includes instructions regarding initial registration, the types of names that may be included in public key certificates, requests to renew expired or revoked certificates, and certain revocation requests.

Part 4 (“Operational Requirements”) includes high-level instructions regarding certain operations that are likely to occur in a PKI. Some of the more critical operations addressed here include the issuance of certificates by Issuers and their acceptance by Subscribers, as well as certificate revocation. This part also includes guidelines for Relying Parties concerning the need to check a certificate's current validity.

Finally. Part 8 (“Specification Administration”) provides instructions regarding the manner in which a Policy Authority may change its Certificate Policy and notify affected parties of those changes.

PART A. INTRODUCTION

Background

State governments have actively pursued methods for creating non-legislative standards for the use of digital signatures verifiable through public key certificates. In May 1997, the National Association of State Information Resource Executives (NASIRE), along with the National Association of State Purchasing Officers (NASPO), the National Association of State Auditors. Comptrollers and Treasurers (NASACT) and several individual states, sought to create a forum to explore this issue in collaboration with private sector participants. Following a competitive solicitation of proposals, the National Automated Clearing House Association (NACHA) was selected to facilitate this effort. These Guidelines are a product of that effort.

Structure of this document

These Guidelines are organized in four substantive parts:

- Part B. “Organization and Governance: Getting Started,” introduces the concept of a Certificate Policy and the Policy Authority that promulgates a Certificate Policy.

- Part C. “Building a Business and Legal Model,” provides a detailed illustration of a particular model for allocating functions and obligations to roles. Beginning with an explanation of the business and legal tools for building a model, this part then sets forth an in depth example of rights and obligations of each party to each other party, depending on the role they play within the model under examination.

- Part D. “Implementing a Business and Legal Model,” outlines several practical issues to be considered as part of choosing a PKI model that fits the particular parties and their transactions. This part explores how variables in the underlying business conditions for a given stakeholder can change the choice of a PKI model and provisions of a Certificate Policy.

- Part E. “Drafting a Certificate Policy,” provides practical suggestions to Policy Authorities as they begin the task of drafting their own Certificate Policies. This part follows the Internet Engineering Task Force PKIX 4 Framework for drafting a Certificate Policy.

The CARAT Task Force has enjoyed benefits of collaboration, to a greater or lesser extent, with several other organizations working on standards for the use of Public Key Certificates. In particular, the helpful suggestions from members of the American Bar Association's Information Security Committee, the ANSI X9F5 Work Group and from CommerceNet have been important throughout the drafting process leading to these Guidelines.

PART B. ORGANIZATION AND GOVERNANCE: GETTING STARTED

This part of the Guidelines introduces the concepts of a certificate-based public key infrastructure, a Certificate Policy and the Policy Authority that promulgates a Certificate Policy. Generally, a Certificate Policy is used to define the interrelated rights and obligations of stakeholders utilizing public key certificates to enable electronic commerce transactions. Though some implementations of public key cryptography can be used to directly signify the role or authority an individual possesses, these Guidelines deal only with public key certificates used to authenticate the identity of an individual. In addition, the Guidelines are intended for use within an environment that is capable of technical interoperability, but is legally bounded to include only certain parties and transactions. The Guidelines do not purport to support a global electronic commerce structure for “stranger to stranger” serendipitous transactions. Rather than propose a theoretical structure for the “open” or “global” use of public key certificates, these Guidelines are tailored for use within business and legal environments in which parties have a contractually based and legally bounded relationship.

B.1 Introduction to Public Key Infrastructure

B.1.1 PKI Service Providers Enable Transactions Between End Entities

A public key infrastructure (“PKI”), literally, is a complex infrastructure of hardware, software, databases, networks, security procedures, and legal obligations. Among other things. PKI allows individuals and entities to identify each other as they transact business on computer networks such as the Internet. It is important to understand that PKI is not a transaction in and of itself, but rather one of a possible number of “enabling” technologies that support and implement actual transactions. Thus, for instance, if the goal is to create an electronic procurement system that allows government agencies to procure goods from private companies, the actual transaction is “procurement” while PKI is the enabling technology that allows electronic procurement to take place.

Building a PKI is not a trivial task. Building a PKI requires the successful execution of a suite of PKI *functions*. “PKI Service Providers” are the *parties* — the legal persons or entities - that perform PKI

functions. In some PKIs, one party will perform all PKI functions. In other PKIs, multiple parties will perform sets of functions. In the ABA's Digital Signature Guidelines, the ABA drafters refer to a Certification Authority ("CA") as the one party responsible for performing a full suite of PKI functions. These Guidelines refer to "PKI Service Providers" as the *parties* that perform a full suite of PKI *functions*.

PKI Service Providers perform PKI functions for the benefit of "End Entities." The parties who perform "End Entity" roles are the parties which engage in actual transactions.[1] If PKI Service Providers did not provide PKI. End Entities would still transact business but would simply use some other identification or security technology, such as biometrics or pen and ink, to conduct business. Stated another way. End Entities will always exist to conduct business, for instance, government to business procurement transactions, but PKI Service Providers will exist only as long as End Entities or their governing bodies deem PKI the best technology to facilitate procurement.

[1]There are two types of End Entities: a Subscriber and a Relying Party. Subscribers are sometimes called Subjects. Subscribers are originators and signers of messages. Relying Parties are recipients of signed messages. In most applications. Subscribers will be Relying Parties and Relying Parties will be Subscribers since communication is almost always bi-directional. For example, if a Subscriber-Offeror originates and signs a offer which requires acceptance, the Relying Party-Offeree must also be a Subscriber if it is to originate and sign an acceptance.

B.1.2 PKI Functions, Roles and Parties

Early thinkers conceived of a Certification Authority as the single party responsible for performing all PKI functions. However, early thinkers recognized that a Certification Authority may delegate a certain set of functions to a Registration Authority. In fact, there are other sets of functions that can be logically and conveniently grouped and delegated. In business models, such sets of functions are those that are often outsourced or that have some other heightened significance.

It is useful to continue the evolution of naming sets of functions. Indeed, PKI functions can be divided into several sets of functions, with each set of functions can represent a *role* Roles can be named according to the nature of the functions in each set. By naming roles and associating functions with roles, these Guidelines do not suggest that in every business model functions will be divided in the same manner. Further, it is not suggested that there will be one-to-one correlation between roles and parties. Indeed, it is envisioned that a *party* may perform one or more roles in a PKI. Further, it is recognized that evolving business models may change the way in which functions are logically grouped: hence, it may be necessary in the future to further evolve the naming of roles.[2]

[2]It is important to understand that all business models are unique. In any given business model, the division of functions among parties will be different. Hence, the roles described in this document may be inadequate in describing some business models. That is, simply because the Task Force states that a party performing Role 1 will perform Functions 1, 2, 3, 4, and 5 does not mean that in all business models a PKI Service Provider responsible for Role 1 will perform Functions 1–5. It could happen that Function 5 is performed by a PKI Service Provider responsible for Role 2. Roles are named simply because a granular vocabulary makes the task of describing rights and responsibilities of parties easier. (It is difficult, for instance, to refer only to a Certification Authority and a Registration Authority when describing functions generally recognized as being performed by a Repository). Accordingly, drafters are cautioned to carefully develop and examine how functions are actually mapped to roles and PKI Service Providers under a particular Certificate Policy.

The roles identified in these Guidelines follow: [3]

[3]There are additional roles that could be named. At this time, the Task Force does not find it useful to define additional roles.

- PKI Service Providers
    - Policy Authority (to be described more fully below)
    - Issuer[4]

[4]Throughout these Guidelines, the Task Force assumes that a Certificate Manufacturer and a Registrar are closely related to an Issuer. That is, it is assumed that the functions performed by the Certificate Manufacturer and the Registrar are functions that are very often the responsibility of the Issuer. Indeed, in the four-corned model used throughout this document, the Certificate Manufacturer and Registrar are generally considered sub-roles of an Issuer. As a result, where the term Issuer is used, drafters should realize that in some cases either Certificate Manufacturer or Registrar could be substituted.

- Certificate Manufacturer
- Registrar (Registration Authority)
- Repository

- End Entities
  - Subscriber
  - Relying Party

An example of how functions are assigned to roles is more fully described in Part C.

B.2 The Role of a Policy Authority

Some authoritative party must formulate and adopt the Certificate Policy, and these Guidelines refer to that party as the "Policy Authority." The Policy Authority is that party or body with final authority and responsibility for specifying a Certificate Policy. Setting a Certificate Policy is a function of organizational governance. Governance is the manner in which an organization structures the roles, rights and responsibilities of people who participate within a given system. The governing body, according to Black's Law Dictionary, means that body "which has ultimate power to determine its policies and control its activities."[5] Thus, the governance of an organization must be viewed as broader than the mere promulgation of a Certificate Policy, although setting Certificate Policy is included in and tightly related to the overall duties of governance.

[5]BLACK'S LAW DICTIONARY, 6TH EDITION, 1990.

B.2.1 Policy and Business: The Parties and The Transactions

The Policy Authority is responsible for assuring the activities of PKI Service Providers and End Entities are conducted in a sound and efficient manner. A threshold issue for the Policy Authority to consider prior to drafting a Certificate Policy is the scope and depth of the underlying business context that has given rise to the need to use secure and/or authenticated electronic communications. A Certificate Policy must fit the basic business needs of the parties, which will differ depending upon the nature of the participants involved and what business transactions they seek to conduct. It is for the above-mentioned reasons that the CARAT Task Force has drafted this document as a set of Guidelines rather than a prescriptive formulaic policy statement. Each Policy Authority seeking to draft a Certificate Policy will have to first make fundamental business and legal policy determinations that are broader than the scope of issues presented within the Certificate Policy.

B.2.1.1. Who are the Stakeholders?

In addition to the Policy Authority, the stakeholders are End Entities and PKI Service Providers if PKI is used to enable transactions between End Entities. Stakeholders could be drawn from any number of groups, such as citizens, consumers, business organizations, government entities, academic institutions, employees, politicians, or any number of other groups. Depending on the stakeholders, very different roles and functions within a PKI system may be appropriate and feasible.

B.2.1.2 What Underlying Transactions are to be Facilitated by PKI?

The transactions facilitated by use of PKI may include medical records or third party payor requests in the healthcare environment; stock trades; baseball card trades; or the trading of promises to work for a new employer. The same parties who engage in different transactions may require different policies for each transaction due to the variations in the underlying legal and economic systems related to each transaction. As a technical matter, it would be convenient for the same parties to use the same

certificates under the same Certificate Policy as part of every transaction they might conduct with each other. However, the regulatory requirements governing, for instance, payment systems are so different from the regulatory requirements governing submission of a bid for a public works project that the obligations and rights of the parties may well require different certificate policies. At some point in the distant future, a broader system may emerge that consolidates several secure communications policies together. However, for the foreseeable future, policies that define the rights, duties and functions of parties can be expected to be related to the underlying transactions and businesses involved.

B.2.1.3 Certificate Policy Subject to Primary Business Drivers

The Certificate Policy must be drafted to support and reflect the underlying business structure. The business mission of the stakeholders and the business drivers that give rise to the specific transactions should be of paramount importance to the Policy Authority. A Policy Authority that focuses on implementing PKI or any enabling technology over the fundamental business mission of the organization may be neglecting governance duties. When a Policy Authority is the same as an overall governing body for an organization, there will be fiduciary duties owed by each individual member to execute the mission of the organization above other goals. The form of an electronic commerce transaction will be a means to an end. The form should follow the function of the organization. In other words, choice of a PKI model and drafting the related Certificate Policy will necessarily be subject to the business needs of the organizations that are served by this enabling technology. Though several models for the use of PKI have been put forward by theorists, these Guidelines explicitly suggest that business people seeking to implement a PKI system do so in a manner primarily consistent with their business rather than based upon a preconceived model of PKI. A detailed examination of several business conditions that may effect the Certificate Policy drafting process is conducted in Part Part D. Implementing a Business and Legal Model, below.

B.2.2 Promulgation of Policy as a Function of Governance

A Certificate Policy will include sections detailing the manner in which the Certificate Policy may be amended, the party responsible for the Policy, and other matters bearing on matters of governance.[6] The determination of these policy questions is a function of governance. These Guidelines refer to the party charged with governance functions as a Policy Authority.

[6]For example. Part E of these Guidelines. “Drafting a Certificate Policy,” incorporates provisions for the listing of “the name and mailing address of the authority that is responsible for the registration, maintenance, and interpretation of this certificate policy” (see Section 1.4) and for the listing of a “specification administration” organization that lists responsibility for procedures necessary to amend the policy, publications or notices and certain approval procedures for relevant documents (see Section 8).

A Certificate Policy, not unlike any other important policy and business decision, will be set in the context of a complex and interrelated set of conditions effecting the rights, obligations and mission of an organization. At the core, a Certificate Policy describes how a Policy Authority governs the parties, scope of business, functional operations, and the obligations of PKI Service Providers and End Entities who engage in electronic transactions. Such matters are not driven by PKI implementations but are based upon the duty of a governing body to carry out the mission of its organization in a sound and prudent manner.

The assumption of these Guidelines is that organizations have business, government, or public interest missions and it is not the mission of an organization to use and promote PKI. Rather, the use of PKI will be for the purpose of securing and authenticating communications and data interchange that is of relatively high value, sensitive, or otherwise important to the mission of the organization. Thus the governance decisions regarding the content of a Certificate Policy will be subordinate to the interests of the underlying communications and transactions, especially with respect to the obligations between “users” or “End Entities.”

B.3 The Structure of Governance

The Policy Authority has ultimate responsibility for specifying the Certificate Policy. The Policy Authority can be described as the governing body, or the designee thereof, which is tasked with promulgating the Certificate Policy in a manner that supports and reflects the needs of the underlying relationships and transactions.[7] Authoritative policy is promulgated by a policy making entity. This entity derives its authority from the governance structure of the organization on whose behalf it sets policy. A governing body may delegate some authority to executive decision makers, but matters that are fundamental to the mission and existence of an organization can not typically be delegated.

[7]Examples of governing bodies abound. For instance in a corporation, the governing body is said to be the Board of Directors. Academic institutions often have a Board of Trustees as a governing body. Governmental entities at the state and federal levels are said to gain their power from the consent of the governed as expressed in the Constitution and implemented or interpreted by the Executive. Legislative and Judicial branches which comprise the governing bodies.

It is customary for governing bodies to subdivide aspects of governance to such lesser groupings as Committees. Councils and Boards. It is often necessary that such lesser grouping be entirely or partially comprised of full members of the governing body. In a given organization, a governing body may chose to have a Certificate Policy promulgated by an Information Technology Committee or an Electronic Commerce Board. A small organization may require a Certificate Policy to be set and approved by the full governing body. A larger organization may only require such policy to be approved by the governing body. Alternatively, a governing body may delegate authority to make such policy to an executive officer. In all cases, this type of policy is made by a governing body or the delegate of the governing body.

For purposes of simplicity, these Guidelines assume that the exercise of governing authority necessary to promulgate a Certificate Policy is in fact performed by a governing body of some sort. In other words, the Policy Authority empowered to draft or select a Certificate Policy would be a governing body, at least with respect to the subject matter contained within that Certificate Policy.

In some situations, different parties may seek to organize a new representative organization with an independent scope of authority and governance structure for the purpose of setting the business, legal and technical decisions related to promulgating a Certificate Policy. Especially in the case of organizations that are engaged collectively in electronic commerce as a fundamental aspect of their mission, their Certificate Policy may be of sufficient importance to warrant formation of a consortium or other legal body to specify and maintain the policy. Electronic commerce implementations may require a web of relationships that spans traditional organizational boundaries and jurisdictions. This, in turn, may require multi-party cooperation, new business partners, leveraging and consolidation of existing infrastructures and in some cases, evolved organizational structures (see, for example, the section below on “Custom Governance Structure”). Generally, however, these Guidelines assume that parties will seek to use PKI to facilitate business within an existing governance structure and that an organization's governance structure will not be materially changed in the short term as a result of using PKI.

Although a Certificate Policy document as a whole is promulgated by a governing body, some elements specified in such a policy should be resolved in the server room rather than the board room. For example, Section 7.1.8 of the PKIX Framework, detailing the “policy qualifiers and syntax semantics” may be an important matter, but probably not an Issuer requiring (or capable of receiving) direct policy determinations at the governance level of an organization. Highly technical issues will probably be initially specified by technical staff.

However, matters like determining the scope of community and applicability; obligations and liability of the parties; fees and financial responsibility; and the confirmation and identification of certificate applicants are fundamental policy issues that require decisions by a those with responsibility to steer the organization. There is no bright delineation between important and trivial usage of PKI. As a rule of thumb, consider whether the Certificate Policy materially effects high value, sensitive or mission critical relationships and transactions. Alternately, a risk, benefit and cost analysis can be performed to determine whether the systems governed by the Certificate Policy are of sufficient relevance and value to warrant formal, high level oversight and approval. If so, then the role of Policy Authority should be fulfilled by one or more members of the governing body or their delegate. For purposes of these Guidelines, it is

assumed that the value and relevance of the Certificate Policy is such that formal policy making channels are necessary and appropriate.

B.4 Form of the Policy Authority

As a governing body, the form of the Policy Authority will be of critical importance to any given business system operating under a named Certificate Policy. The form of the Policy Authority, including whether it is constituted as a representative association of multiple-parties or a single party, has significant practical ramifications. In the first instance, organizers should begin an inquiry into the proper form of a Policy Authority by ascertaining the form the controlling party or parties that contemplate organizing and sponsoring a PKI.

B.4.1 Example Policy Authority Choices from Current Certificate Policy Drafts

The following examples illustrate how various organizations that have published draft Certificate Policies have approached the sections detaining the "Specification Administration Organization" listed in section 1.4 of the PKIX Framework.[8]

[8]As shown in these examples, some policy drafters have opted to call this party a "Policy Management Authority." These Guidelines use the shorter term "Policy Authority" for the sake of brevity and also because it is felt that management of a policy can be considered as a lesser included function of setting policy. Policy implementation and other management issues can be delegated or sub-contracted to a project management or other organization. The ultimate authority and responsibility for making fundamental policy, however, may be considered a non-delegable fiduciary duty of the Policy Authority as a governing body of an organization.

B.4.1.1 U.S. Department of Defense

"A Policy Management Authority (PMA) [whose membership is to be determined] to be determined [*sic*], is responsible for definition, revision and promulgation of this policy. Until the authority is established, the National Security Agency is responsible for definition, revision and promulgation of this policy. The organization to be contacted is…"

B.4.1.2 Government of Canada

Digital Signature and Confidentiality. Certificate Policies for the Government of Canada Public Key Infrastructure. V2.0. August 1998:

"This certificate policy is administered by the Government of Canada PKI Policy Management Authority. Treasury Board Secretariate, Ottawa, Ontario, Canada. The contact person is…"

[NOTE: this certificate policy includes a definition of Policy Management Authority that provides as follows: "A GoC body responsible for setting, implementing, and administering policy decisions regarding CPs and CPSs throughout the GoC PKI."]

B.4.1.3 NACHA

National Automated Clearing House Association. The Internet Council, Authentication and Network of Trust Pilot Program, Certificate Policy:

"This Policy is administered by the National Automated Clearing House Association."

B.4.2 Single Party Policy Authority

The single party natural person is the most simple possible entity. This would be the case of a sole proprietor as Policy Authority. It is far more foreseeable, however, that the party assuming the role of a Policy Authority will be a more complicated legal entity. Any legal person may perform the role of a Policy Authority. Legal persons may include corporations, partnerships, trusts, unincorporated non-profit associations, government bodies and other organizations. While more than one natural person may play

an active part on behalf of such an organization, this would still be considered a single party. Of the several characteristics that are associated with the term “legal entity” two critical for purposes of eligibility to conduct the business of a Policy Authority include: the capacity to form binding contracts and the ability to sue and be sued.

B.4.3 Multi-Party Policy Authority

Still more complex than a single organization serving as a Policy Authority would be the case of multiple organizations joining together to fulfill the functions of this role. Multi-party governance can be relatively informal. This could occur through informal mechanisms, such as a memorandum of understanding or, at a slightly more formal level, a memorandum of agreement. For example, the current practice for organizing multi-state procurement often involves only a short memorandum of understanding. Of course, the underlying bid process, project awards and contracts are considerably more formal in nature. However, there is no need for more formal documentation of the intent to collaborate on multi-state procurements given the relationship of the parties: co-equal, large and sophisticated organizations with interdependent histories. When different organizations join together for purposes of collaborating, it is typical that each organization maintain the right to cease collaboration. Given the voluntary nature of such collaboration, oppressive or rigid governance mechanisms are usually unwise and unwelcome.

When separate organizations chose to approach policy specification of a PKI jointly, it may be advisable to structure joint governance mechanisms. Such governance mechanisms as approval by a certain number of parties or the granting of limited veto rights could be afforded. The issue arises: what would prevent any party from violating an understanding related to performing Policy Authority functions (such as by attempting to substitute different terms of a Certificate Policy than have been agreed upon or agreeing to cross-certify a different PKI without abiding by some process that has been specified). To reach higher levels of assurance, it may be advisable to enter into formal contracts. Based upon contract law, one could compel conduct in compliance with the agreement or possibly prevent conduct in breach of the agreement, or potentially gain compensation for breach. In some cases, it may be advisable for disparate individual parties to form a new single legal entity for the purpose of jointly carrying out the functions of the PA. (see: custom governance below).

B.4.4 Inherited Governance Structures

Today, there are far fewer people who use PKI than people who do. Internet usage, while enjoying radical adoption rates, is also just beginning to hold the market penetration of other more traditional commercial media, such as voice telephony, facsimile and document delivery by land and air. Organizations that begin using PKI to enable business transactions will already have a governance structure. From the point of view of an organization that seeks to make a business by being a PKI Service Provider, several questions will be relevant, such as: What is possible and impossible under existing structures? How much room exists to amend? Is it possible to outsource the policy drafting and administration functions so as to achieve all aims through contract rather than amendment of by-laws? If change in legacy governance system is required, how well or poorly do the PKI roles assumed by the PKI Service Provider overlay to the existing governance?[9]

[9]An example of a proposal to amend a governing structure to facilitate the use of advanced information technologies within an academic institution occurred at UCLA. The UCLA proposal includes detailed recommendations on the IT Organization and Governance Structure (including a governance board and details of several new reporting relationships involved). The UCLA plan would interrelate existing governing bodies (such as offices of the Executive Vice Chancellor) with newer governing bodies, such as an Information Technology Planning Group. (the plan can be found at the following address: http://www.aitb.ucla.edu/itplan/GenMgmt.htm). As in case of UCLA proposal, there may be need to mold existing governance with new governance bodies in an organization that inherits a governing structure.

B.4.5 Custom Governance Structure

Customizing a governance structure to accommodate a PKI facilitated electronic commerce community poses opportunities and challenges. Parties may seek to organize a new legal entity to act as the Policy Authority for any of the following reasons:

- More favorable tax treatment and relief from regulatory obstacles;
- Structured method of collaboration that avoids anti-trust violations;
- Limitations of some forms of liability exposure for participants;
- Member rights and duties that are fair and predictable for large and small participants.

When an organization makes a determination that a new governance structure is required or desirable for purposes of conducting the functions of a Policy Authority, then it is possible to exercise some creativity and latitude in structuring the governance in such a way that it reflects and supports not only the underlying business conditions, but is also tailored to the functions and roles associated with the use of PKI. One approach may be to include seats on a governing board for representatives of each role played in a given PKI.

For example, in the four-cornered model, one might reserve governance positions for one or more parties playing the Issuer, Repository, Relying Party and Subscriber roles. If the issues surrounding governance are too sensitive to allow representation for some or all of these parties, then other governance mechanisms, such as associate non-voting status or membership on an advisory council could be created.

PART C. Building a Business and Legal Model

Once the Policy Authority is formed and active as described in Part B, one of its initial tasks will consist of formulating a conceptual model describing what the participants will do in the project or endeavor that is the Policy Authority's charge. Customs and general industry practices have not yet evolved to the point that the architecture of the business system to carry out the project can be assumed—there is no tried-and-true, textbook approach to organizing the participants in a public-key project. That organizing of the participants must provide not only profitability and general economic efficiency but also a solid legal footing and enforceability for the expectations of the parties.

This part considers how the Policy Authority can organize the participants and structure their interrelationships within a public-key-enabled project. In other words, this part is about how to architect and conceptualize a business-legal model for a public-key business application.

C.1 Basic Conceptual Building Blocks

Once a Policy Authority has determined the objectives of a project, it needs a means to realize them. Public-key technology offers significant utility in securing and authenticating digital information, but it is entirely dependent on human actors doing certain things. In architecting an organizational model, those *functions* that people must perform in order for the technology to be useful and valuable must be assigned to *roles* in the model. The model must also envision a way for actual, real-world *parties* to take on those roles by forming legally binding *obligations*. More specifically, with the project objectives in mind, the Policy Authority's organizational model-building follows more or less these steps:

- **Derive functions** from the operational requirements of the public-key technology. For that technology to work, certain things must be done by devices and the people or business entities that run those devices. That list of *functions* or things that must be done for the technology to work valuably is the starting point for a business-legal framework for a publickey business application. The derivation of functions from roles has much to do with how usefully the technology will perform in the project.
- **Allocate functions to roles.** The Certificate Policy assigns the functions that must be performed for public-key technology to work to classes of participants. Those classes or *roles* should be labeled and their functions and qualifications described. Often, that

labeling and describing occurs in defining role-terms such as “Enrolled Subscriber” or “Authorized CA.” The allocation of functions to roles tends to determine how smoothly and economically the organization will run.

- **Engage parties into the roles through binding obligations.** Persons interested in a project become actual, committed participants by becoming parties to contracts or by becoming subject to other legally binding requirements that impose enforceable duties. *Obligations* are legally binding commitments that could be enforced judicially in case of a failure to perform according to the commitment. *Parties* are the persons who are thus committed.

- **Resolve disputes if an obligation is breached.** In this part, *liability* refers to an obligation which an authoritative tribunal has determined to be unconditionally due and unsatisfied. The tribunal accordingly orders a *remedy* such as monetary damages to correct or compensate for the liability. The collection or other actual realization of a remedy depends on a tribunal's ability to gain jurisdiction to resolve the dispute, which ultimately rests on its power to have its orders enforced by coercion if necessary. The effectiveness of the remedy also depends as a practical matter on the financial responsibility of the person liable.

The next sections examine these steps in greater detail.

C.1.1 Functions Allocated to Roles

Functions, the tasks that devices and/or people must perform for a public key infrastructure to work effectively, derive from the limitations of public key technology, because certain events or conditions must occur for that technology to be useful. For example, public-key technology makes possible verifiable message authenticity or confidentiality, but one of its chief limitations lies in the fact that the cryptographic key pairs used in public-key technology are really only mathematically related numbers. Of themselves, they have no association with any person whose authentication or confidentiality would be valued. Public key certification overcomes this limitation by associating a person with a specified public key, and many functions derive from the needs implicit in effecting that association in valuable, meaningful ways.

In general, the functions necessary to make public-key technology useful include:

- **Key generation and safekeeping**: Public keys and their corresponding private keys need to be generated before they can be used. The utility of public key technology depends heavily on the ability to attribute usage of a particular private key to a particular person or persons, and the attributability of private key usage is undermined by the ability of unknown or unauthorized persons to use the private key. To assure sound attributability, the private key needs to be generated and kept in a way that precludes to a reasonable[10] extent access by persons who are not certified as holding that private key.

[10]As used in these Guidelines and in several other legal publications such as the ABA Guidelines, “reasonableness” and “trustworthiness” imply a balancing of available security measures in relation to the foreseeable need for them. Information security is generally a matter of degree, and as applied in a particular situation the degree of security should take into account the business objectives and needs of a project, benefits that could be gained by further security, and the foreseeable cost including the risk of loss, as well as any other relevant factors. The risk depends on the probability of a loss-causing event, the seriousness or degree of harm the loss would foreseeably present, and the methods that would be available for averting or short-stopping a loss once it begins to accrue.

- **Information acquisition and confirmation**: Information to be listed in a certificate, such as information identifying the Subscriber, needs to be gathered from available sources and confirmed. “Confirmation” implies a level of investigation and inquiry into the accuracy of the information that is reasonable in light of the foreseeable need for accuracy. Often, an applicable Certificate Policy and/or certificate will specify the level of confirmation more precisely.

- **Certificate creation**: The information to be certified, such as names and addresses identifying the Subscriber and stating the public key corresponding to the Subscriber's public key, needs to be expressed in a digital form usable by the intended users and/or applications. The generally accepted certificate form in current practice is specified in ITU X.509. That form requires certain data content and, in very broad categories, the meaning of that data, which will need to be clarified to be fully understood by all participants.

- **Certificate signing**: Once formed, a certificate must be digitally signed or secured in a way that makes it attributable to its Issuer and which makes subsequent alterations of it detectable.

- **Certificate distribution**: The persons who create certificates or who use the related private key are sometimes not the same as the persons who rely on certificates, or at least, their roles are distinct and separable from a business-legal perspective. Consequently, a need exists to distribute certificates to prospective Relying Parties.

- **Certificate revocation**: A certificate may become unreliable after it is issued, or may be issued in error. For example, if the Subscriber listed in a certificate loses control of the related private key, a digital signature created by that private key will not be reliably attributable to the Subscriber as a matter of fact (although attribution may nevertheless be permissible by legal rules until the Subscriber takes appropriate action). Often revoking the certificate (*i.e.* invalidating the certificate from a specified time forward) is the best recourse for a lost private key or a certificate that is apparently effective but nevertheless unreliable.

- **Claims, dispute resolution, and risk management**: Errors in certification on an industrial scale are inevitable, and claims based on those errors are to be expected. Mishaps, losses, or other performance difficulties may lead to disputes that will need to be resolved through an adjudication, arbitration, or similar process. The prospect of losses amounts to a risk that will need to be minimized, but even the best risk minimization will not cost-effectively reduce the risk to zero. A residual risk will need to be financed through means such as insurance, reserves, pooling or other risk-spreading arrangements, or a combination of such means.[11]

[11]Simply shifting the risk to a party not obligated to bear the risk could violate the basic premises of the business model supporting the public-key application. An effective certificate policy and its implementing contracts will eliminate loopholes that permit parties to evade their obligations and shunt risk to others who, under the business model, do not expect to bear the risk.

This list is only partial and its items sketch certification functions only broadly and superficially. Since the function-to-role allocation is effected in the Certificate Policy and its implementing contracts, generally the Policy Authority takes the lead in making that allocation.

The allocation of technology-based functions to roles can occur in varying ways. Multiple conceptualizations of functional roles in various public-key infrastructures have been proposed, and more could be envisioned. Currently, no single, generally accepted formula for allocating functions to roles can be said to predominate over other alternatives, so the possibilities in designing roles are quite unconstrained by convention. However, practical constraints exist, in addition to the objectives of a particular project, or perhaps, in furtherance of those objectives.

C.1.1.1 Considerations in Allocating Functions to Roles

The practicality of a function-to-role allocation and its success in the marketplace will depend on factors such as:

- **Economic efficiency**: Generally, functions should be grouped together and allocated to a participant in a position to perform the function at the least cost.[12] For example, functions that require proximity to remote Subscribers should be allocated to a role that can

operate in a decentralized fashion. Where accumulation of information facilitates one-stop referencing, the opposite is true and centralization is advantageous. Centralization versus distribution, availability of necessary resources (such as evidence necessary for confirmation, financial or risk-bearing capacity, secure operational capacity, degree of sophistication, ability to bear costs, etc.), and other economically significant characteristics of the stakeholders in the project bear heavily on the overall economic efficiency of a function-to-role allocation.

[12]"Cost" is intended here in an abstract, economic sense, and not in the sense of a price in a purchasing context.

- **Clear risk and loss allocations**: If a party cannot clearly and precisely ascertain its risk, prudence may lead it to take steps to carry more risk than it actually bears. For example, it may take security measures to reduce the chance of an event that would cause a loss that, as it turns out, someone else would suffer, or it may obtain insurance to cover such a loss. The consequences of carrying a risk that, due to fuzzy definition, one does not actually bear is economic inefficiency (incurring unnecessary costs), as well as confusion in allocating losses. That confusion leads to conflict and disputes.

- **Conflict avoidance and resolution**: The likelihood of conflict can be reduced and the resolution of conflicts can be eased by making clear distinctions between functions and forensically traceable hand-offs where functions interlock between roles. Overlapping or splitting of a single function between multiple, excessively independent roles can make decision-making complicated; deadlock and buck-passing more likely; and fault and loss more difficult to apportion fairly. However, if decision-making is shared in a group acting according to orderly and efficient procedures, the quality of decisions may increase as well as the control over and shared responsibility for them, all without intolerable additional cost in time and resources.

- **Operational controls and failsafes**: Without splitting or confusing control and responsibility for performing a function, it may be possible to create control points and failsafes to prevent errors or trap them as they occur, or at least before they become harmful. Sometimes functional role relationships can be designed so that one role checks or backs up another. For example, process flows can often include multiple steps such as expect-to-receive, send-and-receive, and acknowledge-receipt, and employee tasks can be scheduled to create a desired level of redundancy. Controls and failsafes, like system security and other risk-minimization techniques, come at a cost, and whether the cost is worthwhile ultimately depends on the Policy Authority's business objectives.

Many other considerations may be relevant in allocating functions to roles, including the needs and preferences of people involved in a particular situation, regulatory requirements, and cultural predilections.

C.1.1.2 Examples of Function-to-Role Allocations

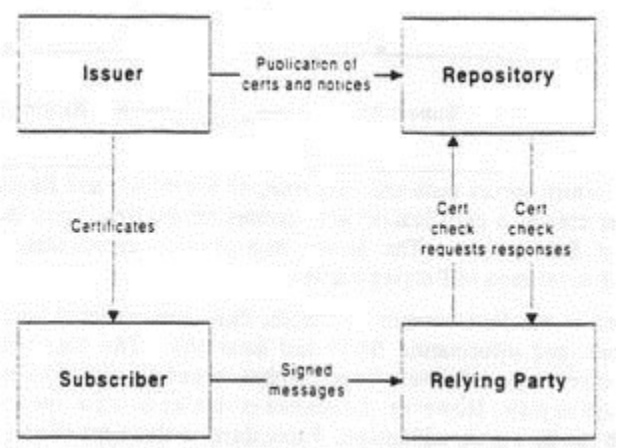
To illustrate how a Policy Authority can design an allocation of functions to roles, this subsection overviews two examples, one diagrammed with three corners and another with four.

These examples are nothing more than illustrative possibilities, and these Guidelines make no recommendation regarding any function-to-role allocations.

C.1.1.2.1 A Four-Cornered Example

This example allocates functions such as issuance and revocation to the role termed *Issuer*. The role defined as the person whom the Issuer associates with a key pair by means of the certificate is the *Subscriber* of the certificate. The work of disseminating certificates, notices of revocation, and related information to parties who may rely on them is performed by a *Repository*. A Repository can also assist

Relying Parties in other ways besides making information available, such as by helping them observe the limitations of a certificate's trustworthiness or assurance or enabling them to obtain further assurance.



These roles and a few basic functions can be diagrammed as a four-cornered structure:

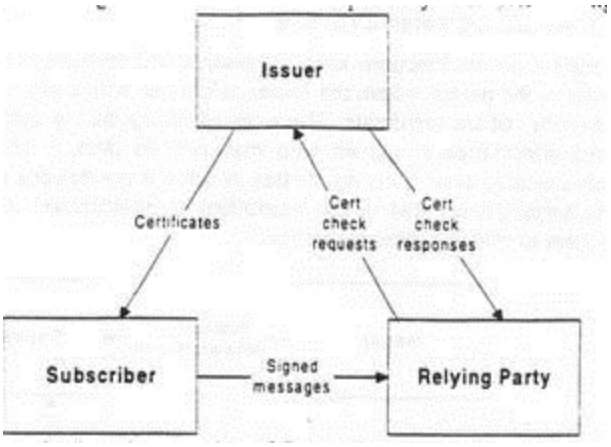
The basic roles of this example—particularly the role of Issuer—are often divided or reallocated into additional roles such as Registrar and/or Certificate Manufacturer, depending on the needs of various projects and the business plans of a particular enterprise. Further, Subscribers and Relying Parties are sometimes together termed “end users” or “End Entities,” and issuers and repositories, as well as Registrars and Certificate Manufacturers, would all be “PKI Service ProviderPKI Service Providers” as that term is used in these Guidelines.

A more detailed examination of the basic four-cornered model follows in section C.2. A Closer Look at the Four-Cornered Model, below. Again, the purpose of including this example is not to mandate or even recommend its usage. Rather, it is merely an illustration.

C.1.1.2.2 A Three-Cornered Example

As a further illustration, this subsection outlines a function-to-role allocation consisting of three principal roles. It can be diagrammed as follows:

In this model, the roles designated “Issuer” and “Repository” comprise a single role designated “Issuer,” which serves both end-user roles of Subscriber and Relying Party. More specifically, the Issuer creates a certification key, creates certificates, signs them, and sends them to their respective Subscribers. The Issuer also revokes certificates, and disseminates notice of certificate revocation to Relying Parties.



Compared to the four-cornered example, this three-cornered structure is simpler in structure, obligations, and information flows and hand-offs. The four-cornered model scales well for projects involving a relatively large number of participants, a variety of transactions, and rather high values in play. However, if a project is smaller in scale, the simplicity of the three-cornered approach can be a great advantage. Particularly in this time of early public-key implementations and pilots, projects often center around a single or a few transactions and a relatively small group of cooperative participants. In such a project, the Policy Authority may well determine to do without differentiated roles for PKI Service Providers, and have a single service provider take care of all PKI functions.

Often, as in the case of the four-cornered model summarized above, the Issuer role or other functions of a PKI Service Provider are modularized into several smaller roles, although keeping all the functions together in the same role provides simplicity, which could be desirable in a pilot, especially if its scale is small. Perhaps the most commonly employed smaller role is that of Registrar. Registrars obtain information from Subscribers for use in certificates, and may also perform other functions involving interaction with Subscribers, such as contract formation, receiving revocation requests, and customer service.

These multi-corner examples illustrate various ways for allocating into roles the basic functions that need to be accomplished for public-key technology to be valuably employed. That function-to-role allocation is the initial step in the organizational engineering necessary to build a publickey infrastructure into a project. Once functions are allocated to roles, the roles need to be accepted by actual parties and hardened into binding legal obligations.

C.1.2 From Roles to Obligations and Parties

Obligations are legally binding duties, and the persons that they bind are termed “parties” in these Guidelines. (Parties may also be “stakeholders” if they have an interest in the project sufficient to make them constituents in or members of the Policy Authority.)

A Certificate Policy, as usually drafted, often does not name its participants, and it rarely commits them to perform their roles with binding legal force. By itself, a Certificate Policy is generally not legally binding, unless it is imposed by sovereign power such as through statutory enactment or regulatory adoption. Without sovereign imposition, the parties can bind themselves to obligations by agreeing contractually to be subject to the Certificate Policy. In the absence of contracts or sovereign enactments, the courts will extend generally applicable legal principles, called the “common law” in the Anglo-American tradition, to cover issues arising in public-key applications.

All of these approaches toward achieving binding legal effect for a Certificate Policy are problematic. The common-law doctrine most likely to be extended to cover public-key applications relates to negligent misrepresentation. That particular doctrine is exceptionally vague, and varies greatly from state to state.[13]

Statutes and regulations are generally difficult to obtain, especially on the international level needed for the present, worldwide economy. Moreover, legislatures or regulatory agencies can fall short of the responsiveness needed to facilitate legitimate business objectives. Contracts must be formed in a required way and on a party-by-party, one-by-one basis, and must fall within certain limitations (such as laws protecting consumers) to be valid and enforceable. All of these means of achieving binding legal effect have drawbacks, but the means perhaps least disadvantaged, particularly for private-sector projects of limited scale, is the contractual alternative. These Guidelines assume, as a basic premise, a preference for contractual approaches toward achieving binding legal effect.[14]

[13]*See* Froomkin. The Essential Role of Trusted Third Parties in Electronic Commerce, 75 ORE. L. REV. 49, 96–103 (1996).

[14]Reliance on contracts to achieve binding legal effect does not rule out other approaches—the question of how to make a certificate policy legally binding is not an either-or question. It is possible to rely in the first instance on a contractual approach and also to rely on a statute such as Utah's as a backup. One can also consider the common-law outcome in the event that both the contract and statute fail to accomplish the requisite binding effect.

C.1.2.1 Contracts and Accounts

A contract that gives binding legal effect to a Certificate Policy is termed an “implementing contract” in these Guidelines. As mentioned, contracts must be formed in a particular way. This section considers contract formation, the implications of the one-by-one approach required for contract formation, and the implications of the relationships that implementing contracts establish beyond the mere incorporation of a project-wide Certificate Policy.

C.1.2.1.1 Contract Formation

In a common law legal system formation[15] of a contract generally requires:

[15]A contract, though formed according to these rules, may be rendered invalid or unenforceable by another rule. For example, statutes commonly termed “statutes of frauds” in the Anglo-American legal tradition forbid enforcement of contracts not expressed in a signed, written form. Consumer protection statutes, common-law restrictions on the enforcement of illegal or unconscionable contracts, and other rules all limit the basic power to make effective contracts.

- **Parties**: Persons (including corporations, government agencies, or other legally recognized juridical entities) who have the legal capacity to contract (*i.e.* are not under the age of majority, adjudicated to be mentally incompetent, or subject to some other legal disability).[16]

[16]*Harrison v. Grobe*, 790 F. Supp. 443, 447 (S.D.N.Y. 1992); *Daniels v. Thomas, Dean & Hoskis, Inc.*, 804 P.2d 359, 363 (Mont. 1990); *see generally* RESTATEMENT (SECOND) OF CONTRACTS §§ 12, 16 (1991).

- **Mutual assent**: The parties to the contract must come to an apparent[17] agreement or “meeting of the minds” on the essential terms of the contract.[18]

[17]An actual, subjective agreement is not required, and the real content of any party's mind at the time of contracting is irrelevant. What counts for contract formation is a *manifestation* of assent, and contract formation is judged by objective criteria. Thus, having evidence of the manifestation of assent is important but undertaking the difficult task of proving what was on anyone's mind at the time the contract was made is unnecessary. *See Zeman v. Lufthansa German Airlines*, 699 P.2d 1274, 1281 (Alaska 1985); RESTATEMENT (SECOND) OF CONTRACTS § 17 cmt (1991).

[18]*Federal Lumber Co. v. Wheeler*, 643 P.2d 31, 36 (Co. 1981).

- **Consideration**: In the Anglo-American legal tradition, a contract must rest on a bargain that is not wholly one-sided, and the law does not protect commitments that are entirely gratuitous.

These contract-formation requirements, other than the requirement of consideration, generally hold true in legal systems outside the Anglo-American tradition as well.

The mutual assent required for contract formation is often indicated by signing written agreements (either with ink or digital signatures), or can be accomplished suitably by another means of manifesting assent in a provable manner. A written or other clear, recorded expression of the agreement helps achieve clarity

and precision in defining the parties' obligations, which in turn makes those obligations easier to perform. Besides a clear, provable expression of obligations, mutual assent requires expression of each party's intent to be obligated. That intention is customarily implied from a signature, but the person offering the contract may, within fair limits,[19] define it to be another act.

[19]One would-be party's power to treat some events as manifestations of assent is limited by fairness considerations. Generally, silence or inaction by one party do not indicate assent. However, assent can be indicated by "acceptance of the benefit or offered services with reasonable opportunity to reject them and reason to know that they were offered with the expectation of compensation." *See* RESTATEMENT SECOND OF CONTRACTS § 69 (1981).

More concretely and assuming the four-cornered model, contract parties can indicate mutual assent and form contracts in the following ways, among others, depending on the needs of a particular project:

- **One-stop double enrollment**: When a person agrees with an Issuer to be a Subscriber, the person can also agree to be a Relying Party. Issuers, perhaps acting through Registrars, may well have direct, personal contact with their Subscriber-customers, and signing a written contract in the traditional manner is not difficult in those circumstances. The relying-party contract can also provide for use of the Repository, although agency or another arrangement will be necessary if the Repository is provided by a party other than the Issuer.

- **Online, digitally signed contract**: If a person, particularly a prospective Relying Party, approaches a contract-based system online and has a digital signature capability, the person can use that digital signature to accept and sign an online offer from the Repository presented via a Web page.

- **Clickwrap**: In some situations, contracts can be formed by clicking an on-screen button labeled "I agree" or making a similar manifestation of assent by entirely electronic means.[20] The document proffering the contract and its agreement button should optimally record evidence for subsequently proving that the contract-formation event occurred. Such evidence should include the system date on which the agreement button was clicked, the user's login identification, the user's network node name (*e.g.* current domain name) and address (*e.g.* current Internet protocol address), etc. The agreement process can also ask for user information and require a password, although confirmation of the information thus obtained will be problematic in an online, clickwrap setting.

[20]See generally T. Smedinghoff, ONLINE LAW 81–83 (1996).

Many variations of or alternatives to these examples are possible. The essential requirements for forming contracts require simply a manifestation of assent by suitable parties to a bargain, and online contracting opens needs and possibilities for creativity in making and documenting such manifestations.

C.1.2.1.2 System Uniformity and Closure

One implication of the contract-formation process just described is the fact that contracts must be made one by one. They can have more than two parties, but all of the parties must complete the assent process for the contract to be validly formed. Moreover, the greater the number of parties involved in a contract, the more difficult it is to amend or terminate it, or to resolve disputes that would otherwise concern fewer people.

The one-by-one nature of contracting makes it difficult to be certain that all participants in a project are bound by its rules, including mainly its Certificate Policy.[21] Achieving assured closure of a system of participants is particularly difficult in the case of Relying Parties. In that regard, see section C.2.4, below. Achieving a desirable level of system closure may necessitate a preclusion of reliance on certificates by prospective Relying Parties who cannot demonstrate that they have contracted for participation in the system, and the section just referenced describes various means of precluding that reliance.

[21]See generally Greenwood. Risk and Trust Management Techniques for an "Open But Bounded Public Key Infrastructure. 38

JURIMETRICS 277, 287–92 (1998).

Making contracts one by one with all participants in a large system can also create challenges of scale. Large-scale contracting requires a tree-structured networking of the contract-formation process in order to reach the level of each individual party, and that networking will require management. One task of the contract manager will be to assure a sufficient degree of systemwide uniformity among the one-by-one contracts, so that they all add up to a coherent system of rights and obligations free of anomalies, despite the capability for individual parties and contracts to include provisions inconsistent with the overall scheme.

Moreover, since contracts are made only between those parties assenting to a given instance of terms, making the contract's efficacy reach all of the parties that it needs to is a further challenge. Contracts generally apply only between the parties to them (a concept lawyers call “privity”), and that limitation on the scope of a contract's binding effect creates a difficulty in scaling contract systems.

Despite all these difficulties, bankcard, automatic-teller, and clearinghouse systems demonstrate that large-scale webs of contracts are feasible. Generally, those systems have arisen after pilot projects and experience-gathering, a stage similar to the stage of public-key development as of this writing. From these small beginnings, they have grown to be worldwide networks of privately made legal rules, and they demonstrate convincingly the ability of contract-based systems to traverse legal-system boundaries in a cost-effective manner. These bankcard, automatic-teller, and clearinghouse examples also demonstrate the need for a central coordinating body. The Policy Authority can fill that role, as can any other agent trusted by all participants in the project to supervise the contract infrastructure.

Although a need to supervise contracting exists in order to establish a consistent and sufficiently extensive system of legal rights and obligations, the scope of that supervision and the limitations on contractual flexibility that it could impose need to be prudently bounded. Implementing contracts should incorporate the Certificate Policy and be consistent with it, but there is no reason to preclude implementing contracts from including additional provisions consistent with the policy to structure and govern the relationship between the parties. That relationship between a service provider and customer is the framework within which public-key services will be obtained and provided, and must have enough range and flexibility to achieve marketability and mutual economic advantage if public-key services are to be commercially viable.

C.1.2.1.3 Ongoing Relationships: Accounts

As just mentioned, an implementing contract essentially establishes a customer relationship. In conventional banking parlance, that customer relationship is termed an *account*.[22] In the four-cornered model, for example, a Subscriber's account is with an Issuer and a Relying Party's account is with its service provider, a Repository. Since an Issuer publishes its certificates into a Repository, it has a publisher's account (as distinct from a relying-party account) with the Repository. Contractually established rights and duties between the Issuer and Relying Party are also necessary, and must be established either by the Repository acting on the Issuer's behalf or by the Issuer directly, as explained below in section C.2.4.

[22]The “account” concept is common in the banking business, but other business traditions may well opt for other approaches to customer relationships. The description of the account concept here is not a recommendation.

Accounts establish ongoing, potentially long-term relationships. They thereby make possible the tracking of an account history, which can greatly enhance an Issuer's ability to confirm the accuracy of information in certificates, and serve other functions as well. It is relatively easy to perpetrate a quick fraud on an Issuer, but to maintain the fraud over time, through various transactions, and from one certificate through the next and the next, is considerably more difficult. Because certified information is most efficiently confirmed on a per-account basis, any number of certificates containing that information can be issued for the account. A prudent Issuer will also manage its certification risk on a per-account basis, cumulating across the whole account the risk of all outstanding certificates for the Subscriber or account holder.

Thus, to sum up the need for contracts and the account-relationships that result from them, the Policy Authority designing a business-legal model needs to provide a way to firm up functional roles into legally binding and enforceable obligations and rights. Contracts are a means to that end, but require design of a process to form all the necessary contracts and to manage that process of contract formation and the enforcement that flows from it. That management process should not, however, prevent vendors competing in the marketplace from developing commercially viable product offerings. Stifling creativity and innovation in customer relations among competing vendors will tend to hinder the effectiveness of the market in continuing the development of public-key infrastructures.

C.1.2.2 Certificates and the Problem of Certificate Meaning

Besides the implementing and account-establishing contracts, the certificates themselves have important legal significance and effect. Contracts are optimally made once per relationship, and amending or remaking them can be difficult, particularly in a large-scale system in which the contract-making network is large and widely distributed. Certificates issued in an account, on the other hand, are more current, and can more easily be tailored to the needs of a particular application or changing environment. Thus, contracts and the certificate policies they incorporate are ideally made once and for all and in rather general terms, but certificates adapt those generalities to a particular customer's or project's present needs and circumstances.

However, the expressive capabilities of certificates in their fielded, standardized form are extremely limited, so limited that it is not possible to know from the face of a certificate exactly what it means. Consequently, standardized certificates leave the rights and obligations of the parties, particularly of the Issuer and Relying Party, in substantial uncertainty. To solve this problem, a certificate profile (a specification of the fields, permissible content, and the range of permissible interpretation for those fields) for a particular certificate type can help make certificates understandable. In addition to or in lieu of a certificate profile, a documentary version of the certificate can place the certificate fields in a natural-language context and clarify their meaning. Such a documentary version of the certificate maps the certificate's fields into a documentary form, in which the declarative context implicit in the certificate is made explicit and clear.

An implementing contract must take into account the certificates to be issued pursuant to the contract and the interpretation to be given them. One way for the implementing contract to deal with the certificates to be issued is for the contract to provide for acceptance of those certificates (in the case of a Subscriber) or for reliance on those certificates (in the case of a Relying Party) in their documentary forms only. The contract thus becomes somewhat open-ended, allowing certificates to vary by type, application, and other certificate-specific circumstances, while the certificates all fall under the legally effectuating and perhaps long-term superstructure of the implementing contract and Certificate Policy.

Implementing contracts and the certificates issued under them (in their documentary renditions) are the legally effective instruments envisioned in these Guidelines as giving legal effect to certificate policies based on these Guidelines. In other words, implementing contracts and documentary certificates translate functional roles in an abstract architecture into binding obligations and enforceable rights. Enforcing those rights is the process of converting an obligation into a liability.

C.1.3. From Obligations to Liability and Legal Remedies

Legally, a significant difference exists between an obligation that is a mere promise, even if that promise is breached (*i.e.*, broken), and an obligation that has been adjudicated as due and immediately and unconditionally enforceable. This part terms that latter sort of adjudicated obligation a “liability,” and uses “obligation” to refer to a simple promise that is as yet unadjudicated and perhaps also unbreached.

The foregoing section concerned itself with the process of converting the functional roles of an abstract design into obligations in order to give legal effect to the functional roles in a public-key infrastructure. This section concerns itself with the conversion of obligations into liabilities, a process in which the obligation becomes fixed and collectable and any issues or conditions about it are resolved. Converting

an obligation into a liability requires a forum to conduct adjudication or a similar dispute-resolution process culminating in a judgment, order, or other award.

C.1.3.1 Choosing a Forum

In general, the parties, and often predominately the plaintiff, choose who will determine liability. The forum or tribunal can be judicial, in other words, the courts of a particular legal system. Which legal system and courts depends on where the party seeking enforcement (the plaintiff) can gain jurisdiction for the court over the defendant (the person against whom the claim of an unsatisfied obligation is asserted) or the defendant's assets. Within the United States, jurisdiction over a business enterprise can generally be established in any state where the enterprise has substantial business activity, and the courts of other states are obliged by the federal Constitution to give “full faith and credit” to the judgments of the courts in sister states. Internationally, jurisdiction is more difficult to obtain, and judgments more difficult to enforce in foreign courts. Moreover, concerns about national or parochial favoritism or other issues may lead to a preference for arbitration in resolving international disputes.

Arbitration is a process similar to adjudication, but is performed by one or more non-governmental officers agreed upon by the parties. Often, arbitrators are more specialized and expert in the subject matter of their proceedings than most judges. Arbitral proceedings are also somewhat less formal and time-consuming than adjudications. However, to compel enforcement of an arbitral award, an arbitral award must be converted into a judicial order by suing on it in a court having jurisdiction, although the court often will not fully review or reconsider the arbitral award, particularly if the parties have agreed that the arbitration would be binding.

Besides courts and arbitration, other forms of dispute resolution can be employed, but are less common in commercial contexts.

C.1.3.2 Remedies

Whatever the forum the disputants choose to convert a breached obligation into a liability, the forum will have the task of devising an appropriate method of redressing or compensating for the liability of the party breaching its obligation. An adjudication of liability holds that the breach occurred and requires redress, but it is another matter to devise a remedy that fits the liability and achieves appropriate redress.

Generally in the Anglo-American legal tradition, monetary damages compensating for liability are preferred over other possible remedies such as orders to perform or refrain from a specified act. Moreover, the monetary compensation generally covers only losses that the breaching party could reasonably foresee as of the time it should have performed.[23] Damages for an unforeseeable or indirect harm, such as an inability to take advantage of a lost opportunity, the consequences of a business interruption, etc., are termed *consequential damages* and are generally not recoverable unless an agreement requires otherwise. Moreover, in cases where tort liability is determined for a defective product, damages are generally due under the law of most states in the United States only for bodily injuries, not for purely economic losses.[24]

[23] *See Prutch v. Ford Motor Co.*, 618 P.2d 657, 661–62 (Colo. 1980); *Hadley v. Baxendale*, 156 Eng. Rep. 145 (Court of the Exchequer 1854); RESTATEMENT (SECOND) OF CONTRACTS § 351 (1981).

[24] *See Rockport Pharmacy, Inc.* v. *Digital Simplistics, Inc.*, 53 F 3d 195 (8th Cir. 1995); *Fireman's Fund Ins. v. SEC Donohue Inc.*, 679 N.E.2d 1197, 1199 (Ill. 1997); *Clark v. International Harvester Co.*, 581 P.2d 784, 791 (Idaho 1978), *see generally* R. R. Fox and P. J. Lottus. *Riding the Choppy Waters of East River; Economic Loss Doctrine Ten Years Later*, 64 DEF, COUNS. J. 260 (1997).

In considering the risk of nonperformance, it is important to consider not only whether an appropriate forum will conclude that liability exists for the nonperformance of an obligation but also what remedy that forum is likely to award. A delay in performing as obligated, for example, may clearly result in liability, but the foreseeable, direct harm caused by a minor business delay can be quite minimal, and therefore, the available remedy is also minimal.

However, legal liability and a legally appropriate remedy are only factors to consider in a dispute. Disputes have other costs, such as the cost of resolving them including attorney and forum fees as well as time, focus, and inconvenience. Conflict can also affect customer relations, especially if one side perceives that the other lacks merit. Each party needs to consider the overall business impact of each dispute in addition to its legal position.

C.1.3.3 Enforcing Remedies and Financial Responsibility

The breach of an obligation can be reduced to a liability for which a forum awards a remedy, but that remedy will not mean much if it cannot be collected or otherwise realized. An award of damages does not mean that the defendant has assets available to pay the damages, and the award, even though judicially ordered, can be discharged (*i.e.* ordered unenforceable) in a bankruptcy case. The ability of a PKI Service Provider to actually make good its promises through real assets is an important factor to consider in evaluating the trustworthiness of the service provider and the significance of its promises.

Various indications of commercial security (as distinct from technical security), credit, or creditworthiness can firm up obligations with real financial assurance. Bonds, standby letters of credit,[25] balance sheets and asset reports, and other indications of financial capacity help assure that a PKI Service Provider is able to satisfy its liabilities and form the foundation of commercial-grade trust.

[25]Bonds and standby letters of credit provide alternative source of funding from which damages can be collected, and that fact in turn, calls for a procedure for collecting the funds. A certificate policy requiring bonds or standby letters of credit should include an orderly process enabling multiple claimants to determine their respective priorities in the available funds.

C.1.4 Conclusion on Model Building Blocks

Putting public-key technology to work requires not only technology that functions securely but also an organizational model or framework capable of using that technology for business purposes in a way that comports with applicable law. Developing that organizational model can consist of allocating technologically based tasks to roles, firming up those roles into legally binding obligations, and enforcing those obligations as the need arises.

Many organizational models can be envisioned and have been suggested. Some have been outlined briefly in section C.1.1.2 above. One illustrative organizational model outlined in that section is the four-cornered model, which the next section examines in greater detail.

C.2 A Closer Look at the Four-Cornered Model

These Guidelines do not require or even recommend any particular model for the business-legal framework necessary for the public-key aspects of a project. The purpose of examining a model in this section is to provide a case study illustrating how the functions of public-key technology can be grouped together efficiently into roles, which in turn can be implemented contractually as obligations. While this case-study exercise may fit some actual business-legal models and certificate policies, it will not fit them all. Opinions vary quite widely, even within the Task Force authoring these Guidelines, about the optimal design of business-legal models for publickey applications. All those opinions tend to rest on theories unvalidated by actual, wide-scale experience in this era of pilots and early implementations. It is simply too soon in the emerging public-key industry to know from actual business experience which business-legal models work the best.

With that cautionary note, a detailed examination of the four-cornered business-legal model follows in this section, after brief consideration of the whole issue of how many corners.

C.2.1 Three Corners, Four, or More?

The examples briefly outlined in section C.1.1.2 above differ, not in the number of end-user roles, but rather in the number of separate roles broken out for PKI Service Providers. Particularly in early business-

legal models, the Issuer and Repository functions were not differentiated, but a Registrar's role often was. In the ABA Guidelines and Utah Act, separate roles were defined for Issuer (certification authority) and Repository, but a separate role for Registrar was hardly mentioned, although the ABA Guidelines recognized the possibility for a variety of "ancillary services."[26] Since then, certificate manufacturing (outsourced operational services in support of an Issuer) and other service-provider roles have gained attention. Clearly, there is nothing even an approaching a definitive or generally accepted division of roles for PKI Service Providers.

[26]ABA Guidelines § 1.2 (1995).

Examining all of the possible role divisions and models and weighing the merits of them all in relation to each other would exceed the scope of this introductory part, but an examination of how to go about building out a business-legal architecture would be too abstract if left at the highly conceptual level of the preceding sections. To illustrate an extensively elaborated business-legal architecture and stimulate thought about alternatives and variations, this section takes up the four-cornered model as a case study.

The three-cornered model summarized in section C.1.1.2 above has, compared to the fourcornered model, the advantage of greater simplicity, and may be easier to implement in pilot projects or projects in which one PKI Service Provider will perform both Issuer and Repository functions for the term of the project. Combining the Issuer and Repository roles also eliminates the need for clear hand-offs between the two roles. However, the four-cornered model, with Issuer and Repository functions allocated to distinct roles (which nevertheless could be performed by the same person), has advantages such as these relative to the three-cornered model:

- **Customer focus**: For the most part, the Issuer serves the Subscriber as its customer (albeit with great consideration for the Relying Party), whereas the Repository serves the Relying Party. The difference between the Subscriber and Relying Party roles is conceptually thorough, and their needs differ almost entirely. Consequently, the basic business objectives of the Issuer and Repository go in different directions.

- **Availability requirements**: Reliance happens more frequently than issuance, and the need for reliance support is therefore greater. It is also more difficult to predict or to constrain reliance within certain hours of the day in a particular time zone. Because reliance occurs frequently and around the clock, a Repository must generally be available 24 hours a day, seven days a week. However, the need to issue certificates at any unpredictable time is generally less than the need to rely on them at such times.

- **Online or offline**: Reliance requires online contact with the Repository over widely available communications channels. Issuance, however, need not be online, and is often performed offline for security reasons. A Repository is therefore an open, on-the-net service, whereas an Issuer provides service from a much less open, and often thoroughly shut up, information system.

- **Local or large and central**: An Issuer must generally have a presence local to the Subscriber, or at least with some direct contact with or proximity to the Subscriber, in order for the Issuer to confirm the accuracy of information about the Subscriber such as the Subscriber's identity. For example, an employer is often in an excellent position to identify its employees because of its familiarity with employees often over significant time periods. The proximity requirements of issuance and the much higher information quality obtained from primary, first-hand sources tends to make the centralizing and scaling of the Issuer role difficult. On the other hand, reliance on a certificate once issued is a global possibility, so a Repository needs to be ubiquitous. The need for efficiency will tend to give an advantage to centralization rather than distribution, in order to prevent hopping around from one location to the next in search of the needed data. Moreover, the utility of a particular Repository increases in proportion to the size of its data inventory, so repositories have an incentive to be large as well as centralized.

- **Risk model**: The value of public key certificates lies in the assurance they provide to Relying Parties, and that assurance translates to a risk for the Issuer. If certificates are valuable, they provide significant assurance and the Issuer undertakes a significant risk. Because of that risk, the expense side of the Issuer's business model will tend to resemble that of an insurance provider: a chance or probability of casualty losses plus operational expenses.[27] A Repository, on the other hand, bears little risk of fraud and the like. Instead, it has a risk of service interruptions, much like a that of a public utility.

[27]If certification risk is transaction-specific, it closely resembles other fraud risks that banks have long borne. For example, banks are familiar with the risk of paying an instrument over a forged endorsement, or making a wire transfer from an account based on fraudulent authorization. The nature of these risks is almost exactly the same as the risk of erroneously identifying the subscriber of a certificate, except that a certificate may not be transaction-specific, unlike a commercial-paper instrument, for example. Many certificates may be relied upon in any number of transactions and by any number of Relying Parties. Thus, unlike forged instruments, which represent single points of risk, many certificates create vectors of risk that can be used in a widely ranging number of transactions.

- **Revenue model**: Just as the expense side of an Issuer's business model resembles that of an insurance provider, so does its revenue side: In essence, the Issuer obtains revenue in return for taking on a risk such as a fraud risk. In contrast, Repository's revenue model for ongoing reliance support resembles that of a public utility.

Although distinguishing between Issuer and Repository has some advantages in the abstract, the distinction is just a theory. The two roles can be, and often are, combined into a single role (as in the three-cornered model) and may in any event be performed by one party. However, in illustrating the development of a model, the remainder of this section assumes that Issuer and Repository are separate roles.

C.2.2 Issuer Functions and Obligations

In the four-cornered model elaborated here, the Issuer of a certificate (sometimes termed a certification authority or CA) is viewed as having certain functions and owing certain obligations to Subscribers and Relying Parties. Generally, the Issuer's obligations with regard to a certificate remain inchoate, or any harm for breach of them is reversible, until the Issuer releases the certificate outside its organization. Usually the Issuer first releases the certificate to the Subscriber for the Subscriber's acceptance.

This section overviews an Issuer's functions and obligations, many of which can be grouped differently than in this general collection or can be given over to others.

C.2.2.1 Issuer-Subscriber Functions and Obligations

Broadly viewed within this example of a four-cornered model, an Issuer does the following for Subscribers:

- **Issue certificates**: Perhaps the Issuer's most fundamental commitment to a Subscriber is to issue certificates for the Subscriber's account as requested by the Subscriber.[28] Once the information to be included in certificates has been confirmed and as long as the Subscriber's account remains in good standing, a Subscriber may obtain certificates for its account by request, in accordance with rules (including the Certificate Policy) applicable to the account. The Issuer generates certificates listing its name in the issuer field,[29] signs those certificates, and returns them to the Subscriber for acceptance.

[28]>Illinous Electronic Commerce Security Act § 15-310(1) (effective July, 1, 1999) hereinafter "Illinous Electronic Commerce Security Act"). Utah Code Ann, § 46-3-302(1)(a) (1996) Like all contractual undertakings, the obligation to issue on request is entered into voluntarily. Indeed, a certifier may well retain a right to determine whether it will issue on a certificate-by-certificate basis. However, complete discretion in determining whether to issue any certificate at all could make the contract rather one-sided and potentially empty, and could raise consideration issues in common-law legal systems.

[29]>The listing of the Issuer's name in the Issuer field of the certificate is the defining act of the Issuer in the four-cornered model. All obligations other than this one can be reallocated by contract or the certificate policy, or delegated to others by the Issuer, but if an Issuer loses its identification as such in the certificate, it ceases to fit the definition of “Issuer.”

- **State certified information accurately**: For Subscribers as well as for Relying Parties, the Issuer obligates itself to represent information in the certificate accurately according to a defined level of certainty or confirmation specified in the certificate and as of the date on which the certificate is issued.[30]

[30]This obligation of accuracy does not apply in relation to the subscriber if the subscriber was the source of the information or is in a better position to know of its accuracy.

- **Notify the subscriber of issuance**: Upon issuing a requested certificate, the Issuer informs the Subscriber of the issuance and provides a means for the Subscriber to review and accept the certificate before it is published or otherwise released to prospective Relying Parties.

- **Invalidate a certificate on request**: The Issuer also promises Subscribers that it will revoke or otherwise invalidate[31] a certificate and give notice of the invalidation on receipt of a verifiably authentic request from the Subscriber of the certificate.[32] Contracts may also provide for other notices regarding certificate reliability.[33]

[31]Revocation is final: a certificate, once revoked, is never again valid. The finality of revocation can sometimes make revocation a somewhat extreme remedy, particularly in cases of uncertainty or where the grounds for invalidation are not lasting. Suspension, the temporary invalidation of a certificate, better fits a situation in which the grounds to revoke are temporary, but, since suspension wholly invalidates the certificate, albeit only temporarily, it can be seen as an excessively black-or-white tool for dealing with uncertainty. It is also difficult to implement in some technological systems, and requires repeated checking for updates. Many public-key systems have declined to provide for certificate suspension in practice. In cases where full, permanent invalidation is unwarranted and the amounts at stake warrant significant attention, a repository can pass through to a prospective relying party a message from the subscriber advising the party of a difficulty that has arisen. Such a message can be much more informative than an either-or notation of temporary invalidity (suspension) because it can explain the situation and enable the relying party to arrive at a more informed decision whether to proceed to rely in a questionable situation or to forbear.

[32]According to most certificate policies and implementing contracts employing the four-corner model, the Issuer may revoke a certificate regardless of whether the subscriber requests or consents to revocation, but only for serious problems and with prompt notice to the subscriber as well as to prospective Relying Parties. A serious problem that is the subscriber's fault may also breach the contract between the Issuer and subscriber, and may result in closure or other deactivation of the subscriber's account with the Issuer.

[33]Suspension of certificates is a means of invalidating a certificate temporarily short of permanent revocation. However, suspension can be somewhat difficult to implement, and is perhaps a rather crude means of dealing with uncertain or unauthenticated grounds for revocation. Rather than resorting to the harsh, all-or-nothing technique of suspension, the repository may pass through a message from the subscriber or other party permitted to give notice to Relying Parties. Such a message would not invalidate the certificate but could explain reason for caution or forbearance in relying on it or indicate what the author recommends, albeit in a non-mandatory way.

- **Publish certificates**: The Issuer publishes certificates and notices of revocation in a Repository. The Repository may also provide other services to Subscribers in cooperation with the Issuer, in addition to serving the Subscribers in their possible role of Relying Parties.

- **Provide important information and customer support**: The Issuer may also inform its Subscriber customers of important information necessary to perform the Subscriber's obligations, and may also agree to provide further customer service. Customer-service commitments vary depending on the contractually required level of service, but perhaps include advice regarding safekeeping of the Subscriber's private key and notification of serious system failures affecting the Subscriber, such as compromises of a key impairing the reliability of a certificate needed to verify the authenticity of a certificate issued to the Subscriber.

- **Observe agreed-upon confidentiality restrictions**: Information in a certificate is ordinarily not confidential, but the certificate may identify the Subscriber by a pseudonym which only the Issuer can associate with a real Subscriber,[34] subject to limitations specified in the contract between the Issuer and Subscriber or as otherwise required by laws such as data protection or privacy statutes. The Issuer should generally keep confidential

information about the Subscriber that does not appear in the certificate, such as evidence used to identify the Subscriber, billing and account history information, etc.[35]

[34]Once the Issuer discloses the certificate-subscriber association, it can become difficult to control the dissemination of that disclosure.

[35]The power of a service provider to keep informatio confidential is limited by the government's power to search. Banks, for example, have been required to open their files in response to search warrants against their customers. *see* United States v. Miller, 425 U.S. 435, 96 S. Ct. 1619 (1976) (subpoena requiring a bank to produce a customer's documents did not violate customer's Fourth Amendment rights); *see also* Bank Secrecy Act of 1970, 12 U.S.C. § 1829b (1997).

Additional functions and obligations may be appropriate in addition to these. For example, an Issuer could agree to assist the Subscriber with key generation or to keep a spare copy of a key used for decryption in case of accidental or improper use of an encryption capability.

From the Subscriber's point of view, the objective of a certificate is ordinarily to enable the Subscriber to send authenticated messages to Relying Parties. However, the Subscriber's motivation to obtain a certificate is often indirect and stems from the needs of Relying Parties. Relying parties realize the most direct benefits from improved message security through publickey certification, because the Relying Party takes the principal, direct risk of a forged message.

C.2.2.2 Issuer-Relying Party Functions and Obligations

Persons who receive and rely on digital messages take risks, among others, that they will be unable (1) to attribute the message to its apparent signer, and/or (2) to demonstrate that the message is the same as the one signed, *i.e.*, that the integrity of the message is intact. Attribution of the message to the signer depends on the certificate linking the signing key pair to the signer. Demonstrating message integrity requires verification by the appropriate public key. By making provable attribution and message integrity possible, a certificate has the effect of transferring much of the risk of nonauthentic digital messages from the Relying Party onto the certificate Issuer. In that risk transfer from the Relying Party to the Issuer lies the core value of certification, and that value is realized most directly by the Relying Party.

Thus, for Relying Parties, the value of certification boils down to the functions and obligations that the Issuer performs to reduce the Relying Party's risk of a nonauthentic message. In the four-cornered model, those functions and obligations consist mainly of:

- **Confirm accuracy**: The Issuer confirms[36] the accuracy of information to be listed in the certificate. Depending on the scope of the duty to confirm, it could include an obligation to state accurately all information foreseeably material to the reliability of the certificate.[37]

[36]The concept of “confirming” includes a level effort in investigating and ascertaining accuracy that is appropriate in light of the uses and reliance foreseeable for the certificate. This relative concept can be further defined in setting a certificate's assurance levels and particularly in specifying a level of certainty. *See* Illinois Electronic Commerce Security Act. §15-310(2), Utah Code Ann. § 46-3-103(8); ABA Guidelines 1.9 (1995) (defining “confirm” as “to ascertain through appropriate inquiry and investigation”). Confirmation must occur for all information listed in the certificate as confirmed, but it does not follow that confirmation must occur every time a certificate is issued. In a contractually based account system, the Issuer may confirm on a per-account basis. The evidence necessary to confirm the accuracy of information to be listed in a certificate can be gathered and confirmation thus performed as the account is opened, for all certificates to be issued in the account. Further, while the account is open, additional information accumulates about claims filed and other incidents as well as about certificate usage, and that information can be additional source material for confirmation of certificates issued in the account.

[37]The obligation of accuracy may be imposed according to varying standards of care. For example, an Issuer could obligate itself to refrain from negligence (*i.e.*, to exercise the degree of care that a reasonable person would exercise in the circumstances), or to be absolutely, unqualifiedly accurate (perhaps up to a specified payout cap).

- **Record certificate acceptance**: The Issuer obtains evidence indicating the Subscriber's acceptance of the certificate before releasing the certificate for reliance.[38] A Subscriber may not be legally bound in relation to a Relying Party if the Subscriber has not accepted the certificate in question, and the Issuer may be in the best position to obtain evidence of acceptance when it occurs.

[38]ABA Guidelines 3.10(2).

- **Provide quality operations**: The Issuer uses a "trustworthy system"[39] to issue and revoke certificates, to publish a certificate or notice of suspension or revocation, and to safeguard its private certification key.[40] If the Issuer creates a private key for the Subscriber, it must also use a trustworthy system to do so. The Issuer must also employ personnel practices that provide reasonable assurance of trustworthiness.[41]

[39]"Trustworthy system" is a relative concept determined according to a reasonableness test. Utah Code Ann. § 46-3-103(37) defines "trustworthy system as "computer hardware, software, and procedures that: (a) are reasonably secure from intrusion and misuse: (b) provide a reasonable level of availability, reliability, and correct operation: (c) are reasonably suited to performing their intended functions." The trustworthiness of the system and more details about it can be specified in contracts and their incorporated technical specifications.

[40]*See also* Illinois Electronic Commerce Security Act § 15-301: Utah Code Ann. § 46-3-301(1) (1996). ABA Guidelines 3.1.

[41]*See also* Illinois Electronic Commerce Security Act § 15-301: Utah Code Ann. § 46-3-201(1)(a) and (b) (1996): ABA Guidelines 3.4

- **Give notice of invalidation**: The Issuer gives notice of revocation (and suspension, if supported) using certificate revocation lists or other suitable means of giving notice, when revocation is required or appropriate.[42] Ordinarily, notice of revocation is published into a Repository, from which Relying Parties obtain it as needed. A certificate, Certificate Policy, or other binding document should inform Relying Parties about where to look for notice of invalidation, especially if a project envisions using multiple repositories within its bounds. Especially where checking for invalidity is automated (as it usually is), the form and manner in which notice is to be given should also be specified.

[42]*See also* Illinois Electronic Commerce Security Act § 15-301: Utah Code Ann. § 46-3-306(3) and § 46-3-307(5) (1996): ABA Guidelines 3.12.

- **Provide quality customer service**: The Issuer must provide customer service and claims support through several service plan options reflected in Relying Party contracts.

The above list can be extended to include other functions, depending on the needs of a particular project. For example, an Issuer could assist the Subscriber by securely keeping a spare copy of a key used for decryption.

C.2.2.3 Other Issuer-Related Roles

An Issuer's basic set of obligations can be divided up and reallocated by a Certificate Policy or delegated by subcontract in many ways. By definition, an Issuer is a person listed in the certificate in the issuer field. Besides that basic, defining representation in the certificate, technical standards such as ITU X.509 often assume the Issuer creates and digitally signs the certificate in which its name appears.

However, in practice, the functions associated with the Issuer in the above lists are often performed by other roles, even within a model that basically tracks the four-cornered concept. For example, some functions that the Issuer could and often does perform are assigned instead to the roles of *Registrar* or *Certificate Manufacturer*. In many models, a "Registrar" or "registration agent" performs tasks such as contract formation with Subscribers, confirmation, and other customer-service functions with the Subscriber. Alternatively in some models, an Issuer outsources the generation and signing of certificates and notices of revocation and related operational and security obligations to a party in the role of "Certificate Manufacturer." The next subsections consider these two examples of roles broken out of the overall issuance functions.

C.2.2.3.1 Registrar

In some situations, using a Registrar local[43] to the Subscribers rather than having the Issuer develop its own extensive local presence can facilitate good customer service and help assure the quality of information necessary for confirmation. For example, a company obtaining certificates for its employees is usually in a good position to address the certification needs of its employees, the prospective Subscribers, and to provide high-quality information, particularly information about them, for inclusion in

certificates. However, the company may not wish to take on the operational demands and the risk that certificate issuance entails. Thus, while the company would be the original source or gathering point of much of the information in the certificates it needs, it has little interest in generating, digitally signing, or taking responsibility for those certificates. A company in such a situation is a good candidate for the role of Registrar, which performs a subset of the functions and obligations ascribed to an Issuer in the above lists.

[43]The local presence that makes the registrar's role advantageous need not be geographic, although it often is. The principal requirement is that the registrar have access to accurate information about the subscriber as needed to confirm the content of certificates. The accuracy of that information actually depends on familiarity rather than proximity, although close proximity often coincides with familiarity.

Conventionally, that subset of issuance functions and obligations assigned to the Registrar role consists of:

- **Confirmation**: The Registrar gathers evidence necessary to confirm the accuracy of information to be included in the Subscriber's certificate(s). To a greater or lesser extent, the Registrar may itself be the source of the evidence. Evidence may come from secondary sources (such as driver's licenses, passports, etc.), or from primary sources such as relatives, friends, co-workers, and other sources with direct familiarity with the Subscriber.

- **Intake of revocation requests**: The Registrar may also receive requests from Subscribers for revocation of their outstanding certificates and forward such requests with the Registrar's endorsement to the Issuer (or other person with authority to revoke). In thus initiating a revocation, the Registrar must ordinarily confirm that the person requesting revocation is the Subscriber or one of a class of persons entitled to revoke the certificate.[44]

[44]Both confirmation for issuance and confirmation for revocation may be performed by the registrar, or the revocation process may be delegated to yet another role, often termed a “revocation officer.” Revocation may also be handled by a person authorized not only to request revocation but also authorized to sign and give the notice that effects revocation. For example, an Issuer may empower a person who also serves as a repository to receive verifiably authenticated requests for revocation from designated persons and then effect the revocation by giving the notice in the repository. Since both repository services and revocation services often require every-day, round-the-clock service levels but Issuer services do not, a repository may be in a position to provide a high level of revocation service more efficiently than the Issuer.

The Issuer may also delegate to the Registrar the authority to enter into a contract with the Subscriber on the Issuer's behalf, as well as in the Registrar's own right, in order to establish the respective obligations of Issuer, Registrar, and Subscriber. A Registrar may also perform various Subscriber-support services, such as help with software use and installation, answering telephone questions about digital signing, and similar help-desk tasks.

Involvement of a Registrar having significant obligations related to issuance requires a clear delineation of responsibility between the Registrar and the certificate Issuer: however, it is not always easy for the Issuer to effectively allocate responsibility to a Registrar. A contract, Certificate Policy, or documentary certificate could state that the Issuer is not liable for functions performed by Registrars. However, from a Relying Party's point of view, it may be misleading for the Issuer to be listed as Issuer in the certificate but yet not to be responsible for the accuracy of the certificate. A Relying Party could conclude that responsibility for certificate content is implicit in the role of Issuer, and much of the written work in the field of public-key technology would give credence to that conclusion. Avoidance of the responsibility inferred from appearing as the Issuer in the certificate could be egregious if the redirection to the Registrar is not apparent from the certificate (and it almost never is), but rather is buried in a perhaps lengthy external document such as a Certificate Policy. In large-scale projects, many Registrars could be active at any given time, and ascertaining which one from a long list is responsible for the certificate may be very difficult. Moreover, if the Issuer received an electronic request from the Registrar, tracing the certificate back to that request, even if it is securely archived and preserved, may be difficult. From a relying-party perspective, with the Relying Party being the ultimate source of value in a public-key infrastructure, placing critical responsibility solely on a Registrar who may be difficult to ascertain is inefficient at best.

Further, in the case of a delegation effected by a subcontract requiring a Registrar to perform an obligation otherwise required of the Issuer, the Issuer remains secondarily responsible for the performance of the duties, even though delegated to the Registrar. In such a situation, a Relying Party could recover from either the Registrar or the delegating Issuer, if the Registrar fails to perform as they are both obligated to do. For example, suppose that Irving Issuer promises Roger Relying Party to speak the truth in Irving's certificates, and Reginald Registrar promises Irving to provide true information for Irving to put into certificates. Reginald, however, provides false information to Irving, and Irving puts it into the certificate. Roger relies and sues Irving, and Irving sues Reginald. Irving is liable to Roger and Reginald to Irving. Aside from being indirect and inefficient, Irving, in effect, ends up as a sort of surety for Reginald, so if Reginald cannot pay Irving. Irving must nevertheless still pay Roger.[45]

[45]This chain-reaction liability results from delegating an obligation that one continues to bear. Alternatively, an obligation can simply be allocated to someone else from the start, but if someone not listed as the Issuer in the certificate is obligated to perform issuance-related functions, the confusion and difficulties outlined in the previous paragraph may result.

If a local person is to be fully responsible for the accuracy of information in the certificate, a good alternative to the Registrar role is to utilize a Certificate Manufacturer. For example, if a company wishes to equip its employees with certificates, the company can have the Certificate Manufacturer generate and sign certificates in the company's name and at its request. The company would thus be the “Issuer” of the certificates, although the Certificate Manufacturer is doing the work of generating the certificates and signing the company's name to them. The work done by the company to have such certificates issued is much the same as the work that the company would perform if acting as a Registrar, but with a clearer attribution of responsibility to the company in the certificate. Since the Certificate Manufacturer is not the Issuer of the company's certificates, the risk of erroneous information in certificates is not borne jointly but rather by the company. Ultimately, if the company were serving as a Registrar, that risk would come to rest on the company through indemnification[46] of the Issuer, but with considerably less efficiency, as the preceding paragraph illustrates. If the company is itself the Issuer, albeit using a Certificate Manufacturer to do the backroom data-center work, the risk of erroneous information in the certificate is borne directly and simply by the company.

[46]An Issuer may well require its registration authorities to indemnify it for providing inaccurate information or failing to perform any other duty for which the Issuer may also be held liable. The Issuer may also inquire into the creditworthiness of prospective registration authorities.

Thus, the Issuer can work with Registrars, but the Issuer-Registrar arrangement can sometimes create a complicated and inefficient sharing of the responsibility for accurate certificate content, which is one of the more important aspects of certification. A certificate manufacturing arrangement may be a way of achieving a simpler and more efficient allocation of responsibility between a local, well informed, and risk-capable party and a secure provider of technological services in aid of certification.

C.2.2.3.2 Certificate Manufacturer

A Certificate Manufacturer provides operational services for an Issuer. The exact obligations and functions of a Certificate Manufacturer depend on the contractual arrangements between Issuer and manufacturer, but conventionally and generally, an Issuer delegates the following obligations and functions to a Certificate Manufacturer:

- **Generate, sign, and publish certificates on request**: On receipt of a request from the Issuer, the Certificate Manufacturer creates a certificate containing the information supplied in the request. The Certificate Manufacturer then digitally signs the certificate using a private key certified as the Issuer's.[47] The Certificate Manufacturer uses a trustworthy system in performing these functions.

[47]The certificate manufacturer holds this private key as trustee or custodial agent of the Issuer. A legal instrument must provide for primary or trustor ownership by the Issuer and custodial possession and use, or trusteeship, by the certificate manufacturer.

- **Key generation assistance**: The Certificate Manufacturer often assists the Issuer[48] in creating the Issuer's key pair that will be used to sign and verify certificates, because the Certificate Manufacturer has a trustworthy system, which is necessary particularly for

generating a certificate-signing key. However, a certificate Issuer outsourcing its operations may well not have a trustworthy system.

[48]An Issuer's key used to sign certificates is particularly important, because uncertainty about the security of that key affects all certificates signed by that key and derivatively, all messages authenticated by reference to those certificates. The need for security in generating an Issuer's private certification key is therefore higher than the need for generating an ordinary subscriber's private key. Since the certificate manufacturer has a secure facility but the Issuer may not, it is advisable to use the secure facility to generate the Issuer's private key.

- **Give notice of revocation**: On receipt of a request, the Certificate Manufacturer also creates notice of revocation in a prescribed form, signs the notice using the private key certified as the Issuer's, and publishes that notice into a Repository.

Generally, a Certificate Manufacturer's role in determining certificate content is entirely passive and procedural: the Certificate Manufacturer puts in the certificates it generates whatever the Issuer instructs it to put in them. A Certificate Manufacturer typically has no obligation to anyone to confirm the accuracy of the content of the certificate or to provide customer service or revocation support directly to a Subscriber. A Certificate Manufacturer is also generally not listed anywhere in the certificate, although it could be in a Certificate Policy. Subscribers and Relying Parties may not and need not know that a Certificate Manufacturer was used in producing the certificate, and the certificate generally does not indicate as much on its face.

The Issuer is listed as such in the certificates, signs them (by directing the Certificate Manufacturer to perform the signing operation), and is the principal contracting party with Subscribers and Relying Parties. Therefore, the Issuer's rights and duties to Subscribers and Relying Parties are primary and direct. The Issuer has a right of recourse against the Certificate Manufacturer for defects in generation, unauthorized signing, faulty publication, and other shortcomings in the performance of the Certificate Manufacturer's obligations.

C.2.2.3.3 Other Roles Assisting Issuers

Other roles related or complementary to the Issuer include:

- **Approver**: Within the Issuer's organization, this role has the authority to commit the Issuer to certify, revoke, or perform other critical, decisive functions. To improve the organization's control over its commitment process, this role can be shared by multiple parties in a defined group, with a quorum and threshold defined for a commitment to be carried out.[49]

[49]Certification systems with young and threshold capabilities are often subject to intellectual property rights

- **Information sources**: Large public and private databases such as company and credit reporting agencies, local governments, driver's license and tax authorities, utility companies, and similar resources can provide information about prospective Subscribers, subject to the privacy laws of the local jurisdiction and the provider's own privacy policies. Information sources outside the Issuer can greatly augment the Issuer's own (and any Registrar's) information-gathering capabilities.

- **Auditor**: Auditors, either within or independent of the Issuer, can provide important control and verification of an Issuer's systems and practices.

Other roles can be parsed out of the Issuer's functions listed above or added on alongside the Issuer to augment or reinforce its performance. From a wide-perspective vantage point in the four-cornered model, the Issuer role consists of serving the Subscriber by introducing reliable information about the Subscriber into the electronic-commerce information well, and removing it when it is no longer reliable. There are many ways to divide up or augment roles to that same basic end.

C.2.3 Subscriber Functions and Obligations

Subscribers are not simply passive beneficiaries of a public-key infrastructure but rather have critical functions and obligations. Generally, the Subscriber's obligations remain inchoate, or any harm for breach of them is reversible, until the Subscriber accepts the certificate. Acceptance is ordinarily the legal watershed that places the Subscriber's obligations in full, unconditional effect.[50]

[50]*See* ABA Guidelines 1.1; Illinois Electronic Commerce Security Act §20-105; Utah Code Ann. § 46-3-304 (1996).

The Subscriber owes duties mainly to the Issuer and to Relying Parties. The remainder of this section outlines those duties.

C.2.3.1 Subscriber-Issuer Functions and Obligations

The four-cornered model envisions a Subscriber as obligated to its Issuer to:

- **Cooperate in confirmation**: Before the Issuer can issue certificates for an account, it must have evidence sufficient to confirm the accuracy of the information to be listed in each such certificate. The prospective Subscriber is often in the best position to provide much of the needed evidence such as governmental identification documents (*e.g.* a driver's license and/or passport), proof of residence, statements from co-workers, and other identifying evidence and information.

- **Request issuance of a certificate**. The Subscriber ordinarily initiates the issuance process. Generally, the Subscriber should not be placed in the position of having to refuse acceptance of a certificate issued without the Subscriber's request or knowledge.[51]

[51]The requirement that the subscriber initiate the issuance process is to preclude officious or over-eager creation and distribution of certificates that could appear effective. The danger is reminiscent of the early days of bank cards, when card issuers massmailed apparently effective cards quite broadly and indiscriminately to potential cardholders. Consumers often ended up bearing the losses due to misuse of such cards, which prompted a statutory and regulatory response that would have been unnecessary, had card issuers exercised greater self-restraint in their promotional campaigns. The situation for certificates is analogous, because an unrequested issuance and distribution of a certificate can lead to reliance unintended by the subscriber but nevertheless causing a loss that the subscriber could be expected to bear.

- **Provide a public key** for inclusion in the certificate. The Issuer may assist the Subscriber in generating the public key, or perform the entire key generation at the Subscriber's request, if the Issuer can do so securely. The public key must function properly in accordance with the algorithm with which it is to be used.

- **Check over the certificate and accept it**, if the information in it is correct. If the Subscriber refuses to accept a certificate because it is incorrect due to information received from the Subscriber, the Issuer will usually expect a reasonable explanation for the inconsistency, or may infer a lack of credibility and call the Subscriber's account status into question.

- **Rightfully hold the private key** corresponding to the public key to be listed in the certificate. “Rightfully hold,” as defined in the Utah Act,[52] has to do with the Subscriber's ownership or legal right to the key to be certified. The private key should not have been stolen or “borrowed” from another Subscriber.[53] An Issuer can check for rightful holding by determining whether the public key appears in another certificate extant within a defined zone of assurance (such as the content of a specified Repository). Conflicting certification of a key pair already certified to another Subscriber can lead to confusion.

[52]*See* Utah Code Ann. § 46-3-103(31) (1996).

[53]Besides reuse of a key pair, perhaps without understanding the confusion that could result, key duplication could possibly occur through a defect or fluke in key generation. For example, key generation programs may not be sufficiently random in the numbers they use to create key pairs, which will increase the probability of duplicates.

- **Provide for publication, if desired**: Certificates issued and accepted by the Subscriber may be published if the contract with the Subscriber provides.[54] Publication makes the

certificate available to any Relying Party who needs it,[55] and may include additional, ongoing support for the Subscriber by the Repository.

[54]Some statutory contractual gap-fillers (which apply if no overriding contractual provision does) provide for publication as the general rule, subject to preclusion by an express contract to the contrary. *See, e.g.*, Utah Code Ann. § 46-3-302(2) (1996).

[55]According to common technical protocols, Relying Parties usually receive a copy of the operative certificate with the signed message from the subscriber. However, that certificate may become garbled in transmission or reliance on that certificate may be precluded (such as by omission of critical data such as the subscriber's identification or the public key) in order to prevent reliance outside contractual bounds. An enrolled relying party can in any event obtain a complete, proper copy of the certificate from the repository, if the certificate is published.

- **Respect the bounds of the community**: Often, particularly in public-key projects common at this writing, certificates are intended for use only within a defined community governed by implementing contracts and a Certificate PolicyCertificate Policy. Use of certificates outside that community may expose some parties to unanticipated risks. Implementing contracts and certificate policies therefore generally require Subscribers to use certificates only within the confines of the community.

The functions and obligations in this brief, partial list interrelate with those of the Issuer listed in above in section C.2.2 above.

C.2.3.2 Subscriber-Relying Party Functions and Obligations

A Certificate Policy often envisions Subscribers as having the following functions and obligations in relation to Relying Parties:

- **Use of digital signatures**: Ordinarily, a project's governing documents, such as its Certificate Policy, will require the Subscriber to use a digital signature on certain communications.

- **Private key safekeeping**: The likelihood of forged digital signatures (signatures that falsely appear to be attributable to the Subscriber) is quite negligible if the technology properly implements the underlying cryptography, and if the Subscriber does not lose exclusive control over the private key used to create the digital signatures. The Subscriber is the role that uses the private key, and the only role that can keep it safe. Ordinarily, a Certificate Policy and/or contracts between Subscriber and Relying Party will require the Subscriber to keep private keys secure.

- **Initiate certificate invalidation when appropriate**: Often, only the Subscriber can know when an event warrants revocation of a certificate, such as when the Subscriber has lost exclusive control of the private key or when facts stated in the certificate become inaccurate with the passage of time.[56] The Subscriber is obligated to the Relying Party to have the Issuer invalidate the certificate when the need arises.[57]

[56]If inaccuracies crop up in the certificate and could mislead Relying Parties, the subscriber should correct them. The Issuer should do so as well, but generally has no obligation to monitor the ongoing accuracy of the information in the certificate. The Issuer “speaks” in the certificate on the date when it is issued, and to a great extent, the subscriber is thereafter in a much better position to know when information becomes inaccurate. Once signed and issued, the contents of a certificate cannot be altered, even by its Issuer, without the alteration invalidating the digital signature on the certificate. The only way to update a certificate is to revoke it and issue a new one containing the corrected information. The subscriber should therefore have the inaccurate certificate revoked and request issuance of a new corrected one.

[57]The subscriber owes the duty to request revocation to the relying party, but generally not to the Issuer, although the Issuer carries out that request by revoking. In other words, the *function* of revoking is carried out by the subscriber and Issuer, but the *obligation* to revoke is owed by the subscriber to the relying party (except in any cases where the Issuer should revoke without the subscriber's consent).

- **Certificate quality and suitability**: Certificates are not all the same. Some provide greater assurance than others. A given certificate may not be suitable for a given application. The Issuer of a certificate may be someone whom the Relying Party does not trust. A

Certificate Policy or Subscriber-Relying Party agreement may well require the Subscriber to have and use a certificate that reasonably fits the Relying Party's needs.

The Subscriber and Relying Party may agree on other functions and obligations as well.

These functions and obligations are between each Subscriber and Relying Party. PKI Service Providers such as issuers and repositories ordinarily have no proper role and may be intruding or meddling if they intervene in the Subscriber-Relying Party relationship. Moreover, since the Subscriber and Relying Party decide the terms of their relationship, the Issuer ordinarily does not provide assurance to Relying Parties about whether the Subscriber will use its digital signature capabilities in a manner conducive to sound reliance. For example, the Issuer does not and can not assure that a Subscriber will adequately safeguard her private key(s). The Issuer could report about the Subscriber's capabilities for private key safekeeping, but is not in a good position to know whether the Subscriber uses those capabilities properly.[58]

[58]However, although the Issuer generally does not opine in a certificate about the safety of the subscriber's private key(s), it may make insurance available to cover errors in private key safekeeping. That insurance may bolster a relying party's confidence in the safety of the private key, although it is, strictly speaking, not within the scope of the certificate as certificates are generally understood.

C.2.4 Relying Party Functions and Obligations

Relying parties have functions and obligations, and, since parties in the relying-party role are particularly likely to be aggrieved when other roles err, the Relying Party's functions and obligations often work as defenses to or limits on the claims that a Relying Party may properly press. This section considers those Relying Party obligations and the scope of the Relying Party's rights, after considering how rules can become applicable to Relying Parties to establish their obligations and rights.

Establishing Relying-Party Obligations

According to the assumptions underlying these Guidelines and explained in section C.1.2.1. an Issuer enters into contracts with the parties relying or expected to rely on certificates from the Issuer. The purpose of those contracts (which incorporate and give legal effect to the Certificate Policy) is to define clearly the rights of Relying Parties in relation to the Issuer. Without a clear definition, those rights are governed by the rather vague and unpredictable rules about negligent misrepresentations or by other common-law principles.[59] That vagueness and unpredictability would cause the Issuer to bear a potentially higher risk, incur a higher cost for risk bearing, and set higher pricing than would be necessary for clearly defined rights.

[59]*See* Froomkin. The Essential Role of Trusted Third Parties in Electronic Commerce, 75 ORE. L. REV, 49, 93–103 (1996) For the contract to effectively preclude recourse to noncontractual rights of action, the contract must provide that suit for breach of the contract is the relying party's exclusive remedy, or a similar provision is necessary. Precluding the relying party's recourse to general legal protections may lead to consumer-protection or unconscionability issues, particularly if the contractual remedies are substantively overreaching or one-sided or if the process for making the contract tends to underinform the prospective relying party about important terms.

An Issuer may form implementing contracts with Relying Parties by signing written agreements (with either ink or digital signatures) or by any other means of manifesting assent in a provable manner. Section C.1.2.1.1 describes the legal requirements for contract formation in the Anglo-American tradition, and notes alternatives to paper contracts such as “clickwrap.”

The formation of a contract with a certificate Issuer can be accomplished by the Issuer itself directly, or by another person acting as the Issuer of the agent. In the four-cornered model, the Repository has direct (but perhaps only electronic) contact with Relying Parties, and Relying Parties ordinarily access the Repository, rather than the Issuer (unless the Issuer and Repository roles are performed by the same party), to check the validity of certificates and obtain other certificate support and services. Because the Issuer's contact with Relying Parties is less direct at best, the Repository may act as the Issuer's agent in contracting with Relying Parties, especially if all Relying Parties are not Subscribers and have contact

with the Issuer in that role. As an alternative to agency in making the contract, the Repository can contract with Relying Parties in its own right and designate the Issuer an intended third-party beneficiary. In the Anglo-American legal tradition, third-party beneficiaries can enforce the contract directly against the person obligated to benefit them, but in other legal systems, the contractual rights of third-party beneficiaries are generally and traditionally recognized to a lesser extent.

However the Issuer enters into contracts with Relying Parties, the contracts establish the Relying Party's rights in relation to the Issuer. Contracts also establish the relative rights of the Relying Party and Repository, and the Repository-Relying Party provisions could appear in the same document as the Issuer-Relying Party provisions, especially if the Repository is acting as the Issuer's agent. Upon encountering a new Relying Party, the Repository may open an account for the new Relying Party in the Repository in order to provide ongoing, direct service to the Relying Party.

For convenience: a contract with a Relying Party should not be made every time the same Relying Party accesses a Repository but rather only once. Checking for prior contract formation (which is sometimes termed “enrollment”) when a Relying Party connects with the Repository will make Repository usage more convenient for Relying Parties. To distinguish enrolled prospective Relying Parties from the unenrolled, the Repository could use a shared secret or issue enrolled Relying Parties a simple certificate for communication with the Repository,[60] unless the Relying Party already has a certificate from an Issuer within the system. The consequence of failing to determine that a Relying Party was previously enrolled is that the possibly vague, uncertain rules applicable in the absence of a contract will apply to the certificate, and that lack of clear rules will make disputes more difficult to resolve and the risks of certification less predictable.

[60]Especially in the case of a contract formed online, this simple, relying-party certificate may well contain no confirmed identification of its subscriber, the enrolled relying party. Usage of such a certificate should therefore ordinarily be confined to the issuing repository, and its reliance on such a low-grade certificate should be appropriately limited. Relying parties contracting with the repository online could be invited to apply for more reliable certificates from a system Issuer

Checking for a contractual relationship with a Relying Party also helps prevent strangers from relying on certificates without being subject to clear rules, such as the intended Certificate Policy. If a significant possibility exists (as it well might) that reliance on certificates could occur outside the contractual bounds of the project, it will be in the interest of the issuers and other participants in the project to ensure that recipients of digital signatures backed by the system's certificates do not rely on those certificate without a contract in force to govern their relationship. The Certificate Policy and/or Issuer(s) may seek to preclude reliance on the certificates by persons who could receive them without being subject to an implementing contract. Means of precluding reliance by the unenrolled include.[61]

[61]This list is drawn from an e-mail by Dwight Arthur to the NACHA CARAT group dated July 21, 1998.

- **User notice**: The Issuer may include in the certificate a conspicuous, easily readable notice stating that a recipient of the certificate must enter into an implementing contract before attempting to rely on the certificate or exercise any rights in relation to its Issuer or Subscriber.

- **Documentary certificate**: The Issuer may include in the certificate a conspicuous, easily readable notice stating that the meaning and significance of the certificate is specified in a documentary version available at a specified URL. The documentary certificate would indicate that the certificate is void and meaningless to persons who have not made a contract to rely on it.

- **Subscriber requirements**: The Certificate Policy or implementing contracts may require Subscribers to refrain from sending certificates to persons outside the boundaries of the contractually obligated community.

- **Repository checking**: When a prospective Relying Party contacts a participating Repository to ascertain the current validity of the certificate, the Repository can identify the Relying

Party by means such as a shared secret and determine whether a prospective Relying Party is enrolled before permitting the prospective Relying Party to proceed.[62]

[62]This method assumes that a certificate recipient checks the repository. While checking for revocation is highly advisable, it is far from certain that all Relying Parties will invariably check before relying. However, the system can force a check by omitting critical information, such as the subscriber's public key, from the certificate. See the certificate token option.

- **Encryption in the certificate**: The Issuer may encrypt critical information, such as the Subscriber's public key, in the certificate.[63]

[63]Encryption within the certificate and algorithms for validation of certificates containing such encryption is the subject of intellectual property claims.

- **Certificate tokens**: The Issuer may omit critical information, such as the Subscriber's public key, in what would otherwise be a certificate, and issue that partial certificate to the Subscriber. The needed information could be supplied by a transactional certificate issued in response to the prospective Relying Party's online request.

- **Pseudonymous certificates**: The Issuer may omit information identifying the Subscriber from the certificate, except for a reference to an identifier which only the Issuer can interpret. The significance of the identifier could be interpreted by the Issuer in response to a request.[64]

[64]Once released, the dissemination of the interpretation may prove difficult to control. This method is similar to the omission of critical information and may also be the subject of intellectual property claims.

- **Incorporation by reference**: The certificate may refer Relying Parties to a Certificate Policy, certification practice statement, or other external document requiring contractual enrollment as a prerequisite to reliance on the certificate.[65]

[65]Incorporating an external document can fail if the reference is not clear, the authenticity of the referenced document is lacking or uncertain, or if the intent to incorporate (which is distinct from the intent merely to cite) is not clear from the reference. Simply referencing a certificate policy by an object identifier in the certificate may well fall short in both the adequacy of the reference and the expression of an intention to incorporate. An object identifier is nothing more than a unique series of numbers, and its association with a particular document exists apart from those numbers and can be unreliable or obscure. An object identifier is thus not a reference but rather a means of disambiguating references. Moreover, simply listing on object identifier in a field can be interpreted in many ways other than as effecting an incorporation.

- **Critical policy field**: The certificate may indicate by a standardized, binary flag that the field referencing the Certificate Policy is “critical,” and could thereby perhaps imply that compliance with the policy is mandatory, including its requirement to enter into implementing contracts.[66]

[66]It is by no means certain that recipients of a certificate will infer that the certificate policy is mandatory from the fact that a policy field is marked “critical,” and even if such an inference is drawn, binding legal effect requires more than an assertion that a counterparty is bound. Furthermore, implications drawn from the critical flag depend on technical parsing and on familiarity with the interpretation specified in the current version of ITU X.509, which may be too abstruse for consumers or non-technologists.

- **Noncirculation of certificate information**: Particularly where the Relying Party and Subscriber are the same person, system may forego issuing certificates and instead keep the information that a certificate would contain within a secure, limited-access database or directory.

As noted, some of these methods of precluding reliance by unintended Relying Parties are more effective than others. Indeed, some may have so little effect as to be not worth the effort.

C.2.4.2 Relying Party-Issuer Functions and Obligations

As described above in section C.2.2.2, the Issuer provides certain assurance to Relying Parties in the form of a certificate. The usage of and reliance on certificates is limited by obligations required of the

Relying Party in an implementing contract and in the Certificate Policy, and perhaps also by general laws governing reliance on certificates specifically and/or factual representations generally.

Pursuant to contracts with the Issuer. Relying Parties promise to:

- **Rely within limits**: Assured reliance on certificates issued by the Issuer is limited by beginning and end dates (validity:notBefore and validity:notAfter), revocation,[67] reliance limits[68] (a monetary amount per transaction and/or time period), and other provisions limiting the certificate's assurance level. Validity may also be limited to one specified digital signature (a "transactional certificate"[69]) or in other ways depending on the Relying Party's needs. In addition, the Relying Party must also take into account notice of other facts or considerations affecting the basis for reliance: in other words, the Relying Party must rely reasonably and justifiably. (All of these limits on reliability are subject to rejection and/or negotiation. A person is generally not obligated to rely if the limits imposed are unacceptable.[70])

[67]Since the party would rely at its peril if the certificate is revoked or suspended, the party would need to check the repository listed in the certificate for notice of revocation. Often, a relying party is not under a contractual obligation requiring it to check for revocation, but rather, it relies at its peril in relying on a revoked certificate.

[68]Utah Code Ann. § 46-3-309(1) (1996) (significance of recommended reliance limit).

[69]*See, e.g.*, Utah Code Ann. § 46-3-103(36) (1996) ("A transactional certificate means a valid certificate incorporating by reference one or more digital signatures."): § 46-3-103(38) ("... a transactional certificate is a valid certificate only in relation to the digital signature incorporated in it by reference").

[70]Besides referring an unacceptably signed message back to the subscriber, the relying party could inquire through the repository whether additional assurance or another certificate is available for the subscriber's account. If the Issuer-subscriber and Issuer-repository contracts permit, the repository can forward to the relying party a higher-assurance, already-issued certificate on file in the repository so that the relying party can rely more appropriately on the subscriber's digital signature. Issuance of a new certificate for this purpose is the subject of intellectual property rights and may accordingly be restricted.

- **Rely on the meaning ascribed to the certificate**: The terse, standardized form prescribed for public key certificates lacks the capability to express clearly and precisely what a certificate means. The Issuer can use an online. Web-based process referenced by a URL in a certificate to decode and interpret the certificate into a pre-defined documentary form. The Relying Party must therefore rely only on the meaning given the certificate in its documentary form.

- **Confidentiality and information retention**: The Repository and/or the Issuer may retain information indicating that the Relying Party has been enrolled and providing some background data about the Relying Party (such as name, billing address, etc.). This information should generally be kept confidential.

- **Claims and dispute resolution**: A Relying Party may agree that all disputes or allegations of loss arising from a certificate must be resolved through a procedure of filing, adjusting, settling, and arbitrating written claims. Further, an implementing contract or Certificate Policy may require that claims be filed before a deadline specified in the certificate (usually a time extending for a specified amount of time after the validity:notAfter date[71]). The contract or policy could bar a claim (make it thereafter unenforceable) after that deadline.[72]

[71]Note that the validity period of the certificate (as specified in the validity field) is the period during which reliance may occur, and that period is not the same as the period during which claims may be filed.

[72]For purposes of risk management, the certificate is risk-neutral from the claims bar date on, by analogy to a claims-made insurance policy. *See, e.g.*, National Union Fire Ins. Co. v. Talcott, 931 F.2d 166 (1st Cir. 1991); Brumfield v. Shelton, 831 F Supp. 562 (E.D. La. 1993); Gilliam v. American Cas. Co., 735 F. Supp. 345 (N.D. Cal. 1990) (applying a payout cap based on the timing of the claim rather than of the loss-causing occurrence).

A specific implementation may include other functions and obligations as well.

C.2.4.3 Relying Party-Subscriber Functions and Obligations

The Relying Party is ordinarily obligated to the Subscriber to rely on the certificate within the limits set in it and in accordance with its meaning. Further, the Relying Party has a general duty to rely reasonably and to take into account any material information in addition to the certificate of which the Relying Party has notice. In particular, the Relying Party should be bound by any notice given, including notice by publication in a designated Repository, concerning the validity of the certificate at the time of reliance.

As in the case of Subscriber duties to Relying Parties, the obligations of Relying Parties to Subscribers are not ordinarily within the purview of an Issuer.

C.2.4.4 Relying Party-Repository Functions and Obligations

The Relying Party is a user of the Repository's online information and the technology for delivering it. Therefore, the Relying Party owes the Repository a duty to observe the Repository's security rules, pay according to a fee schedule, and perform similar obligations of online service users.

C.2.5 Repository Functions and Obligations

A Repository is an online source of up-to-date information about certificates, their current reliability, related network infrastructure, legal obligations, and other information helpful for secure electronic commerce. Generally, the value of an information resource like a Repository increases according to the amount of information available in it and the service levels for providing that information. Therefore, repositories in a mature public-key infrastructure may well be large, central, and continually operated stores of online information about certificates and electronic commerce. A defining characteristic of repositories in the four-cornered model is that they are oriented mainly toward the reliance process; in other words, a Repository's principal customer is the Relying Party.

C.2.5.1 Repository-Relying Party Functions and Obligations

The Relying Party is the focal point of the value to be received through public key certification, because the Relying Party most directly bears the risk of authentication failures. Legally, a forgery is generally treated as ineffective as the purported signer's signature unless the signer was negligent in enabling the forgery or otherwise at fault. Since a loss due to forgery falls on the Relying Party at first and perhaps also at last, the assurance of authenticity that public key technology benefits most immediately and greatly the Relying Party. However, many public-key business models tend to underserve the Relying Party even though the Relying Party has the greatest customer potential because it can realize the greatest benefits from public-key technology.

A Repository is obligated to Relying Parties to provide its available information in an accurate and timely manner. However, a Repository generally does not have a duty to confirm the accuracy of the information it provides, particularly if the information is provided as a certificate, notice of revocation, or other document issued by someone else. In other words, where the Repository simply acts as a conduit passing along records provided and signed by others (such as certificates and notices of revocation not issued by the Repository), the Repository passes along that information as-is. However, implementing contracts with a Repository may provide otherwise.

C.2.5.2 Repository-Subscriber Functions and Obligations

Although the Subscriber is for the most part a customer of the Issuer, a Repository may also have obligations to the Subscriber, obligations which it may provide through the Issuer who maintains the principal customer relationship with the Subscriber in the four-cornered model. The possibilities for Repository-Subscriber services have not been extensively explored, but two of the more commonly suggested are to protect Subscribers' privacy and provide account statements to them.

C.2.5.2.1 Privacy and Other Information Rights

Subscribers are the persons about whom information is published in a Repository, which is a generally available, online information resource. The Repository therefore may have an obligation to safeguard the Subscriber's rights of privacy, confidentiality, and information accuracy, if implementing contracts, an applicable Certificate Policy, or other laws provide for such rights.

Statutes in most legal systems other than the United States (for the most part) require large databases holding information about many members of the public to restrict access to and/or the visibility of information that can be related to a specific individual. To some extent, a Subscriber's rights under such a statute (often termed a “data protection statute”) may be the subject of an overriding agreement or a waiver. However, in some legal systems, data protection statutes may impose certain requirements for agreements or waivers, or may otherwise protect the Subscriber's privacy from being given away too lightly.

Aside from legal rules, privacy may simply be a customer need or desire that a Subscriber may be willing to pay for. Drawing from banking experience, confidentiality and discretion in disclosing customer information is often highly valued and may be a prerequisite to doing business.

Where access to and/or visibility of information about the Subscriber is limited, the limitations generally remain subject to law-enforcement and administrative searches and seizures, although most legal systems require a process and/or sufficient cause to justify the search and seizure.

C.2.5.2.2 Account Statements

Banks traditionally report to customers the activity in their accounts to aid in discovering errors. Account statements to Subscribers can similarly be useful for certification accounts. For example, if the Subscriber's private key has been compromised, the Subscriber may not know of the problem—indeed, a smart thief intent on forging signatures will endeavor to escape detection. However, if forged signatures with the stolen key turn up on the Subscriber's account statement, the Subscriber can discover the compromise and take corrective action.

Account statements can also help in determining whether the Issuer, Repository, and others are properly carrying out agreed-upon confidentiality and privacy restrictions.

Technology can help greatly in processing account statements and reconciling signatures made with the reliance on them.

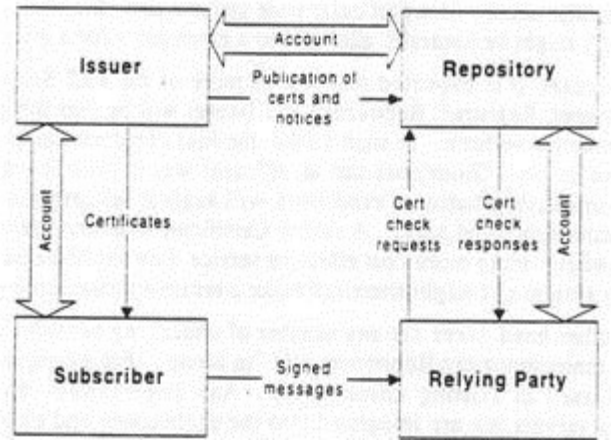
C.2.5.3 Repository-Issuer Functions and Obligations

A Repository and an Issuer it serves will generally agree on the terms and conditions governing publication by the Issuer of information (such as certificates and notices of revocation) into the Repository. A Repository is obligated to perform according to that agreement.

The agreement may also provide for other services by the Repository to issuers besides publication. For example, as noted in section C.2.4.1 above, a Repository can assist issuers in making contracts with prospective Relying Parties.

C.2.6 Conclusion on Four-Cornered Model

The four-cornered model, as diagrammed below, basically allocates roles according to customer relationships and interactions.



However, this model is only one alternative and is capable of much variation. This introductory part of the Guidelines examines it—not because it is definitive (it isn't), but because it illustrates the sort of business design work underlying a public-key project and its implementing contracts and Certificate Policy. The next section considers how such a design is implemented in such contracts and other documents.

PART D. IMPLEMENTING A BUSINESS AND LEGAL MODEL

D.1 Tailoring Certificate Policy to Reflect and Support Underlying Business and Legal Conditions

The first step in writing a Certificate Policy should be assessing the requirements of the underlying business model. If, for example, it is known that a particular party will have to identify and authenticate a set of people who would fill the role of “Subscriber” in a PKI, then the drafter must consider whether that party would be capable of performing the functions of the Registrar. If, for example, this party had some reason why such functions would not be delegated, then unwillingness or inability to act as a Registrar would significantly complicate the drafting of a policy. A party may be rendered unfit to perform as a Registrar due to such business or legal conditions as restrictive union contracts, limited technical ability to securely communicate with the Issuer or unwillingness to use a different Certificate Manufacturer (such as with a party that has an exclusive arrangement with one or more sub-standard Certificate Manufacturers).

The initial allocation of functions to roles, and roles to parties will, in the first instance, depend upon an assessment of the business conditions. Such an assessment will define the parties that will be available to accept roles. There may be some latitude available in matching a given role or function to any of several parties, depending upon the transactions and other factors. However, it is also likely that the transactional needs of the system will strongly indicate or require that a particular party play and particular role or functions. The roles of Subscriber and Relying Party are good examples of this. In a public sector bidding system, the Subscriber might be a given set of private sector vendors who submit bids and the Relying Party might be limited to a particular agency of a particular state government. Similarly, the role of Registrar and even Repository might be naturally allocated to a given party for a given business system.

In many cases, it is expected that one or more of the PKI Service Providers roles (Certificate Manufacturer, Registrar, Repository and Issuer) will be “up for grabs” and available for a third party vendor to perform. In such a case, the four cornered model of PKI relationships discussed elsewhere in these Guidelines can an efficient way to allocate roles. However, it is also likely that the underlying business conditions will suggest refinements and modifications of the roles and functions in novel ways. A secure Certificate Manufacturer or Repository business may be capable of providing more cost effective service than would be possible by any of the parties to a business system and might therefore make a sensible outsourcing partner.

On the other hand, there are any number of underlying business and legal conditions that might suggest maintaining the Repository role “in house.” For example, an organization might be able to avail itself of

existing infrastructure. Any given system may be better served by existing directory servers that are integrated into the applications and existing business practices of some parties who seek to create a PKI and Certificate Policy. This could be the case with a large organization that has implemented an X.500 server and that all relevant parties already tie into for purposes of e-mail and other network services. There may also be legal or policy reasons that are not bound up with existing infrastructures but that nonetheless mitigate against outsourcing the Repository role. For example, the information to be placed in the certificates may be deemed too sensitive to permit a third party Repository to see (for privacy reasons) and a third party Repository might be unwilling to agree not to compile and sell names or other transactional data. Any number of underlying business reasons may cause a decision not to outsource the Repository role. However, as noted in the review of the four-cornered model and elsewhere in these Guidelines, as between two initiating End Entities who intend to be Subscribers and Relying Parties, a review of business conditions for their intended system might indicate that outsourcing of all PKI Service Provider roles and functions is desired.

D.1.1 Parties and Transactions Together Define the Underlying Business Structure

Together, parties and transactions define the underlying business structure enabled by PKI. Examples of underlying business structures might include:

	Party Relationship	Example Transaction Types	
1.	Business to Government	public procurement	Regulatory interaction
2.	Business to Business	supply chain	Joint projects
3.	Government to Government	sensitive information sharing	Reporting requirements
4.	Employees and Contractors to Employer	human resources	payroll management
5.	Prospective and Current Consumers to Business	account creation	account usage
6.	Licensed Professionals and other Citizens to Government	submittal of filings	Requests for information
7.	Students and Faculty to staff	course registration	Grading

In implementing an electronic business and legal model. Policy Authorities cannot ignore legal and regulatory conditions that apply to parties and transactions in the paper-based world.

D.1.1.1 Legal and Regulatory Conditions Related to Certain Parties

Under example one (1), above, contracting with a government can raise special issues that bear upon obligations in a PKI environment. For example, in a government environment, parties must be aware of the following:

- **Sovereign immunity** shielding government from certain sources of liability. Irrespective of the terms of any Certificate Policy, government parties come to the negotiation table with certain liability characteristics that are not typical of private sector parties;

- **Public records laws** that can severely restrict the confidentiality of transactional data (for example, in some jurisdictions, even the contract to provide PKI services to a government entity must be a public record, resulting in an inability of PKI providers from maintaining confidential liability terms between government clients):

- **Limitations of business partners** may exist that limit or regulate the parties with whom government may transact (as in requirements to contract with small, local or minority owned businesses and moratoria against contracting with business from certain countries, such as Burma).

In addition, any of the parties may have preferences or aversions to contracting with other parties or may have special requirements governing the type and manner of transactions it will enter into. These preferences and requirements might be based upon external pressures, such as the need to comply with strings attached to grant money or they may be based on internal pressures, such as agreements with organized labor or longstanding operational procedures.

D.1.1.2 Legal and Regulatory Conditions Related to Certain Transactions

Under example five (5), above, in the securities context or the banking context certain notice requirements and other regulatory issues may create special circumstances that would effect the latitude available to a Certificate Policy drafter. The obligations of PKI Service Providers or others to disclose materials, to keep records private, or to honor or dishonor a given signature (whether digital or not) may effect the duties of all parties with respect to usage of any particular communications system - including PKI.

D.2 The Role of the Certificate Policy in the Context of the Business Environment

The Certificate Policy can be used for any number of purposes, as detailed above. Legally, one of the more important and complex uses of a Certificate Policy is as a set of operating rules. To serve as enforceable operating rules, parties would have to sign “implementing contracts” as discussed elsewhere in this document. Other documents and sources of obligation would also bear upon the efficacy of the Certificate Policy, such as public law, licenses and conduct that could give rise to common law causes of action in tort. For these reasons, one may not be able to glean all of the relevant rights, obligations and roles of parties merely by reading a Certificate Policy, or any given set of documents.

D.2.1 Sources of Power or Sources of Authority Underlying Certificate Policy Making Process

The range of factors and related documents that are relevant to the relationships spelled out within a Certificate Policy will depend in large part upon the source of power or authority by which the Policy Authority promulgated the policy. As described above, a vital initial issue to be determined prior to the drafting of any particular Certificate Policy is the identity of the parties, especially the stakeholders and in particular, the Policy Authority. This section proffers examples of how the identity of the Policy Authority can radically affect the underlying business conditions related to a given PKI. The content and scope of a Certificate Policy will necessarily change (perhaps radically) depending on the status of the Policy Authority. A threshold question is: by what right does the Policy Authority promulgate a Certificate Policy? It is too facile to merely indicate that a Certificate Policy may become legally enforceable based upon contract.

The basic questions remains: why will parties who would be subject to a Certificate Policy agree to be bound by a contract? As discussed below, sources of power and sources of authority of a Policy Authority will materially shape any given Certificate Policy.

D.2.1.1 Power Based on Position in Private Market

An organization with great power in a private market might be capable of becoming a Policy Authority based on its position in the market. This might be the case with a very high-value purchaser who supports a large supply chain or with a network service provider with a large base of users in an inelastic market.

D.2.1.2 Authority Based on Provisions in Public Law

Other organizations might have great power based on grants in public law. This might be the case in a jurisdiction that has enacted a law empowering a particular governance body to create policy on a certain matter (as with the California Law Enforcement Telecommunications System[73]) or a law entitling a government body to license a PKI Service Provider (as with the Utah Department of Commerce which promulgated detailed regulations governing licensure of Certificate Authorities and Repositories).

[73]The CLETS system was created by the California legislature through enactment of a statue. The statute designates a governing body and that body drafts contracts which bind other parties who seek to gain access to the criminal justice information contained within the CLETS system. For more information including the governance structure and downloadable copies of the major implementing contracts) see: [http://caag.state.ca.us/cas/ppp/ppp.htm].

D.2.1.3 Agreement Based on Consent of the Parties

Still other membership organization might gain power based on consent and private contract among interested parties. This might be the case among parties who chose to set up or join a representative non-profit council to draft and issue Operating Rules which the parties would then voluntarily agree to follow by contract (as with the Electronic Benefits Council of NACHA). A key element of this source of authority is the fact of agreement as the basis of enforceability. Unlike a system prescribed by public law and implemented through contracts with parties who may have little or no choice but to comply, a truly private system based on agreement can be amended or abandoned by the parties. Though such power to change the rules could be a source of instability, it is also a significant strength of these systems. The ability for parties to adapt to changing business, legal and other relevant conditions in a responsive and agile governance structure can be critical for the success of a system in the fast-changing electronic commerce markets. By way of contrast, Certificate Policies premised upon power or authority, absent discussion among the parties, can be insulated from the reality of rapid change in the short-term and therefore are vulnerable to becoming obsolete in the long-term.

D.2.2 Order of Precedence of the Certificate Policy vis-#agrave#-vis Other Documents

Depending upon the source of authority underlying the process of drafting or otherwise selecting a Certificate Policy and other business and legal conditions, additional documents will either control or be controlled by that named policy. Documents that have a higher order of precedence

for purposes of interpreting other documents are said to be “controlling.” Documents that are governed by other documents are “controlled” or “subordinate” to the higher documents. In some cases, documents seem to neither govern nor be governed by other documents. Such “peer” level documents are usually not a problem, unless the documents are binding on the same parties and provide inconsistent or conflicting obligations. Structuring the governance model of a PKI will involve a careful investigation of all such related documents. When necessary, measures will have to be taken to clarify the order of precedence of each such document.

D.2.2.1 Higher Level “Controlling” Documents

It will be common for any of the following documents to exist as at a higher level than the Certificate Policy and to govern the terms of the Certificate Policy:

- **Constitution and Statutes** of the jurisdiction or jurisdictions in which the Certificate Policy will be effective or may be litigated or otherwise interpreted

- **Court Orders** that are in effect and which govern the subject matter or parties

- **Public Administrative Regulations** that directly effect the subject matter or parties
- **Charter and Bylaws** of the organization in question
- **Higher Policies** that the organization has afforded a controlling status
- **Important Contracts** that are difficult or impossible to materially change at the time in question:

D.2.2.2 Lower Level "Subordinate" Documents

It will also be common for any of the following documents to exist as at a lower level than the Certificate Policy and to be governed by the terms of the Certificate Policy:

- **Lower Policies** that the organization has ranked below the Certificate Policy
- **Implementing Contracts** that are created pursuant to the terms of the Certificate Policy
- **Sub-Contracts** that are entered into by any of the parties for the purpose of delegating functions assigned to them under the Certificate Policy
- **Memoranda of Agreement and Memoranda of Understanding** crafted to assist the parties

D.2.2.3 Peer Level Documents

As mentioned above, sometimes the Certificate Policy will duel for precedence with other documents that are neither clearly governing nor governed by the Certificate Policy. Such documents might include any of the following:

- **Other Certificate Policies** which have been agreed upon by a party to the present Certificate Policy
- **Documented Practices** of a party to the Certificate Policy
- **Related Contracts** entered into by a party to the Certificate Policy
- **Existing Employment Agreements** binding upon a party to the Certificate Policy

Similarly, service level guarantees from Internet providers and software licenses with warranties of fitness for a particular purpose may create ambiguous situations where the expectation of the parties may be different in the event of a dispute involving a Certificate Policy. These types of documents can often be expected to encompass one of the parties allocated responsibilities under the Certificate Policy and one or more non-parties to the Certificate Policy who are, nevertheless, playing a role in the business structure (Internet service providers, software developers and sellers, perhaps even private standards bodies). A Policy Authority has a duty to be diligent in assuring the Certificate Policy is realistically scoped. The expectations of the parties would be frustrated by promulgation of a Certificate Policy that purports to govern rights and obligations of parties but that is in fact going to be overridden by other documents with different terms and leading to different outcomes. The range of issues addressed within the PKIX Framework is so broad that a prudent Policy Authority will seek the advice of knowledgeable counsel as part of the process of setting policy.

D.2.3 Analogous Contractually-Based Governance Structures

D.2.3.1 Several Analogous Structures Exist

There are several examples of governance structures that depend upon parties to opt in by contract. These systems usually avail themselves of a single higher level document that is referenced by the contracts signed by each party. For example, the Electronic Benefits Council of the National Automated Clearinghouse Association uses a high level document known as “operating rules” which are referenced by contracts. The mere fact that a party signs a contract in order to participate in a system does not necessarily mean that the system is governed entirely or even predominantly by private law or subject to changing agreement by the contracting parties. For example, the VISA system (discussed in more depth below) requires each party to sign a contract, but critical liability provisions and other terms are directly specified by public law. Similarly, the CLETS example described above is founded upon a statute enacted by the California legislature, but each party must nonetheless sign a contract to participate in the network. Other systems, such as the program stock trading networks and the multi-lateral network peering agreements for Internet service providers, provide more variations on the theme. In sum, several examples of governance structures based upon contracts exist in the marketplace today.

D.2.3.2 Mini-Study: The VISA Model

Visa is a membership association of approximately 21,000 financial institutions in 250+ countries and territories worldwide. The association is governed by an International Board of Directors, and Members belong to geographic Regions which have their own Boards reporting up to the International Board. The payment system supports: 600+ million Visa cards, 14+ million merchant locations, and 400+ thousand ATMs.

Membership categories, rights and obligations are spelled out in the By-Laws. Several categories of membership are available, depending on the type of activity the Member wishes to engage in (issuing cards, acquiring tax from merchants, etc.).

Large Members may sponsor smaller Members, and assume certain responsibilities for the financial performance of their sponsored Members. Members also sponsor (and assume certain liabilities for) processors, third-party servicers or other agents that support their business.

Visa owns proprietary payment system brands/marks (Visa, Plus, Interlink, Electron) and runs the Visa payment system (i.e. clears and settles Visa-branded transactions between Members). A key component of the payment system is a comprehensive set of Operating Regulations which define how the brands are to be used and how transactions are to be processed by all parties. Members must agree to abide by OpRegs as a condition of their Membership. A formal dispute resolution process is also a part of the OpRegs.

Members sign contracts (“agreements”) with consumers and merchants which govern how Visa transactions will be processed between these parties. By extension, these agreements also imply and/or specify adherence to the processing rules that apply between Visa and its Members. Certain standard contents of these agreements are specified in the OpRegs: beyond that. Members are free to add more provisions of their own— especially regarding fees, pricing, etc.—so long as those provisions do not conflict with Visa policy or regulations, or with any applicable legislation or regulation from a local governmental agency. This freedom of agreement format is required in order for the system to work effectively in the 250+ worldwide jurisdictions and thousands of local sub-jurisdictions in which these agreements are concluded.

A key point is that Visa does not have any direct contract or relationship with consumers or merchants. OpRegs bind Members and Visa, but not Visa and end users of the payment system. For example, OpRegs may allocate liability for fraud losses according to certain rules regarding how the transaction was authorized, whether a signature was obtained, the form of the signature, etc. But this loss allocation is between Members: separate rules govern how much loss a cardholder or Merchant will bear in any given situation, and these rules often incorporate various forms of protective legislation (including, e.g., Reg Z and Reg E) which are required to be incorporated (either explicitly or implicitly) in the Members' agreements with merchants and consumers.

Visa may also establish policies for consumer protection in its own OpRegs (e.g., limiting debit cardholder liability to 50 if a fraud or card loss is reported within two days): however, these policies are binding on the Member, and Visa will sanction the Member if these policies are not followed.

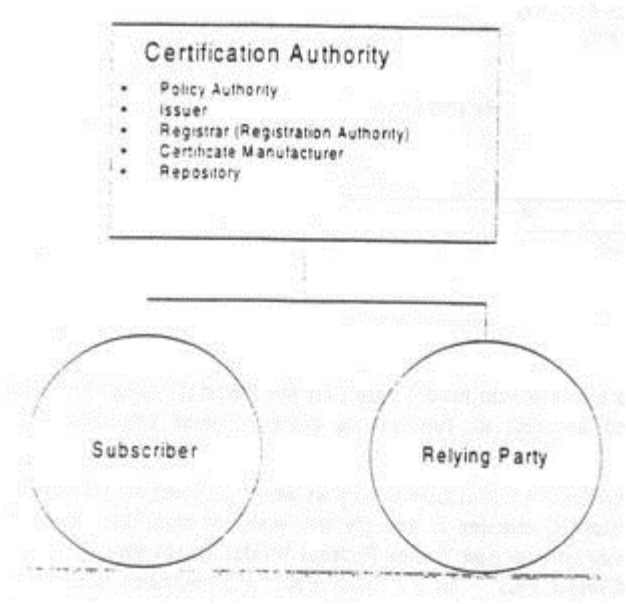
Another key part of the Membership arrangement is Visa's role in managing risks of the payment system. Visa constantly evaluates Member soundness and the quality of Member programs, and may impose a variety of sanctions up to and including shutting down a Member's Visa programs and revoking membership if the offending Member's activity is deemed to be a danger to the overall payment system, the brand, or other Members.

D.2.4 The Relationship of PKI Models to the Certificate Policy Implementation

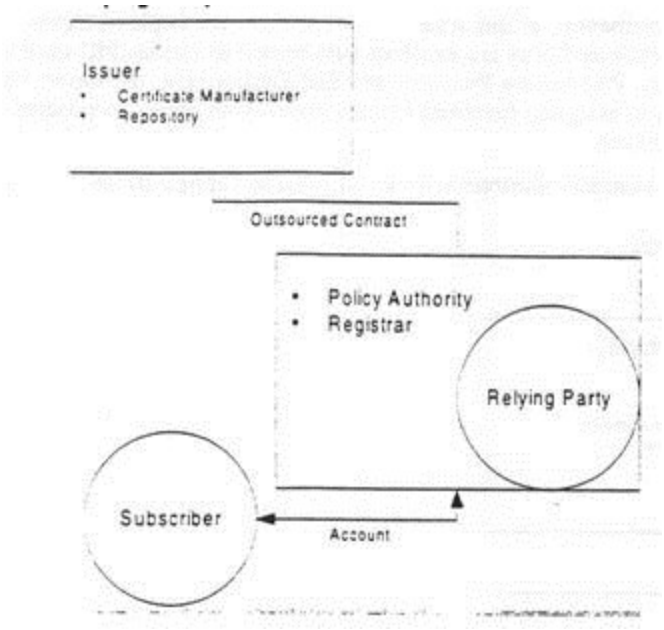
D.2.4.1 Underlying Business Conditions and Allocation of PKI Functions to Roles

Not all business models mix and match roles in the same way. In addition to the four-cornered PKI model detailed in Part C of these Guidelines, a number of other possible models exist. As mentioned in Part C, it is premature to suggest that any particular model is predominantly used in the market or generally recommended at this time. In this section, the implementation issues surrounding drafting of a Certificate Policy are explored with respect to various PKI models. In any model, a Policy Authority, PKI Service Providers and End Entities exist. However, there is a wide latitude for flexibility in assigning functions to roles and roles to parties, depending upon the underlying business conditions.

The following diagrams and examples illustrate some of the possible configurations.



The Certification Model is usually associated with “Open PKI.” In Open PKI, it is envisioned that Subscribers will hold one or more certificates of varying classes. Any Relying Party may then accept Subscriber certificates of a suitable class for any transactions. The idea of Open PKI is exciting because Open PKI has the potential to support an infinite number of transactions with relatively few certificates per Subscriber. At the same time, however, because a certificate could be used for countless types and numbers of transactions, it is difficult to manage or limit the risk of liability in an Open PKI. Most PKI Service Providers are not willing to open themselves to unlimited or uncontrollable liability. Further, it may be more difficult for a Certificate Policy that generically defines a “class” of certificates to contemplate ancillary business and regulatory consideration that affect the parties and the transaction enabled by PKI.



The Relying Party model is a hypothetical model based on the Federal Model Certificate Policy Draft (March 25, 1998) and as well as functioning pilot projects underway at the state government level.[74]

[74]At least two live State pilot projects utilize this general model.

The Federal Model Policy envisions a Certificate Policy as being defined by a Relying Party, an industry association, or a group of entities to specify the level of trust that must be met by certificates used for a *particular transaction*.[75] The Federal Model Policy envisions a model that more closely resembles a "Closed PKI." In a Closed PKI, a Subscriber usually posses one certificate which it uses for one type of transaction with a known Relying Party. Under the Federal Model Policy, the Relying Party plays a central role in that it not only is the principal Relying Party, but it also acts as Policy Authority and a Registrar.

[75]Federal Model Certificate Policy Discussion Draft (March 25, 1998), page 6.

In a live PKI pilot project resembling the above diagram, PKI Service Provider roles were allocated to parties in the following manner:

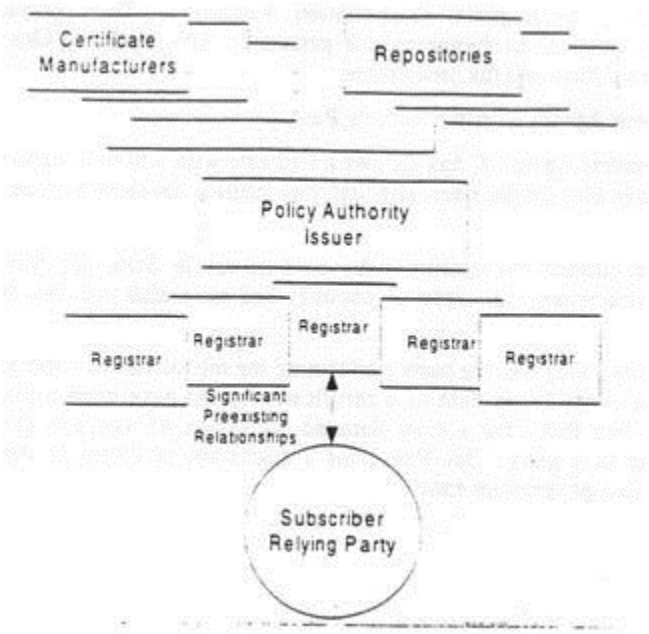
- Private Company A and Bank B are Issuers
- Private Company A created a root key for Bank B in its "hardened facility."
- Private Company A manufactures certificates on behalf Bank B using Bank B's root key. Bank B's certificates are then issued to Subscribers of Government Agency C.
- It is unclear whether any party performs Repository services.
- Government Agency C. State Administrative Agency D, and State Administrative Agency E (under which the pilot was created) are the Policy Authority.
- Government Agency C is the Registrar (Registration Authority). Two individuals at Government Agency C perform the Registrar role personally using existing Government Agency C's records and callback and fax procedures.
- A Division of Government Agency C is the Relying Party

- The Division of Government Agency C has its own certificate with which it signs receipts. As a result, the Division is also a Subscriber, although this status is not shown in the diagram above.

- Private companies from around the country who do business in State are Subscribers. Subscribers must file and renew their licenses annually and must also pay fees and taxes semi-annually.

It should be noted, in the above diagram, the party performing the role of Issuer - the party that, at the least, places its name in the Issuer field of a certificate - could have been performed by Government Agency C.[76] See Part C for a more detailed discussion of issues to consider in assigning the role of Issuer to a party. See Part B for a discussion of issues to consider in assigning the role of Issuer to a government entity.

[76]Another alternative would have been for Private Company A. Bank B and/or the Government Agency C to place their names in the Issuer field of the certificate. This co-branding of a certificate may result in additional liability for any one of the parties listed in the certificate but it may also give the certificate more legitimacy or provide marketing benefits. Yet another alternative would be the formation between the parties of a joint venture, partnership, or other legal entity which would place its name in the Issuer field of the certificate.



The Electronic Court Filing Model is a hypothetical model that could be applicable in any U.S. State where parties would perform the following roles:

- The Policy Authority and the Issuer would be either a State Bar or a legal entity made up of a members from a State Bar, Court Clerk Associations, State Supreme Court, Federal Courts, and Administrative Office of the Courts (or like entities).

- Certificate Manufacturers and Repositories would be private companies performing Certificate Manufacturer and Repository services. Certificate Manufacturers and Repositories would operate in a particular state if accredited by the Policy Authority or by a means defined in the Certificate Policy. To foreclose monopoly and ensure interoperability, the Certificate Policy or a technical document incorporated by reference in the Certificate Policy would define a set of technical standards to be followed by Certificate Manufacturers and Repositories in order to sell PKI services to members of the State Bar or Court Administrators.

- Registrars would be court clerks located throughout a State. State Bar offices, or any other bricks and mortar establishments where attorneys and judges have a significant preexisting relationship.

- Subscribers and Relying Parties would be lawyers, judges, and court administrators. Subscribers would have one certificate that would be issued by the Policy Authority but which could be manufactured by any one of several Certificate Manufacturers who operate under a statewide Electronic Court Filing Certificate Policy.

In addition to the above examples, there are a wide variety of other role allocations and business models that can be envisioned and that are likely to evolve.

D.3 Determining Whether and How to Draft a Certificate Policy

According to the PKIX Framework, a Certificate Policy may serve the following purposes:

Provide a human-readable, named policy which may be used by a certificate user to decide whether or not to trust a certificate for a particular purpose:

- Generate a policy that can to be recognized by both the user and the Issuer of a certificate [note: under these Guidelines, the parties would include the Certificate Manufacturer, the Registrar, the Issuer, the Repository and users would include the Subscriber and the Relying Party who would all recognize the policy]:

- Simplify comparison between two certificate policies during cross- certification between certificates issued under different policies;

- Create a benchmark for comparison between the policy and the documented practices of a PKI Service Provider to ensure that the provider's practices faithfully implement the policy;

- Constitute a basis for accreditation of a PKI Service Provider by providing a policy against which the providers practices can be accredited.

A Certificate Policy can assist an organization in the pursuit of the above purposes. In addition, the PKIX Framework can provide a valuable check-list for policy makers, managers, attorneys, technologists and others to use while evaluating a given or proposed implementation of certificate-based PKI. The comprehensive nature of the PKIX Framework creates a good summary list for beginning such an evaluation. The exercise of running through the issues presented in the PKIX Framework can assist an organization in making the determination of whether such a policy is needed or helpful in the context of their current or contemplated usage of certificates. These Guidelines point toward use of the PKIX Framework as a starting point for policy development in large part because of the need for interoperability among users of secure or authenticated electronic records and signatures. Such interoperability is not only needed at the strictly technical level, but also at the policy level.

Indeed, interoperability among policy documents is of vital importance in the fast-paced electronic commerce business environment. Though many parties and transaction types may never overlap, it is anticipated that organizations will be able to realize economic efficiencies or quality enhancements by easily communicating securely and with authentication among a wide array of new parties. Electronic commerce, as part of the emerging information economy is pushing organizations to form numerous and quickly shifting alliances with a growing array of other organizations. New markets of customers are becoming available via the Internet that have been uneconomical to reach in the past. Existing relationships can be made more effective and less costly through the use of security and authentication over open networks. As e-commerce market forces are brought to bear upon organizations, organization will derive increasing value from the ability to quickly exchange policy documents to evaluate and determine whether it will be possible to send and rely upon important or confidential records over open

networks. Policy evaluations will be greatly hampered if policy documents follow non-uniform or conflicting structure and content type.

On the other hand, availability of uniform policy formats can enable rapid scalability by enabling decision makers to quickly evaluate other policies and determine whether the desired business transactions can take place under the existing policy, or whether the policy and practices need to be amended or whether no business case exists given the current state of policies and the costs or time allotment entailed in bringing them into shape. Similarly, such policies can form an efficient method of effecting agreeable operating rules or system rules among parties with existing business relationships but no standard method of using PKI. The PKIX Framework, although imperfect, provides organization with a basis for policy interoperability.

D.3.1 Criteria for Making the Determination

Policy Authorities should weigh several factors as while determining whether a Certificate Policy is necessary or desirable. Some factors include:

D.3.1.1 Does your use of PKI involve certificates?

If your PKI does not involve certificates, then a Certificate Policy may be the wrong form of policy. Using PKI-based digital signatures that are not verifiable with reference to a certificate would not implicate many of the issues addressed in a Certificate Policy. Other forms of policy may be desirable to govern such matters as key usage or binding a party to a key, but the Certificate Policy may be inappropriate.

D.3.1.2 Is this a single party system?

If a single-party system is envisioned, then a formal governance body may not exist and, as a result, a formal policy may not be needed. However, in very extensive and geographically dispersed entities, such as governments or large corporations, internal formal policy may be an appropriate management tool. Such internal policy would be appropriate in cases where sensitive, high value or mission critical applications depend upon the proper functioning of certificate-based PKI to operate.

D.3.1.3 Is the underlying transaction of low-value?

If the underlying transaction is of low-value, then a full Certificate Policy may be inefficient or uneconomical to develop. The term value, in this context, is broader than a direct cost measure. A cost, benefit, and risk analysis or similar analytical tool can show whether an application is of high value or not. Even relatively low cost applications may entail high risk in terms of litigation exposure or reputation in the event of system failures. Similarly, a low-cost system may be a high-benefit for an organization, by bringing in a regular revenue stream or directly facilitating the mission of the entity.

D.3.1.4 Is there already a Certificate Policy in play?

If another Certificate Policy exists and has been promulgated by a party with whom your organization must interact but with whom you have little or no bargaining power, then drafting a Certificate Policy of your own may be unnecessary. However, the exercise of drafting may still be valuable as a method of testing whether the other organization's Certificate Policy adequately specifies important provisions.

D.3.2 Scope and Detail of the Certificate Policy

A Certificate Policy may have a broad scope of coverage for many different types of underlying transactions but still be relatively undetailed and short. For example, amendment to an existing policy document that already handles many of the issues that need to be addressed for a given system, such as: financial responsibility, archival, audits, etc. On the other hand, the Certificate Policy could be very detailed, but could only have a very narrow scope to deal with a single transaction between two parties.

Alternately, the Certificate Policy could be short and undetailed and narrow in scope (as with an internal application or a relatively informal application between well-established parties).

D.3.2.1 Public and/or Private Parties in Contract Systems

Because of the difficulty with drafting guidelines in the absence of a particular set of business and legal conditions, these Guidelines were developed with certain assumptions about the nature of the parties and transactions. Such assumptions include the assumption that Policy Authorities will seek to draft Certificate Policies to support systems in which each party has signed a contract and entered into a closed or otherwise bounded transactional system. Further, the Guidelines have been written to support both public sector and private sector parties in the drafting of Certificate Policies.

The section of these Guidelines that provides guidance in the form of drafting instructions for a Policy Authority assumes either a fairly significant set of transactions and/or at least two separate parties. This is because it is expected that the audience for this document seeks to draft a Certificate Policy to facilitate the use of public key certificates for non-trivial business interests that expand beyond the boundaries of a single party.

D.3.2.1.1 Reference Model: Business to Government Procurement in a Bounded Contract System

Another reason these Guidelines do not contemplate a single narrowly defined transaction is because publication of a policy document tailored to the needs of a particular business environment and specified transactions would not be easily ported to another environment with different parties and transactions. These Guidelines are meant to be useful to a range of public and private sector parties who seek assistance drafting policies supporting a range of applications. Unfortunately, it would be nearly impossible to draft a sound policy that is so vague that any number of different transactions could be accommodated. Such a document would not provide sufficient guidance for Policy Authorities who would attempt to use this document to craft a Certificate Policy for needs of their organization. For these reasons, these Guidelines were drafted with a general business environment in mind as reference model. The general business environment used as a reference point is as follows:

- Buyers and sellers with a contract in place governing the terms of the purchase and the business relationship:
- The purchase and sale are conducted via online, web-based catalogues:
- Shopping, enforceable quotes, approved orders, and confirmations are secured and authenticated to some extent based upon the browser certificates of buyers and the server certificates of sellers; and
- The buyer is a public sector party and the seller is a private sector party.

Though the Guidelines were drafted with periodic reference to a business to government procurement example, at the same time, these Guidelines take care to indicate throughout the document how different business environments might effect the policy drafting process.

D.3.2.1.2 Variations

These Guidelines have been drafted primarily to support closed or bounded communities. In the future, however, it is possible that more open systems will emerge. Some commentators have suggested that standards-based “registries” and reputations-based “clearing houses” will open the way for stranger to stranger secure and authenticated communications globally based upon certificates.[77]

[77]Assuming Certificate Policies continue to proliferate at the current rate, then a widely accessible and organized means for accessing such policies will become increasingly valuable. There is a need to attach meaning to a given OID and to make the related policy materials available in a manner that is capable of dynamic updating. The need for an online and reliable policy and document registry will become more pronounced over time.

Accreditation of a PKI Service Provider could create part of the foundation missing for less closed systems supporting secure and authenticated electronic commerce. According to the PKIX Framework, a Certificate Policy can form the requirement set for accreditation of PKI Service Providers. The PKIX Framework states:

> "Certificate policies also constitute a basis for accreditation of CAs. Each CA is accredited against one or more certificate policies which it is recognized as implementing. When one CA issues a CA-certificate for another CA. the issuing CA must assess the set of certificate policies for which it trusts the subject CA (such assessment may be based upon accreditation with respect to the certificate policies involved)."

The states of Utah and Washington have enacted laws that provide for the licensing of Certificate Authorities. These statutes initially caused alarm among some members of Congress and the banking community due to fear of a patchwork of conflicting state laws governing the conduct of interstate commerce facilitated by PKI. However, these states have worked on cross-boarder recognition agreements to smooth the treatment of PKI between their jurisdictions. The states of California and Texas both enacted regulations that would deem accredited Certificate Authorities to be qualified as for special "approved" status for doing business with the state government or issuing certificates that may be relied upon by the state government. It is hoped that accreditation can provide a means of normalizing the treatment of certificate usage throughout state governments and between public and private sector parties who evaluate PKI Service Providers. Each of the states mentioned in this paragraph actively participates in the CARAT Task Force, in addition to other states and state government professional organizations. The advent of more standardized private law based treatment of PKI could set the stage for interoperability between levels of government and the private sector.

Accreditation of a PKI Service Provider for all purposes is beyond the scope of these Guidelines. These Guidelines have been drafted to support the creation of "affinity" Certificate Policies that govern categories of like parties, similar transactions and non-conflicting business environments. Such a Certificate Policy would not provide useful policy for accreditation of a PKI model as necessarily fit for all possible parties, transactions and environments. However, such a policy could be suitable for adoption by multiple organizations for such purposes as:

- Multi-state procurement and/or joint private sector procurement;
- Citizen to government account usage and/or consumer to private business account usage; or
- Government to government sensitive information sharing and/or hospital to hospitalsensitive information sharing.

For the time being, however, these Guidelines are expected to be used merely to facilitate the drafting of Certificate Policies that govern relatively closed or bounded communities, perhaps around a set of affinity applications. It is interesting to note, however, that the four cornered model discussed in Part C of this document would be particularly well suited (and designed?) to support scalable and more "open" PKI.

PART E. DRAFTING A CERTIFICATE POLICY

The following part is a Guideline for drafters of Certificate Policies.

E.1 These Guidelines Follow the IETF PKIX 4 Framework

The IETF PKIX 4 Framework is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF) and its working groups. The purpose of the IETF PKIX 4 Framework is to assist writers of certificate policies by providing a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a Certificate Policy. The IETF PKIX 4 Framework, although still

a working draft, has become a *de facto* standard for organizing both Certificate Policies and Certificate Practice Statements.

In the following sections, the CARAT Task Force provides to Certificate Policy writers drafting instructions for IETF PKIX 4 Framework sections 1, 2, 3, 4, and 8. The CARAT Task Force omits sections 5, 6, and 7 as these sections cover technical details that are too specific for guidelines.

Note, many commentators agree that the IETF PKIX 4 Draft is not the ideal outline for structuring a Certificate Policy. Nearly all writers will be tempted to change the outline to suit a particular set of logical needs. Nevertheless, the Task Force recommends using the IETF PKIX 4 Draft for the sake of interoperability and efficiency.

E.2 Organization

The Task Force has structured these Guidelines to follow the IETF PKIX 4 Framework. The Task Force has not renumbered or reorganized headings. However, where additional subject matter is appropriate, the Task Force has added headings, highlighting such headings by underlining them (for paper documents) and bolding them in red (for electronic documents).

In some cases, the Task Force has not provided drafting instructions for all low-level subheadings, but has instead collapsed low-level subheadings and included Discussion under a higher-level subheading. For instance, comment on subheadings 1.3.1, 1.3.2, and 1.3.3 are found in the Discussion under subheading 1.3. Finally, where there is no content under an IETF PKIX 4 Heading, the Task Force writes "No Stipulation."

For purposes of clarity and organization, the Task Force has added Drafting Instructions, Discussion, and Cross-References to each section of the IETF PKIX 4 Framework. Note, a Certificate Policy will *not* normally follow this three-part format.

- *Drafting Instructions*: At the beginning of each section, the Guidelines contain Drafting Instructions aimed at helping drafters write certificate policies. Drafting Instructions are written at a high level and are intended to be globally applicable to a variety of business models. Drafters are cautioned to consider differences in individual projects when attempting to apply any drafting instructions to their *specific* business model.

- *Discussion*: The second part of each section is a discussion that explains the Drafting Instructions or highlights specific issues that drafters should consider. The Discussion provides background, context, and an educational overview of the issues involved with the corresponding Drafting Instructions.

- *Cross-Reference*: Some sections of the IETF PKIX 4 Draft contain similar or, arguably, the same subject matter as other Framework sections. Where the subject matter of sections overlap, the Task Force provides cross-references to related sections.

- Where there is no content under a Drafting Instruction, Discussion, or Cross-Reference, the heading is absent.

INTRODUCTION

1.1 Overview

Drafting Instructions

The overview of a Certificate Policy is an introduction to the Policy. The overview states the drafter's methodology in organizing and structuring the Policy. The overview may also state the type of

transactions the Certificate Policy supports, the parties engaged in the transactions, and broad assumptions necessary to understanding and interpreting the Certificate Policy.

Discussion

1. A Certificate Policy should contain the "requirements" specified for the utilization of PKI for the particular type(s) of transactions in which End Entities will participate. In the context of an overview, it is helpful to state at a high or summary level the type of transactional relationship that the Certificate Policy supports as well as the identity of the parties that will participate in the transaction. If expressed at a high level, an overview can help to facilitate the establishment of the contractual arrangements between PKI Service Providers or a Policy Authority and End Entities.

2. The overview section is a high-level introduction to the Certificate Policy. Drafters are cautioned not to unnecessarily duplicate information contained in section "1.3 Community and Applicability."

3. Some policy writers include "introductory" statements directly below the heading "1. INTRODUCTION." Other policy writers include "overview" statements under "1.1 Overview." Still other policy writers include statements under both headings. Introductions and overviews are usually very similar and sometimes redundant. Unless there is a clear reason to do otherwise, drafters should include introductions and overviews under the heading "1.1 Overview" but not directly under "1. INTRODUCTION.".

Cross-Reference

Section 1.3 Community and Applicability.

1.2 Identification

Drafting Instructions

A Certificate Policy may be referenced in this section by an object identifier ("OID") assigned to the policy in the United States by the American National Standards Institute ("ANSI").

The following format is often used:

> This Policy is registered with _____, and has been assigned an object identifier ("OID") of _____.

Discussion

1. What is an OID?: An object identifier ("OID") is a unique numeric or alphanumeric identifier that unambiguously names an object. An object is anything that can be named, such as a Certificate Policy. It is envisioned that OIDs will be embedded in digital certificates so that PKI Service Providers. End Entities, and others can determine the set of rules under which an Issuer/Certificate Manufacturer has generated a certificate.

2. OIDs should be registered: The International Standards Organization ("ISO"), internationally, and ANSI, in the United States, facilitate the registration of OIDs for organizations. The purpose of registration is philosophically similar to the registration of legal entity names (corporations, partnerships, etc.) undertaken by the Secretary of State in most U.S. states. The idea is to ensure that all OIDs are unique. In this way, if a certificate references a Certificate Policy with an OID, there should never be confusion over which set of rules governs the certificate. Accordingly, if a Certificate Policy drafted under these Guidelines is to be referenced by an OID, the OID should

be registered with ANSI or an appropriate international standards body. OIDs should never be contrived.

3. Establishing an OID: The first step in obtaining an OID is to register an organization through an application process established by the American National Standards Institute ("ANSI"). See http://web.ansi.org/public/services/reg_org.html for more information on how to register an organization: see also ISO/IEC 9843-1: 1992. CCITT X.600. Organization Names are a unique numeric name and an optional alphanumeric name. Once an organization registers a numeric organization name the organization may create object identifiers by appending additional numeric suffixes to the organization name. For instance, if an organization name were {2 16 840 1} then an object identifier for a Certificate Policy written by that organization could be {2 16 840 1 100}.

American National Standards Institute (ANSI) Contact Information:

Address:

American National Standards Institute11 West 42nd Street13th floorNew York, N.Y. 10036

Telephone:+ 1 212 642 49 00

Telefax:+ 1 212 398 00 23

E-mail:info@ansi.org

WWW:http://www.ansi.org/4. Organization Name Registration Fees: As of August 1998. ANSI's fee schedule for organization name registration is as follows:

Registration fee for both name forms (numeric and alphanumeric)	$2,500
Registration fee for numeric name	$1,000
Registration fee for alphanumeric name (numeric name previously assigned)	$1,500
Challenge Fee	$2,500
Challenge Loser Fee	To be Determined
Inquiry Fee (per item)	$100

See http://web.ansi.org/public/services/org/fee.html.

5. OID Lookup: Presently, there is no standard means of looking up an OID. As a result, the establishment of an OID at this time may not be helpful in referencing a Certificate Policy. As more OIDs are registered, as demand for standard lookup procedures increases, and as standard rules for the use of OIDs develop. OIDs may prove to be a useful method of referencing a Certificate Policy. Accordingly, it is a business judgement whether or not to obtain an OID for a Certificate Policy.

6. International Name Registration: ANSI provides registration services for organizations within the United States. Organizations operating outside the United States must register with standards bodies in their home country. See http://www.iso.ch/ generally and http://www.iso.ch/addresse/membodies.html specifically for more information on standards bodies outside the United States. 7. Trademarking an OID to Deter Use by Issuers/Certificate Manufacturers Not a Party to the Certificate Policy: In a closed system, all certificates should contain the same OID which references the Certificate Policy with which the OID is associated. Likewise, because the system is closed, all Issuers/Certificate Manufacturers who generate certificates using the OID should be contractually bound to abide by the terms of the Certificate Policy to which the OID is associated. However, there is no means by which a Policy Authority (or anyone else) can prohibit Issuers/Certificate Manufactures who are not bound by the Certificate Policy from creating certificates with the same OID. As a result, a Relying Party could rely on a certificate from an Issuer/Certificate Manufacture who is not bound by the Certificate Policy. If reliance results in loss to the Relying Party, the Relying Party may have no recourse against the rogue Issuer/Certificate Manufacture or, at least, the rights and obligations of the Relying Party and the Issuer/Certificate Manufacture may be unclear.

If a Policy Authority wishes to deter rogue Issuers/Certificate Manufacturers from using a specific OID, a potential solution may be to trademark the OID. However, it is unclear whether an OID can be trademarked.

8. Whether an OID in a Certificate Incorporates a Certificate Policy by Reference?: Incorporating an external document can fail if the reference is not clear, the authenticity of the referenced document is lacking or uncertain, or if the intent to incorporate (as distinct from the intent merely to cite) is not clear from the document. Simply referencing a Certificate Policy by an object identifier in the certificate may well fall short in both the adequacy of the reference and the expression of an intention to incorporate. An object identifier is nothing more than a unique series of numbers, and its association with a particular document exists apart from the numbers and can be unreliable or obscure. An object identifier may not be considered a reference at all, and simply listing it in a field can be interpreted in many ways other than an effecting an incorporation.

1.3 Community and Applicability

Drafting Instructions

The community and applicability section contains headings under which drafters may state the roles to be played by parties in the system; the legal names of the parties operating under a Certificate Policy, or a means by which legal names can be ascertained: and the specific transactions governed by the Certificate Policy.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

    - 1.3.1 Certification authorities
    - 1.3.2 Registration authorities

- 1.3.3 End entities
- 1.3.4 Applicability

2. Section 1.3 of the IETF PKIX 4 Framework envisions a PKI with only two PKI Service Providers: Certification Authorities and a Registration Authorities. The CARAT Task Force, however, has defined additional PKI Service Providers. As a result, section 1.3 of the IETF PKIX 4 Framework does not fit well with CARAT vocabulary. A better outline for these Guidelines would be the following:

    - 1.3.1. PKI Service Providers
    - 1.3.2. End Entities
    - 1.3.3. Applicability

3. Defining the Roles of PKI Service Providers: Under a PKI Service Providers section, drafters would define the roles that parties operating under the Certificate Policy are expected to perform. A role definition might include a summary of the functions assigned to each role. Drafters should note that obligations arise based on functions assigned to a particular role. Thus, if a Party playing Role 1 is responsible for Functions 1, 2, and 3, then that Party will have obligations associated with Functions 1, 2, and 3. Obligations are stated in Section 2 of the IETF PKIX 4 Framework and should not be duplicated in this section.

4. Stating the Legal Names of PKI Service Providers: Alternatively or additionally, this section may state the legal names of PKI Service Providers performing roles, or a means by which the legal names of the PKI Service Providers can be ascertained.

Once a Certificate Policy is drafted, it is cumbersome to make changes to the document because change will usually require ratification and republication of the Certificate Policy and may require publication of a notice of change to Subscribers and Relying Parties. While it is useful to be able to add parties to Certificate Policy, it is not practical to change the Policy every time a new party joins the system. As a result, drafters may choose not to list the legal names of parties in a Certificate Policy.

If it is desirable nevertheless to have a means of ascertaining the parties to a Certificate Policy, drafters should consider incorporating party names by reference to an outside document. If the Certificate Policy is an electronic document, incorporation by reference may be done by including in the Policy a Uniform Resource Locator (“URL”) (i.e., web address) that points to a document (database or directory) listing all PKI Service Providers. If the Certificate Policy is a paper document, incorporation by reference may be done by attaching a paper addendum to the Policy. The utility of incorporation by reference is that new parties to the Certificate Policy can be added without the need for redrafting, ratifying, and republishing the Policy.

5. Bricks and Mortar and Online Locations of Registrars: Usually, Registrars take a Subscriber's initial application and verify the Subscriber's identity or credentials. If in-person identification is required. Subscribers must know the location of Registrar's physical locations. The Certificate Policy or a document incorporated by reference may provide the location and hours of operation of and Registrar's bricks and mortar establishment. If online identification is required, then Subscribers must know the Uniform Resource Locator (“URL”) (i.e., web address) of the Registrar's online establishment. This section of the IETF PKIX 4 Framework is the most appropriate section to list or incorporate by reference physical and online locations and hours of operation of Registrars.

6. Online Location of Repositories: If a system uses Repositories, this section is the most appropriate section to list or incorporate by reference the online locations of Repositories.

7. End Entities: In the End Entities section, drafters may state the types of Subscribers and Relying Parties who are authorized to use the system. It is not necessary and, indeed, it would be cumbersome to list the names of all Subscribers and Relying Parties. It is, however, important to ascertain in a closed system on a per transaction basis whether Subscribers and Relying Parties are contracted into the system.

8. Applicability: The applicability section may state the transactions governed by the Certificate Policy. The applicability section may also state transactions which are specifically prohibited under the Policy.

1.4 Contact Details

Drafting Instructions

In this section drafters should identify the Policy Authority, its scope of authority, and the contact person for the Policy Authority for purposes of communications related to the Policy.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

    - 1.4.1 Specification administration organization
    - 1.4.2 Contact person
    - 1.4.3 Person determining CPS suitability for the policy

2. 1.4.1 Specification administration organization: This document uses the term Policy Authority rather than Specification administration organization. This section will contain the legal name of a Policy Authority administering the Certificate Policy. This section may also contain the names and organizations of Policy Authority members.

    a. Membership: Unlike other PKI Service Providers, there will be only *one* Policy Authority. A Policy Authority may be a single entity. Alternatively, a Policy Authority may be an association of members. Policy Authority membership may be comprised of representatives of PKI Service Providers and End Entities. Policy Authority membership may also include government officials or even be a government agency.

    b. Primary Duties: The primary duties of a Policy Authority are to organize and administer a PKI and to write (or facilitate the writing) of the Certificate Policy that governs the PKI. A Policy Authority may or may not be responsible for organizing and administering the transaction being facilitated by PKI.

3. 1.4.2 Contact person: Contact details should be supplied for a person to contact at the Policy Authority.

4. 1.4.3 Person determining CPS suitability for the policy: Contact details should be supplied for the person who determines whether a company's documented practices are in compliance with the requirements of the Certificate Policy. If the person determining compliance is not the Policy Authority this should be stated.

2. GENERAL PROVISIONS2.1 Obligations

Drafting Instructions

A Certificate Policy should describe the obligations of each PKI Service Provider and End Entity to each of the other parties that are subject to the Certificate Policy.

Cross-Reference

See Part C. above.

2.2 Liability

Drafting Instructions

A Certificate Policy should describe any limits or requirements governing liability of parties based upon breach of contractual obligations by one or more parties to other parties.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

    - 2.2.1 CA Liability
    - 2.2.2 RA Liability

2. Strictly speaking in legal language, liability is a duty that has been adjudicated as immediately and unconditionally due. A liability has generally been reduced to a specified monetary amount or, less frequently, to a specific performance or injunction, and a court will direct law enforcement officials to collect or otherwise enforce the judgment. An obligation, on the other hand, is a duty generally based on a promise, and, although its performance is required, it is nevertheless not enforceable without an adjudication that converts it into a liability.[78]

[78]This distinction is not always maintained colloquially, although failure to observe it can lead to conceptual confusion.

Cross-Reference

See Part C. above.

2.3 Financial responsibility

Drafting Instructions

A Certificate Policy should indicate whether any PKI Service Provider is required to produce evidence of financial responsibility or indications of creditworthiness that help to assure that a PKI Service Provider is able to satisfy its liabilities.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

    - 2.3.1 Indemnification by Relying Parties
    - 2.3.2 Fiduciary Relationship
    - 2.3.3 Administrative Process

2. Evidence of financial responsibility or of creditworthiness might include instruments such as bonds or standby letters of credit. Other evidence of financial responsibility might include insurance policies

or balance sheets and asset reports. Where there is a right to collect, a Certificate Policy may also indicate how such rights are to be exercised.

3. Obligations that exist as part of a legally unenforceable ethos are important, but commerce generally insists on legal enforceability. An obligation that cannot be legally enforced may not be trustworthy by commercial standards.

The breach of an obligation can be reduced to a liability through adjudication (or arbitration), but that liability will not mean much if it cannot be collected.

4. In particular, it is to an Issuer's advantage to provide such assurances, and Relying Parties are well advised to seek such assurances before trusting a party, especially if the party is an Issuer.

2.4 Interpretation and Enforcement

Drafting Instructions

A Certificate Policy should describe all legal documents contemplated in addition to the Certificate Policy and should indicate the order of precedence of those documents.

2.4.1 Governing law

Drafting Instructions

A Certificate Policy should state the governing law under which the Certificate Policy will be interpreted. A Certificate Policy should also indicate whether implementing contracts and other relevant agreements may state governing law other than that stated for the Certificate Policy itself.

Discussion

1. A Certificate Policy may be governed by the laws of one state or by the laws of several states. In a single-jurisdiction contract system, a Certificate Policy should be governed by the law of the jurisdiction. It is possible, however, that a larger contract system would permit the same Certificate Policy to be interpreted under the law of more than one state. While inconsistent legal interpretation of a single Certificate Policy among jurisdictions is not an ideal result, such a result may be necessary in order to accommodate important parties to the system who negotiate inclusion of different choice of law provisions. Indeed, with respect to consumers, it may be impossible to separate a legal dispute from the jurisdiction in which the consumer has it principal contacts.

2. Since the Internet has no international borders, it may be pertinent to include provisions of law for international disputes, and/or disclaimers disavowing any intent to provide services to parties outside the US.

2.4.2 Severability, survival, merger, notice

Drafting Instructions

A Certificate Policy may contain contract provisions such as severability, survival, merger, and notice.

Discussion

1. The legal categories of severability, survival, merger and notice may require parsing into individual subheadings either under 2.4.2 (example: 2.4.2.1, etc.), or as separate headings under 2.4. To

maintain consistency with the PKIX document, and for the purposes of this initial document, they are maintained under 2.4.2 and categorized as appropriate.

2. If a Certificate Policy contains contract provisions, the Certificate Policy should state the order of precedence of the Certificate Policy contract provisions and provisions of other contracts, such as implementing contracts. It may not be possible in all situations to override the provisions of preexisting contracts with the provisions of the Certificate Policy.

3. Survival: The PKIX Standard includes a reference for a clause related to "survival". However, it is unclear as to which definition of "survival" was intended. There are two clear meanings of "survival." First, "survival" may refer to the continuation of the representations and warranties of the Certificate Policy in the event that clauses are severed, or the Policy as a whole fails when subjected to legal tests. (2) Second, "survival" may refer to the continuation of rights, duties and obligations as applied to successors and assigns of the certificate holder. For the purposes of this document, "survival" is assumed to be specific to the successors and assigns of parties associated with the Certificate issued.

4. Notice: Many legal obligations arise or are discharged as a result of notice or lack of notice of an event. A means of giving notification to all parties should be stipulated in a Certificate Policy. The following describes issues to consider regarding notice:

    a) *Physical Notice*: Physical notice may include a writing delivered by hand or certified or registered mail.

    b) *Virtual Notice - Insecure*: Insecure electronic methods of delivery such as fax and unsigned e-mail may be appropriate in certain circumstances. Those circumstances, if desired, should be documented in the Certificate Policy to provide notice of appropriate uses of each type of delivery.

    c) *Virtual Notice - Secure*: Notice by secure electronic methods, such as digitally signed messages, should be primary means of providing notification to all parties. A Certificate Policy may require parties to obtain a Registered E-Mail Address which would be considered a secure and reliable place to send and receive notification from all related parties. If Registered E-Mail Addresses are used, then a Certificate Policy may deem a message sent to a registered email address as received.

    d) *Notice Obligations*: With respect to notice, parties may be responsible for providing notification of (1) changes to the party's registered e-mail and postal address: (2) security compromises on the secrecy of the Subscriber's Private Key. Other types of notice events pertinent to the maintenance of the provisions of this Certificate Policy are covered throughout this document.

    e) *Acknowledgement*: In certain cases, notification may be considered ineffectual until the sending party receives a secured electronic acknowledgement.

5. Merger and integration. This section should include requirements that implementing contracts include provisions which incorporate the Certificate Policy and any other relevant documents and which specifies the order of precedence of the documents. For example, the Certificate Policy may provide that contracts shall include provisions which require that the contract is governed by the Certificate Policy.

6. Other Contract Provisions: Other contract provisions that may be contained in Certificate Policy are confidentiality, acts of God, termination, assignment and sub-contracting, waiver, and equal dignities clauses.

7. Acts of God: PKI Service Providers are usually obligated to provide backup procedures that contemplate and eliminate service failures as a result of Acts of God. Drafters should carefully consider whether standard Acts of God provisions should excuse PKI Service Providers in case of “unforeseen disaster.”

8. Examples:

Severability

In the event that any one or more of the provisions of this Certificate Policy shall for any reason be held to be invalid, illegal, or unenforceable in the courts of any state or of the United States of America, such unenforceability shall not affect any other provision, but this Certificate Policy shall then be construed as if such unenforceable provision or provisions had never been contained herein, and insofar as possible, construed to maintain the original intent of the parties.

Survival

Each and all of the provisions of the Agreement shall be binding upon and shall inure to the benefit of the parties hereto and their respective successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this Policy are assignable by the parties, by the operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this Policy, and provided further that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

Notice

Whenever any person hereto desires or is required to give any notice, demand, or request with respect to this Certificate Policy, such communication shall be made either using digitally signed messages consistent with the requirements of this Certificate Policy, or in writing. Electronic communications shall be effective upon the sender receiving a valid, digitally signed acknowledgment of receipt from recipient. Such acknowledgement must be received within five (5) days, or else written notice must then be communicated. Communications in writing must be delivered by a counter service that confirms delivery in writing or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows: Such communications shall be effective upon receipt.

Party's requiring receipt of notice under this Certificate Policy are required to provide notice of (1) changes in said party's address including postal and e-mail addresses: (2) security compromises on the Subscriber's Private Key: (3) changes in financial and/or personal information which would change the basis upon which the Certificate has been granted, and (4) any other notice pertinent to the maintenance of the provisions of this Certificate Policy.

Merger

It is expressly agreed that the provisions set forth herein constitute all understanding and agreements between the parties. Any prior agreements, promises, negotiations, or representations not expressly set forth in this Agreement are of no force and effect. No term or provision of this Certificate Policy directly affecting the respective rights and obligations of any party may be orally amended, waived, supplemented, modified, or terminated, except by an authenticated message or document of such affected party, except to the extent provided otherwise herein.

2.4.3 Dispute resolution procedures

Drafting Instructions

Dispute resolution procedures should be addressed in the Certificate Policy and should include mechanisms for resolving disputes short of litigation.

Discussion

1. This section would also include any requirements that may need to exist in implementation contracts to include dispute resolution for the contracts themselves. In addition, there should be discussion of resolving disputes prior to going to formal third party ADR. There should be reference to some help desk like functions, and formal process to communicate a formal request for action/payment (rather than having parties go right to litigation).

2.5 Fees

Drafting Instructions

This section may state whether PKI Service Providers are authorized to charge fees and any limitations or caps on fees.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

    - 2.5.1 Certificate issuance or renewal fees
    - 2.5.2 Certificate access fees
    - 2.5.3 Revocation or status information access fees
    - 2.5.4 Fees for other services such as policy information
    - 2.5.5 Refund policy

2. Types of fees that PKI Service Providers might charge are access fees on certificates, certificate status information, or CRLs. Usually, a fee should not be charged for reading a Certificate Policy.

2.6 Publication and Repository

Drafting Instructions

A Certificate Policy should state what information must be published by PKI Service Providers.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

    - 2.6.1 Publication of CA information
    - 2.6.2 Frequency of publication
    - 2.6.3 Access controls
    - 2.6.4 Repositories

2. It is presumed that a Policy Authority will make the Certificate Policy available to all parties. Nevertheless a Policy Authority may requires a PKI Service Provider to also publish the Certificate Policy to all parties to the Certificate Policy.

3. PKI Service Providers may be required to publish the following, among other things: issued certificates that reference the Certificate Policy, a Certificate Revocation List ("CRL") or online certificate status database, and the Issuer's certificate for its signing key.

Cross-Reference

See Section 2.1.1 and Section 2.1.5.

2.7 Compliance audit

Drafting Instructions

A Certificate Policy should include adequate and enforceable methods to assure compliance by each party participant.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

    - 2.7.1 Frequency of entity compliance audit
    - 2.7.2 Identity/qualifications of auditor
    - 2.7.3 Auditor's relationship to audited party
    - 2.7.4 Topics covered by audit
    - 2.7.5 Actions taken as a result of deficiency
    - 2.7.6 Communication of results

2. A Certificate Policy should establish a reasonable sound method of establishing compliance with that policy. This may be accomplished by providing for such measures as: contractual warranties of compliance with liquidated damages clauses or agreed upon mechanisms for oversight: self-audit (or self-reporting of audits conducted by independent auditors): in the case of an Issuer, proof of licensure by a state which licenses Issuers (CAs) (e.g., Utah and Washington) may be relevant and if applicable, evidence of acceptance by other states via reciprocity arrangements. If licensure were used as a policy compliance method, then the licensed party would also be expected to provide other evidence of compliance on those topics not addressed by licensure, such as an audit or contractual warranties.

There are different types of audits. There are, for example, financial audits and there are security audits for technical requirements and audits that are restricted to assuring compliance with other documented practices. In addition, there are regulatory audits, such as OCC audits of banks. IRS audits of tax paying individuals and entities, etc. Some public agencies may undergo audits by other public entities, such as the GAO or state Auditor offices.

3. Depending on the scope of the application and the particular obligations upon parties to the application, any number of methods might be appropriate to assure policy compliance. The compliance method used, whether it be audit based or not, should be selected based upon a cost, benefit and risk assessment associated with the obligations in question. If the pilot is strictly

internal, or if there is very little money or other liability associated with the pilot, then relatively lax compliance measures may be appropriate. If the application entails significant risk, then more elaborate and costly compliance measures may be appropriate. These matters would be expected to be fully detailed within the applicable contracts among the parties.

2.8 Confidentiality

Drafting Instructions

A Certificate Policy should provide that information in certificates is not confidential. A Certificate Policy should provide that other personally identifiable information not in a certificate should be considered confidential, unless otherwise provided in the Certificate Policy. Notices of any kind, including certificate revocation, should not be considered confidential with respect to parties to whom such notice is due under the Certificate Policy.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

    - 2.8.1 Types of information to be kept confidential
    - 2.8.2 Types of information not considered confidential
    - 2.8.3 Disclosure of certificate revocation/suspension information
    - 2.8.4 Release to law enforcement officials
    - 2.8.5 Release as part of civil discovery
    - 2.8.6 Disclosure upon owner's request
    - 2.8.7 Other information release circumstances

2. Data v. Transactional Privacy: There are two types of privacy that must be considered with respect to electronic transactions: data privacy and transactional privacy. Data privacy refers to the privacy and accuracy of data that a subject knows is being collected. Transactional privacy refers to the privacy and accuracy of transactional data that a subject may not know is being collected. Transactional information is generated whenever an electronic transaction takes place. Transactional information may or may not be collected as it is generated. When transactional data is collected, even if the subject of the transaction has no knowledge of collection, the subject has the same expectation of privacy as when a data is knowingly given.

3. Means and Methods of Using Data: Expectation of Privacy: There are different means and methods of using data which a subject either gives freely or which is collected without the subject's knowledge.

    - Computer Matching is any computer-supported process in which personal data records relating to many people are compared in order to identify cases of interest. Data records are usually collected with the knowledge of the subject. However, a subject may not know that information given for a known purpose, such as a certificate application, might also be used to create a saleable customer list using computer matching techniques.

    - Dataveillance is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons. Personal dataveillance is the investigation or monitoring of an identified person, generally for a specific reason. Mass

dataveillance is the investigation or monitoring of groups of people generally to identify individuals by interest. Dataveillance is usually done by monitoring transactional data.

Computer matching, dataveillance, and other data management and logging techniques should be employed by PKI Service Providers to increase the security of PKI systems and reduce the risk of fraud. Further, in some situations, techniques employed to maintain secure systems should not be publicized simply because knowledge of anti-fraud techniques potentially gives rise to new and inventive types of fraud. Nevertheless, subjects, especially End Entities who are consumers, have an expectation that any information collected about them, with or without knowledge, will be remain private.

4. The OECD Guidelines: The Organisation for Economic Co-operation and Development. Guidelines Governing the Protection of Privacy and Transborder Data Flow of Personal Data state the following Guidelines which the CARAT Task Force recommends to Policy Authorities in developing confidentiality and privacy protections:

    - *The collection limitation principle*: data should be obtained lawfully and fairly.

    - *The data quality principle*: data should be relevant to their purposes, accurate, complete and up-to-date.

    - *The purpose specification principle*: the identification of the purposes for which data will be used and destruction of the data if no longer necessary to serve that purpose.

    - *The use limitation principle*: use for purposes other than those specified is authorized only with consent of the data subject or by authority of law.

    - *The security safeguard principle*: procedures to guard against loss, corruption, destruction or misuse of data should be established.

    - *The openness principle*: it should be possible to acquire information about the collection, storage and use of personal data systems.

    - *The individual participation principle*: the data subject normally has a right of access and to challenge data relating to him or her.

    - *The accountability principle*: a data controller should be designed and accountable for complying with the measures to give effect to the principles.

Organisation for Economic Co-operation and Development, Guidelines Governing the Protection of Privacy and Transborder Data Flow of Personal Data, in 80 OECD Document C 58 (1980), reprinted in 20 I.L.M. 422 (1981).

5. Anonymous Transactions: One way to inhibit the use of transactional data is to keep transactions anonymous.

6. Public Relations: Since some pilots have a public relations or other public aspect, there will be a tension between maintaining confidential information and making public statements. The Policy Authority should assure that parties to any pilot are aware of the practices and policies associated with public statements to the media and other public statements from the beginning of the participation of party in the pilot.

7. Public Records Law: Particularly to the extent that pilots involve government entities that must abide by public records laws, maintaining confidentiality of data will be an important item for pilot policy and contracts.

8. Release to law enforcement officials and release as part of civil discovery: In some cases, otherwise confidential information may be required by law to be released, either to law enforcement officials or as part of civil discovery.

9. Privacy of Information in a Certificate: A certificate is usually publicly available. Accordingly, information in the certificate should not be considered confidential.

Cross-Reference

See Part C.

2.9 Intellectual Property Rights

Drafting Instructions

A Certificate Policy should specify intellectual property requirements as well as limits on the use of intellectual property related to the Certificate Policy and materials governed by the Certificate Policy. The Certificate Policy should limit the assertion of intellectual property rights on information that must be available in accordance with other sections of the Certificate Policy. In addition, any requirements related to intellectual property that must be included in implementing contracts or other agreements may be specified.

Discussion

1. Consider advisability of prohibiting intellectual property rights in certain aspects of system.

2. Trademark of OID may be acceptable.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

Drafting Instructions

A Certificate Policy should require Applicants/Subscribers to sign a Subscriber Agreement during the application process and before a certificate is issued. A Certificate Policy should specify the means by which communications between certificate Applicants/Subscribers and Issuers/Registrars or other PKI Service Providers are conducted.

Discussion

1. Subscriber Agreement: These Guidelines are intended for use with closed PKI systems. Accordingly, participation should be limited to defined Applicants/Subscribers who have signed a Subscriber agreement.

2. Application Process: Depending on the particular business model, an applicant may complete an application and sign a Subscriber agreement before the application is submitted for approval or an applicant may first complete an application and then, if approved, sign a Subscriber Agreement. Where the Applicant/Subscriber is to be a Relying Party, s/he may sign a Relying Party agreement simultaneously with the Subscriber agreement.

3. Communication: The Certificate Policy should state how a certificate application can be communicated from the Applicant/Subscriber to the Issuer/Registrar or other PKI Service Provider. Potential options include electronically via E-mail or a web site, (provided that all communication is secure

such as by using a suitable cryptographic protocol for electronic communications), by first class U.S. mail, or in-person.

The choice of the communication method is dependent upon a number of factors including whether an in-person identity confirmation process is required (see section 3.1.9 below) or whether the applicant is already known to the Issuer/Registrar or other PKI Service Provider such as in the case of an employee or an established customer.

3.1.1 Types of names

Drafting Instructions

A Certificate Policy should require that Issuers/Registrars express all names specified in a certificate as X.509 Distinguished Names. Any other information that may be required will be based upon the needs of the particular application.

Discussion

1. X.509 Standard: These Guidelines assume that an X.509 version 3 certificate will be used. Thus the Distinguished Name must conform to the X.509 standard.

2. Identifying information: In determining what other information, if any, may be required. Certificate Policy drafters should consider the applicant's common name, street address, locality name (the name of a city or town), state or province name, and country name. The Distinguished Name may also include an organization name (if the applicant has a significant identifying relationship with a particular organization) and an e-mail address (if the applicant has one and reads mail received at that address).

3. Privacy: In many applications, the information contained in a certificate will not be confidential. Accordingly, Certificate Policy drafters should seriously consider the privacy concerns associated with requiring that personally identifiable data be provided in certificate fields.

3.1.2 Need for names to be meaningful

Drafting Instructions

A Certificate Policy may, but need not, require names to be meaningful.

Discussion

1. Meaningful names: In the case where it is determined that a Certificate Policy should specify independently meaningful names, (i.e. where the name itself has meaning) Certificate Policy drafters should consider the following:

Element	Description
Common name	The first name, middle name or middle initial (if the Subscriber has a middle name), and the surname of the Subscriber, in that order, separated by space characters.
Street address	The physical location where the Subscriber resides or conducts business or where the Subscriber can receive paper mail.

Locality name	The city or town where the Subscriber resides or conducts business.
State or province name	The state or province in which the Subscriber resides or conducts business.
Country name	The nation in which the Subscriber resides or conducts business.
Organization name	An organization with which the Subscriber has a significant relationship. The organization name serves only as an additional identifier of the Subscriber and does not imply employment or any authority to act on behalf of the organization unless the certificate and/or its policy specifically provide otherwise.
Electronic mail address	An electronic mail address at which the Subscriber can receive electronic mail via the Internet. (Unless the Certificate Policy provides that the certificate is to be used within another network.)

2. Pseudonymous certificates: As noted in the Discussion section of Guideline 3.1.1. Certificate Policy drafters may seek to protect the privacy of Subscribers by choosing not to include personally identifiable data within a certificate. In this case, the name data in a certificate would still be uniquely associated with the Subscriber, but a Relying Party would link the certificate to the identity of the Subscriber through the use of other external information such as role and/or authority databases. Such certificates are known as pseudonymous certificates because the identity of the Subscriber is dependent upon information not included in the certificate.

3.1.3 Rules for interpreting various name forms

Drafting Instructions

A Certificate Policy may specify whether presence of Organizational Name is required. If an Organizational Name is required, a Certificate Policy should also specify whether the organizational name serves only as an additional identifier of the Subscriber, or indicates employment or the authority to act on behalf of the organization.

Discussion

1. Agency law implications: Whether the organizational name serves only as an additional identifier of the Subscriber or whether it indicates employment or authority is a significant issue for the Certificate Policy drafter because certificates can provide a SSubscriber with the authority to speak for an organization and thus incur liability for the organization based upon established agency law.

3.1.4 Uniqueness of names

Drafting Instructions

A Certificate Policy should assure that the Distinguished Name listed in a certificate is unambiguous and unique in relation to the person named within a defined naming domain.

Discussion

1. There are important technical and legal implications to this instruction.

   Technical perspective: From a technical perspective, all names listed in a given domain, such as a directory, must be unique. Otherwise, software relying on the uniqueness of names will "break." Breaking a directory or other unique domain will usually result in service interruptions.

   Legal perspective: From a legal perspective, even where there is a service interruption resulting from technical problems, legally there may be no actual damages that flow from the service interruption. That is, a directory may break, but if no one is actually damaged then there are no legal consequences. Thus, while a non-unique (or ambiguous) name is potentially catastrophic from a technical perspective, the legal consequences of ambiguity may not always be catastrophic.

3.1.7 Method to prove possession of private key

Drafting Instructions

A Certificate Policy should provide that an Issuer/Registrar must confirm that the Applicant/Subscriber is in possession of the private key corresponding to the public key specified in the application; that such private key is capable of creating a digital signature verifiable by the public key and an algorithm listed in the certificate; that the private key has not knowingly been compromised since its creation; that the public key is not shown in another certificate listed within a defined domain; and that there are no reasonable grounds to suspect that the Applicant/Subscriber's private key was obtained through theft, deceit, eavesdropping, or other unlawful means.

Discussion

1. Due diligence: The Issuer/Registrar or other PKI Service Provider must perform basic due diligence during the certificate application approval process.

3.1.8 Authentication of organization identity

Drafting Instructions

These Guidelines are intended for personal identity certificates only.

3.1.9 Authentication of individual identity

Drafting Instructions

A Certificate Policy should specify how the identity and other assertions of an Applicant/Subscriber are to be confirmed, whether in-person or through the use of online techniques.

Discussion

1. Options: In determining the method used to confirm the assertions of an applicant, drafters of a Certificate Policy should consider matters such as convenience and cost. For example, when an applicant is available in the same physical facility as the Issuer/Registrar or other PKI Service Provider, then in-person identity confirmation may be a convenient and relatively low cost method. It should also be recognized that the use of multiple databases to further confirm the assertions of an applicant could substantially increase the reliability of the confirmation process. In some cases, such as low-value or low-risk transactions, or where the applicant is in a distant location and is already known to the Issuer/Registrar or other PKI Service Provider, online

confirmation alone may be more appropriate. In other cases, a combination of in-person and online confirmation may be appropriate.

2. In-person identity confirmation: If personal appearance by the applicant with an Issuer/Registrar or other PKI Service Provider is required by a Certificate Policy, then all Applicants/Subscribers must appear in-person for identity confirmation prior to the issuance of a certificate. When confirming the assertions of an Applicant/Subscriber, Issuers/Registrars or other PKI Service Providers should require the Applicant/Subscriber to submit sufficient evidence of identity. Sufficient evidence of identify might be two pieces of identification, such as a valid government-issued picture ID or other identifying document that reasonably appears to the Issuer/Registrar or other PKI Service Provider to corroborate the applicant's assertion of identity.

3. Online confirmation: If a Certificate Policy permits online confirmation of identity and other Applicant/Subscriber assertions. Issuers/Registrars or other PKI Service Providers may require that the Applicant/Subscriber submit information that can be verified against independent databases. The information provided by the Applicant/Subscriber should be in substantial agreement with the information on the queried databases, considering any tolerances specified in the particular Certificate Policy.

4. Additional information: As described above, identity confirmation is of two fundamentally different kinds. A Certificate Policy should be clear about which of the two is involved. Confirmation procedures of Applicant/Subscriber assertions should be appropriate for the intended transaction supported by the certificate.

5. Standing Behind a Certificate: An Issuer/Registrar may “stand behind” a certificate. “Standing Behind” a certificate means that an Issuer/Registrar guarantees or warrants that the information in a certificate is true. Where an Issuer/Registrar agrees to stand behind a certificate its confirmation practices are irrelevant. Either the information in the certificate is true or it is not. If information is not true, the Issuer/Registrar will be liable for damages flowing from inaccuracies. An Issuer/Registrar may state reliance limits on a certificate. Where an Issuer/Registrar stands behind a certificate and states reliance limits, the Issuer/Registrar may disclaim or limit liability to Relying Parties who rely on certificates for amounts beyond the reliance limit. Reliance limits are useful for transactions that can be reduced to monetary terms. Reliance limits are not useful for transactions that cannot be reduced to monetary terms. An example of a transaction that cannot be reduced to monetary terms is a certificate that is used to identify a mother who may authorize her child to be let out of school. If a certificate is issued to an imposter who kidnaps the child, a reliance limit is meaningless. Where an Issuer/Registrar agrees to stand behind a certificate, it may not be necessary to state confirmation procedures in a Certificate Policy.

6. Promise to Perform Confirmation Procedures: As an alternative to standing behind a certificate, an Issuer/Registrar may promise to perform a stated set of confirmation procedures. Assuming the Issuer/Registrar performs the set of confirmation procedures according to a reasonable standard of care, the Issuer/Registrar may limit or disclaim all damages flowing from inaccuracies. Where an Issuer/Registrar agrees to perform a set of confirmation procedures, those confirmation procedures should be detailed in the Certificate Policy along with procedures for generating audit trails sufficient to determine whether confirmation procedures were performed in case of dispute.

3.2 Routine Rekey [Renewal]

Drafting Instructions

A Certificate Policy should specify the requirements that a Subscriber must meet in order to obtain renewal of his or her certificate, provided that the original certificate has not been revoked.

Discussion

1. Certificate renewal: Certificate drafters should consider how soon before the expiration of a certificate a renewal request may be made and how such request may be made. For example, if a renewal request is made electronically, then the Subscriber should submit the renewal request using a digitally signed message generated with the Subscriber's private key that corresponds to the public key contained in the original certificate.

3.3 Rekey after Revocation [Renewal after Revocation]

Drafting Instructions

A Certificate Policy should not permit renewal of a certificate that has been revoked or that has expired.

Discussion

1. Renewal limitations: If a Subscriber does not have a valid certificate which was issued under a Certificate Policy, then a new application and confirmation of identity and other assertions should be required.

3.4 Revocation Request

Drafting Instructions

A Certificate Policy should provide that a revocation request submitted electronically using a digital signature verifiable by a valid certificate will be processed. The Certificate Policy may allow a revocation request submitted in any other manner to result in the revocation of the certificate once the Issuer/Registrar or other PKI Service Provider is satisfied that the revocation request is authentic and has been submitted by a person authorized by the Subscriber to request revocation.

Discussion

1. Revocation considerations: The method used to confirm a revocation request should be as secure as is appropriate given the underlying business need. Significant liability could be the result of an invalid revocation.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Drafting Instructions

A Certificate Policy should prescribe the minimum content to be used for a certificate application. The Certificate Policy should also specify that all applications are subject to review, approval, and acceptance by the party specified in the Certificate Policy.

Discussion

1. In this section of a Certificate Policy, the Policy Authority should specify who is eligible to initiate the certificate application process. This requires the Policy Authority to have a clear understanding of how it envisions the application process to function. For example, the Policy Authority may specify that only the individual to be named as the Subscriber may initiate the certificate application process (perhaps requiring the approval of a duly authorized representative of the sponsor), or the Policy Authority may require a department head (or other authorized individual) to initiate the process on behalf of specific individuals.

2. If this application process is initiated electronically, it may be in either a secure or insecure environment. How secure the application process needs to be depends on the sensitivity of the intended use of the certificate and other relevant factors such as the relationship between the parties.

3. The Policy Authority may prescribe the approval process to be utilized in determining whether or not to issue a given certificate. This approval process includes the method for confirming the identity of the applicant (see Section 3.1.9). The totality of the application process (whether in person or on-line, whether initiated by the applicant him or herself, or by someone on their behalf, whether the applicant has to be an employee of a specific entity to have their application approved, etc) should be constructed so as to specifically apply to the particular business need the Policy Authority is implementing the PKI to address. In many business models, this function may be given to a Registrar; however, this may be allocated to another role.

Cross-Reference

Section 3.1, Initial Registration, Section 3.1.9, Authentication of Individual Identity

4.2 Certificate Issuance

Drafting Instructions

A Certificate Policy should require the issuance of a requested certificate only after the Subscriber identification and confirmation process is completed. The Certificate Policy should also require that the Subscriber be notified of the issuance of the certificate and should specify the process by which the certificate is delivered or otherwise made available to the Subscriber.

Discussion

1. When developing a Certificate Policy, the Policy Authority needs to specify who will be notified in the event of a rejected certificate application. In all likelihood, the Registrar will need to be notified; however, there may be situations (depending on the risk of unauthorized applications) when notifying the applicant of the rejection of their application is not advisable.

2. When the application is issued, the certificate *should not* be delivered or made available to any party other than the Subscriber (i.e. the certificate should not be delivered to a department head for distribution to personnel).

Cross-Reference

Section 3.1.9. Authentication of Individual Identity

4.3 Certificate Acceptance

Drafting Instructions

A Certificate Policy should require an Issuer to specify how the Subscriber accepts or rejects the certificate. Furthermore, the Certificate Policy should require the Subscriber to acknowledge that by accepting the certificate s/he agrees to the terms and conditions contained in the Certificate Policy in relation to that certificate.

Discussion

1. The policy developed by the Policy Authority should specify what constitutes acceptance of the certificate by the Subscriber. Accordingly, the contract between the Subscriber and the party

authorized under the Certificate Policy to enter into agreements with Subscribers (a Subscriber Agreement) should address the same issue. Under a particular Certificate Policy, acceptance can be treated in several ways. For instance, a Subscriber may be required to expressly indicate acceptance of the certificate, or may be deemed to have accepted the certificate when he or she uses it. A Policy Authority, in determining exactly what should constitute acceptance for a given Certificate Policy, should consider many factors, such as the number of Subscribers, the convenience (or lack thereof) of requiring express acceptance, and the importance of a Subscriber's proactively looking at a plain text version of his/her certificate to insure the accuracy of its contents before expressly indicating that he/she accepts the certificate, etc.

2. Whatever the method of acceptance being prescribed by the Certificate Policy, it must be made clear to the Subscriber that when s/he accepts a certificate s/he is agreeing to comply with the terms of the Certificate Policy (this provision is generally found in a Subscriber Agreement).

4.4 Certificate Revocation

4.4.1 Circumstances for revocation

Drafting Instructions

A Certificate Policy should specify the circumstances under which a certificate should be revoked. A Certificate Policy should provide for permissive revocation upon request of the Subscriber and required revocation when it is reasonably determined that a certificate is unreliable.

Discussion

There are two types of revocation: permissive revocation and required revocation. Permissive revocation occurs when a Subscriber requests revocation. Required revocation occurs when any party reasonably determines that a certificate is unreliable.

1. Permissive Revocation: A Subscriber may request revocation of his or her certificate at any time for any reason.

When developing a Certificate Policy, the Policy Authority also needs to determine whether an authorized representative of the Policy Authority or another member of the community that is subject to the Certificate Policy should be permitted to request the revocation of a certificate issued under the Certificate Policy, and if so, under what circumstances. For example, depending on the business model, the Registrar may also be permitted to trigger the revocation of a certificate.

2. Required Revocation: A certificate should be required to be revoked under the following circumstances:

- Whenever any of the information on the certificate is no longer accurate
- Whenever the private key associated with the certificate, or the media holding the private key, is or is suspected of having been compromised
- Whenever the Subscriber is no longer a member of the community that is subject to the Certificate Policy.
- Upon the request of the Subscriber
- If the Issuer determines that the certificate was not properly issued in accordance the Certificate Policy and/or any other applicable practice documents

- If the Issuer ceases operations. In such event, all certificates issued by the Issuer shall be revoked prior to the date operations cease.

3. A Certificate Policy should require that a Subscriber promptly notify the Issuer of any facts which could affect the reliability of a certificate, including but not limited to a compromise of the private key, a termination of the Subscriber's relationship with the community subject to the Certificate Policy, or a change in the factual information that appears on the certificate.

4. When drafting a Certificate Policy, the Policy Authority needs to consider the circumstances, if any, under which an authorized individual other than the Subscriber may be required to request revocation of a certificate. For instance, if an authorized representative is aware that the Subscriber is using the certificate inappropriately or that the Subscriber's employment is about to be terminated, the Certificate Policy may also permit this individual to request the revocation of a certificate.

Cross-Reference

Section 4.4.2.

4.4.2 Who can request revocation

Drafting Instructions

A Certificate Policy should indicate which parties are permitted to request revocation of a certificate.

Discussion

1. As in Section 4.4.1 above, when drafting a Certificate Policy, the Policy Authority needs to consider the circumstances, if any, under which a certificate revocation request by someone other than the Subscriber must be honored. The Certificate Policy should also address the issue of whether, and under what circumstances, non-Subscribers should be required to request revocation. For instance, if an authorized representative is aware that the Subscriber is using the certificate inappropriately or that the Subscriber's employment is about to be terminated, the Certificate Policy may also permit this individual to request the revocation of a certificate. If the Policy Authority wishes to allow an individual other than the Subscriber to be able to request revocation of a certificate, the Policy Authority will need to add that party to this section.

2. A Certificate Policy might only allow the Subscriber and Issuer to request revocation of a certificate. However, in cases where the Registrar is a separate entity, then the policy would probably allow the Registrar to request revocation as well because the Registrar may reasonably be expected to be in possession of information that is relevant to the validity of the certificate. For similar reasons, a Certificate Policy may permit a party such as a Repository to initiate revocation under prescribed circumstances, such as when a Repository is in possession of information that reasonably suggests that the Subscriber's private key has been compromised. It should be obvious, however, that an Issuer should be cautious in responding to requests for revocation that do not originate from the Subscriber, and that non-Subscriber requests should be honored only in circumstances where the risks of permitting reliance on a questionable certificate outweigh the inconvenience or potential loss to the Subscriber that could result from revocation.

Cross-Reference

Section 4.4.1.

4.4.3 Procedure for revocation request

Drafting Instructions

A Certificate Policy should specify the procedures to be followed by authorized parties in submitting a revocation request. Such procedures should require a certificate revocation request to be promptly communicated to the Issuer in a manner that allows the Issuer to ascertain the identity of the party initiating the request. A Certificate Policy should require an Issuer promptly to revoke a certificate for which it has received a revocation request from a Subscriber or other authorized party if the request complies with the procedures specified in the Certificate Policy.

Discussion

1. Depending on the business model being utilized, the revocation request may be submitted either directly to the Issuer or through another party such as the Registrar.

2. Because the various parties involved in a PKI have differing rights with respect to certificate revocation, it is important for the Issuer to obtain reliable evidence of the identity of the party initiating the request. Therefore, a Certificate Policy should require that if a certification request is communicated electronically, it should be digitally signed with the private key of the Subscriber. Alternatively, the Certificate Policy should provide that the Subscriber may request revocation by contacting the Issuer or a Registrar in person and providing adequate proof of identity.

3. If the Policy Authority has determined that the Certificate Policy will allow someone other than the Subscriber to request the revocation of a certificate, the Policy Authority should prescribe the procedure to be used by such individual or entity. If the party requesting revocation is not the Subscriber, the Policy Authority should consider whether and in what manner the request must be substantiated. In addition, the Certificate Policy should address whether any other due process is to be followed before revocation. For example, a Certificate Policy may address the issue of whether prior notice of revocation should be given to the Subscriber and whether the Subscriber should have an opportunity to object. Of course, there may be circumstances when Policy Authority may not wish to grant such due process rights to a Subscriber, such as when a Subscriber's employment is involuntarily terminated by a member of the community subject to the Certificate Policy and that employer has the right under the Certificate Policy to revoke the Subscriber's certificate.

4. The Policy Authority should realize that there are liability issues associated with the revocation of a certificate, and should require a high level of authentication/confirmation of these requests before revoking a certificate.

4.4.4 Revocation request grace period

Drafting Instructions

A Certificate Policy should specify how often requests for revocation must be processed.

Discussion

1. The length of time between the Issuer's receipt of a revocation request and the time the Issuer is required to revoke the certificate should bear a reasonable relationship to the amount of risk the participants are willing to assume that someone may rely on a certificate for which a proper revocation request has been given but not yet acted upon.

How quickly revocation requests need to be processed (and CRLs or certificate status databases need to be updated) depends upon the specific application for which the Policy Authority is drafting the Certificate Policy. A Policy Authority should recognize that there may be risk and cost tradeoffs with respect to grace periods for revocation notices. If the Policy Authority determines that its PKI participants are willing to

accept a grace period of a few hours in exchange for a lower implementation cost, the Certificate Policy may reflect that decision.

Cross-Reference

Section 4.4.9, CRL Issuance Frequency (If Applicable)

4.4.5 Circumstances for suspension

Drafting Instructions

These Guidelines do not support certificate suspension.

Discussion

1. Suspension is the temporary invalidation of a certificate, but since it wholly invalidates the certificate, albeit only temporarily, it can be seen as an excessively black-or-white tool for dealing with uncertainty. In cases where invalidation is unwarranted but the amounts at stake warrant significant attention, a PKI Service Provider can provide a message to a prospective Relying Party advising the party of a difficulty that has arisen. Such a message can be much more informative than a simple notation of temporary invalidity (suspension) because it can explain the situation and enable the Relying Party to arrive at a more informed decision whether to proceed to rely in a questionable situation or to forbear.

4.4.6 Who can request suspension

No Stipulation.

4.4.7 Procedure for suspension request

No Stipulation.

4.4.8 Limits on suspension period

No Stipulation.

4.4.9 CRL issuance frequency (if applicable)

Drafting Instructions

A Certificate Policy should require the Issuer to provide, promptly following revocation, notice to potential Relying Parties and any other parties specified in the Certificate Policy of the fact of revocation. A Certificate Policy should require prompt updating of the certificate revocation list, if one is used, or of the certificate status database, as applicable, and should require all revocation requests received by the Issuer and the resulting actions taken by the Issuer to be archived. A Certificate Policy should specify the manner and the period in which the certificate revocation list or certificate status database should be updated following revocation.

Discussion

1. It is critical for a Policy Authority to understand, and to reflect such understanding in a Certificate Policy, the importance of providing prompt notice of the fact of revocation to all potential Relying Parties. In current practice, this amounts to updating certificate revocation lists (CRLs) or certificate status databases in a timely manner. Exactly how often these updates need to take place is a function of the particular business of the Policy Authority or the intended use of the

certificate. For example, a university that is using certificates in order to allow students access to its library database may not be overly concerned if a Subscriber with a revoked certificate uses the library database once or twice before the CRL or certificate status database is updated (say every 24 hours). However, that same university using certificates for procurement is likely to be very concerned if a Subscriber with a revoked certificate authorizes a shipment of goods and the CRL or certificate status database had not been updated in time to reflect the revocation of the certificate (here updating only every 24 hours is probably not advisable).

2. Because the timing of notice to Relying Parties depends on how quickly an Issuer revokes a certificate and then advertises the fact of revocation, a Policy Authority may wish to consider requiring Issuers to perform the update of CRLs or certificate status databases simultaneously with the act of revocation. Whether or not a Policy Authority decides to require this may depend on a number of factors such as the foreseeable adverse consequences of delayed notice and the cost to the participants of simultaneous revocation and notice.

3. It is possible and perhaps likely that other forms of revocation advertisements may become available for use within PKI systems, and Policy Authorities should consider the usefulness of such forms in light of the requirements of their particular systems. As with CRLs and certificate status databases, such forms should be viewed in light of how well they provide effective notice of the fact of certificate revocation to potential Relying Parties, as well as other factors such as the cost to use those forms.

Cross-Reference

Section 2.6, Publication and Validation Services, Section 4.4.4 Revocation Request Grace Period, and Section 4.4.11 On-line Revocation/Status Checking Availability

4.4.10 CRL checking requirements

Drafting Instructions

If a certificate revocation list is used, a Certificate Policy should specify when a Relying Party should check a certificate revocation list in order to establish that the Relying Party's reliance upon a certificate was reasonable.

Discussion

A Policy Authority may determine that Relying Parties must check a CRL prior to every instance of reliance on a certificate. However, a Policy Authority may just as reasonably determine that checking a CRL for each instance of reliance is excessive and unnecessary, depending on the circumstances involved. For example, if a Relying Party engages in frequent transactions involving one or a few Subscribers or involving small-dollar transactions, it may be reasonable to permit checking of a CRL for something fewer than every certificate. Nevertheless, a Certificate Policy should address the issue of the Relying Party's obligations to check a CRL, since this bears directly on the reasonableness of reliance upon a certificate. In so doing, a Certificate Policy should also address what the appropriate consequences might be in the event a Relying Party fails to check a CRL as required.

4.4.11 On-line revocation/status checking availability

Drafting Instructions

A Certificate Policy should require the Issuer to provide, promptly following revocation, notice to potential Relying Parties and any other parties specified in the Certificate Policy of the fact of revocation. A Certificate Policy should require prompt updating of the certificate status database, if one is used, and should require all revocation requests received by the Issuer and the resulting actions taken by the Issuer

to be archived. A Certificate Policy should specify the manner and the period in which the certificate status database should be updated following revocation.

Discussion

1. This section is closely related to Section 4.4.4 and essentially duplicates Section 4.4.9 above. This section restates the drafting instructions in Section 4.4.9 as they apply to on-line certificate status databases as opposed to CRLs. A Policy Authority must look at the whole process (how quickly to process revocation requests, how often to update certificate status databases and how often to publish such update to a Repository) in light of the specific application for which the Policy Authority is drafting the Certificate Policy. See Section 4.4.9 for a more complete discussion of the business considerations.

Cross-Reference

Section 4.4.9 CRL Issuance Frequency (If Applicable)

4.4.12 On-line revocation checking requirements

Drafting Instructions

If an on-line certificate status database is used, a Certificate Policy should specify that the frequency with which a Relying Party must check the database in order to establish that the Relying Party's reliance upon a certificate was reasonable.

Discussion

A Policy Authority may determine that Relying Parties must check an on-line certificate status database prior to every instance of reliance on a certificate. However, a Policy Authority may just as reasonably determine that checking an on-line certificate status database for each instance of reliance is excessive and unnecessary, depending on the circumstances involved. For example, if a Relying Party engages in frequent transactions involving one or a few Subscribers or involving small-dollar transactions, it may be reasonable to permit checking of a certificate status database for something fewer than every certificate. Nevertheless, a Certificate Policy should address the issue of the Relying Party's obligations to check the status of a certificate online, since this bears directly on the reasonableness of reliance upon a certificate. In so doing, a Certificate Policy should also address what the appropriate consequences might be in the event a Relying Party fails to check a certificate status database as required.

Cross-Reference

Section 4.4.9 CRL Issuance Frequency (If Applicable), and Section 4.4.10 CRL Checking requirements.

4.4.13 Other forms of revocation advertisements available

No Stipulation.

4.4.14 Checking requirements for other forms of revocation advertisements

No Stipulation.

4.4.15 Special requirements re key compromise

No Stipulation.

4.5 Security Audit Procedures

Drafting Instructions

A Certificate Policy should assure that each party that undertakes important obligations also agrees to maintain adequate electronic records that pertain to such obligations. Policies should assure that sufficient records are kept to allow parties to access relevant and necessary information and to assist in carrying out the dispute resolution policies specified or permitted under the policy and as agreed upon by the parties. Record-keeping requirements should be tailored to meet no more than the actual needs for recordation based on the circumstances surrounding the business environment that the policy exists to facilitate.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

    - 4.5.1 Types of event recorded
    - 4.5.2 Frequency of processing log
    - 4.5.3 Retention period for audit log
    - 4.5.4 Protection of audit log
    - 4.5.5 Audit log backup procedures
    - 4.5.6 Audit collection system (internal vs external)
    - 4.5.7 Notification to event-causing subject
    - 4.5.8 Vulnerability assessments

2. In some cases, a given business system may require such record keeping not only to resolve disputes, but also to detect irregular patterns as they emerge for the purpose of preventing security breaches. The availability of auditable records may also be required under other applicable law, depending on the specific application and participating parties. The scope, detail and procedures surrounding record keeping policies should be proportional to the risks and costs in question. For example, an application which is only a relatively small dollar pilot may require only negligible records audit procedures.

Record-keeping requirements should be tailored to meet no more than the actual needs for recordation since record keeping can be time-consuming and costly, policies written under these guidelines should not require undue or excessive electronic record-keeping.

3. The issue raised in Section 2.7 as to whether to seek quality assurance through pre-audit, government license, contractual warranties or otherwise should not be confused with the word “audit” as it appears in this section. This section refers to the internal record-keeping procedures followed by participants that may form the basis of a future audit. The fact that a particular Certificate Policy written in compliance with these guidelines may include requirements under this section does not necessarily mean that the policy must require a quality assurance audit as a pre-condition to participation by a party. Policies that opt to assure quality assurance through contractual warranties may also specify that a party must be contractually required to keep records that are sufficiently accurate, comprehensive and secure from tampering for the purpose of assuring compliance with contractually agreed upon processes. In the event of future litigation that is based in whole or in part upon alleged breach of a contractual warranty to use a certificate in a certain way or to avoid issuing a certificate under certain circumstances, then the adequacy of credible records to show what actually happened will be important. Such records can prevent

unnecessary litigation by permitting parties to reconstruct a chain of events or the records could be critical in determining the outcome of a dispute that does end up in litigation.

4. In circumstances where financial remedies are a sufficient cure for any unfounded reliance on a certificate, then a Certificate Policy may not require specific security procedures to be taken by PKI Service Providers. Specifying security procedures in all circumstances may, in fact, interefere with a PKI Service Provider's business decision as to the most effective security procedures and risk management protocols.

5. Types of event recorded: A Certificate Policy may require all significant security events on the Issuer, Registrar, and Repository systems be automatically recorded to protected, electronically time-stamped audit trail files. Typical events that might be recorded by an Issuer include, but are not limited to, the following examples, (1) certificate issuances (2) certificate suspensions (3) certification revocations (4) changes of Issuer authority or delegations of authority (5) changes of Issuer employee access rights which impact certificate granting or revocation processes (6) internal Issuer key pair generation.

6. 4.5.3 Retention period for audit log: A Certificate Policy may state how long temporary audit trail files are required to be maintained onsite so that ad hoc reports and incident investigations can be made immediately, and set forth how they are to be securely archived thereafter in Section 4.6. Drafters might require that such files be retained for a period of months or years on-site, and then be securely archived off-site. Long-term (off-site) storage for audit trail records should be accomplished via media storage for a period of years after the date of the event.

7. 4.5.5 Audit log backup procedures: A Certificate Policy should require backup procedures of audit trail files to allow the same requirements and procedures afforded other critical files within an Issuer Registrar, and Repository's automated systems.

8. 4.5.7 Notification to event-causing subject: A Certificate Policy may state some automated scheme to report critical audited events to an appropriate person or system for immediate response as directed in the security plan.

9. 4.5.8 Vulnerability assessments: A Certificate Policy may require vulnerability assessments to be made by the Issuer, Registrar, and Repository of all internal processing applications and as needed by external audit functionaries. If required, such reports should be closely controlled and are required to be made available to the Policy Authority or other audit or compliance organizations upon request.

4.6 Records Archival

Drafting Instructions

This section of a Certificate Policy should include any requirements for records archival.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

    - 4.6.1 Types of event recorded
    - 4.6.2 Retention period for archive
    - 4.6.3 Protection of archive
    - 4.6.4 Archive backup procedures

- 4.6.5 Requirements for time-stamping of records
- 4.6.6 Archive collection system (internal or external)
- 4.6.7 Procedures to obtain and verify archive information

2. A Certificate Policy should address the archival requirements for certain data and files by PKI Service Providers, including how long that information is required to be securely maintained and whether these electronic records are required to be time-stamped. Data and files that a Certificate Policy may require to be archived include computer security audit data, certificate application data, certificates and CRLs generated, key histories and all correspondence between PKI Service Providers within the system. In the event the primary archives are lost or destroyed, a Certificate Policy may also require a complete set of back-up copies be maintained, and be readily available within a specified period of time. To prevent the loss or destruction of these archives, the Certificate Policy should also specify how the archived information is to be protected, both physically and cryptographically.

3. 4.6.1 Types of event recorded: A Certificate Policy may require that the following data and files be archived by or on behalf of Issuers, Registrars, and Repositories, according to their proper function: (1) computer security audit data. (2) certificate application data (3) certificates and CRLs generated (4) key histories (5) and all correspondence between the parties of the PKI.

4. 4.6.2 Retention period for archive: A Certificate may specify for how long key and certificate information must be securely maintained, and for how long audit trail files must be maintained.

5. 4.6.4 Archive backup procedures: Adequate backup procedures should be in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies can be recovered.

6. 4.6.5 Requirements for time-stamping of records: A Certificate Policy may specify that electronic records must be time-stamped by a trusted third-party time keeper.

7. 4.6.7 Procedures to obtain and verify archive information: If a security audit is required by a Certificate Policy, the Policy may require the auditor to verify the integrity of the archives and if the originals or the archives are corrupted or damaged in any material way, the corrupted or damaged copy should be replaced.

8. Drafters should pay attention to public law and internal organizational procedures for additional archive requirements.

4.7 Key changeover

Drafting Instructions

A Certificate Policy should indicate the minimum procedures, including process for secure new key distribution, associated with the change of a key pair used by Issuers to sign certificates.

Discussion

1. Key changeover refers to the change to a new key pair used by the Issuer to sign certificates. Among the issues to be considered are:

   - any notice requirements

- assuring reliability of the process for showing how the generations of keys interlock - such as by signing a hash of the new key with the old key.

4.8 Compromise and Disaster Recovery

Drafting Instructions

A Certificate Policy should require that PKI Service Providers to have in place a disaster recovery/business resumption plan in place.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

   - 4.8.1 Computing resources, software, and/or data are corrupted
   - 4.8.2 Entity public key is revoked
   - 4.8.3 Entity key is compromised
   - 4.8.4 Secure facility after a natural or other type of disaster

2. A disaster recovery plan could include any of the following:

   - set up and have operational a facility located in a geographically separate area that is capable of providing corresponding services in accordance with the Certificate Policy in the event of an unanticipated emergency.
   - provisions for redundancy of critical components, such as servers.
   - complete and periodic tests of the readiness of the backup facility.

For security reasons, this plan should not be made generally available. However, it must be made available to the individuals performing a security audit.

3. 4.8.2 Entity public key is revoked: A Certificate Policy may require Issuers to have in place a key compromise plan that addresses the procedures that will be followed if the Issuer's private signing key, the key used to issue certificates or used by a higher level Issuer, is compromised. This plan should include procedures for revoking all affected certificates and promptly notifying all affected parties operating under the Certificate Policy.

4. 4.8.4 Secure facility after a natural or other type of disaster: A Certificate Policy may require all PKI Service Providers to provide secure or backup facilities in contemplation of natural or other types of disasters.

Cross-Reference

Section 2.4.2 (Acts of God).

4.9 CA Termination

Drafting Instructions

If any PKI Service Provider ceases operation, the provider should promptly notify all parties operating under the Certificate Policy. A Certificate Policy should also specify a PKI Service Provider's obligations

as operations are ceasing. A Certificate Policy should require that all certificates issued by the Issuer that reference the Certificate Policy be revoked no later than the time of the termination.

8. SPECIFICATION ADMINISTRATION

Drafting Instructions

A Certificate Policy should provide for the process by which the policy is promulgated, amended and terminated and should provide for any other relevant functions of the Policy Authority with respect to specification of the Certificate Policy.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

    - 8.1 Specification change procedures
    - 8.2 Publication and notification policies
    - 8.3 CPS approval procedures

2. This section would include such issues as: the procedure for changing the policy; publication and notice requirements; approval process for other documents (such as the documented practices of a party or boilerplate documents of parties) and other substantive or procedural matters relating to the role and functions of the Policy Authority with respect to specification of the Certificate Policy.

Cross-Reference

Section 1.4.

Appendix IETF PKIX Framework

1. INTRODUCTION

1.1 Overview

1.2 Identification

1.3 Community and Applicability

1.3.1 Certification authorities

1.3.2 Registration authorities

1.3.3 End entities

1.3.4 Applicability

1.4 Contact Details

1.4.1 Specification administration organization

1.4.2 Contact person

1.4.3 Person determining CPS suitability for the policy

2. GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA obligations

2.1.2 RA obligations

2.1.3 Subscriber obligations

2.1.4 Relying party obligations

2.1.5 Repository obligations

2.2 Liability

2.2.1 CA liability

2.2.2 RA liability

2.3 Financial responsibility

2.3.1 Indemnification by relying parties

2.3.2 Fiduciary relationships

2.3.3 Administrative processes

2.4 Interpretation and Enforcement

2.4.1 Governing law

2.4.2 Severability, survival, merger, notice

2.4.3 Dispute resolution procedures

2.5 Fees

2.5.1 Certificate issuance or renewal fees

2.5.2 Certificate access fees

2.5.3 Revocation or status information access fees

2.5.4 Fees for other services such as policy information

2.5.5 Refund policy

2.6 Publication and Repository

2.6.1 Publication of CA information

2.6.2 Frequency of publication

2.6.3 Access controls

2.6.4 Repositories

2.7 Compliance audit

2.7.1 Frequency of entity compliance audit

2.7.2 Identity/qualifications of auditor

2.7.3 Auditor's relationship to audited party

2.7.4 Topics covered by audit

2.7.5 Actions taken as a result of deficiency

2.7.6 Communication of results

2.8 Confidentiality

2.8.1 Types of information to be kept confidential

2.8.2 Types of information not considered confidential

2.8.3 Disclosure of certificate revocation/suspension information

2.8.4 Release to law enforcement officials

2.8.5 Release as part of civil discovery

2.8.6 Disclosure upon owner's request

2.8.7 Other information release circumstances

2.9 Intellectual Property Rights

3 IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of names

3.1.2 Need for names to be meaningful

3.1.3 Rules for interpreting various name forms

3.1.4 Uniqueness of names

3.1.5 Name claim dispute resolution procedure

3.1.6 Recognition, authentication and role of trademarks

3.1.7 Method to prove possession of private key

3.1.8 Authentication of organization identity

3.1.9 Authentication of individual identity

3.2 Routine Rekey

3.3 Rekey after Revocation

3.4 Revocation Request

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.2 Certificate Issuance

4.3 Certificate Acceptance

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for revocation

4.4.10 CRL checking requirements

4.4.11 On-line revocation/status checking availability

4.4.12 On-line revocation checking requirements

4.4.13 Other forms of revocation advertisements available

4.4.14 Checking requirements for other forms of revocation advertisements

4.4.15 Special requirements re key compromise

4.4.2 Who can request revocation

4.4.3 Procedure for revocation request

4.4.4 Revocation request grace period

4.4.5 Circumstances for suspension

4.4.6 Who can request suspension

4.4.7 Procedure for suspension request

4.4.8 Limits on suspension period

4.4.9 CRL issuance frequency (if applicable)

4.5 Security Audit Procedures

4.5.1 Types of event recorded

4.5.2 Frequency of processing log

4.5.3 Retention period for audit log

4.5.4 Protection of audit log

4.5.5 Audit log backup procedures

4.5.6 Audit collection system (internal vs external)

4.5.7 Notification to event-causing subject

4.5.8 Vulnerability assessments

4.6 Records Archival

4.6.1 Types of event recorded

4.6.2 Retention period for archive

4.6.3 Protection of archive

4.6.4 Archive backup procedures

4.6.5 Requirements for time-stamping of records

4.6.6 Archive collection system (internal or external)

4.6.7 Procedures to obtain and verify archive information

4.7 Key changeover

4.8 Compromise and Disaster Recovery

4.8.1 Computing resources, software, and/or data are corrupted

4.8.2 Entity public key is revoked

4.8.3 Entity key is compromised

4.8.4 Secure facility after a natural or other type of disaster

4.9 CA Termination

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

5.1.1 Site location and construction

5.1.2 Physical access

5.1.3 Power and air conditioning

5.1.4 Water exposures

5.1.5 Fire prevention and protection

5.1.6 Media storage

5.1.7 Waste disposal

5.1.8 Off-site backup

5.2 Procedural Controls

5.2.1 Trusted roles

5.2.2 Number of persons required per task

5.2.3 Identification and authentication for each role

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

5.3.2 Background check procedures

5.3.3 Training requirements

5.3.4 Retraining frequency and requirements

5.3.5 Job rotation frequency and sequence

5.3.6 Sanctions for unauthorized actions

5.3.7 Contracting personnel requirements

5.3.8 Documentation supplied to personnel

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

6.1.2 Private key delivery to entity

6.1.3 Public key delivery to certificate issuer

6.1.4 CA public key delivery to users

6.1.5 Key sizes

6.1.6 Public key parameters generation

6.1.7 Parameter quality checking

6.1.8 Hardware/software key generation

6.1.9 Key usage purposes (as per X.509 v3 key usage field)

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

6.2.2 Private key (n out of m) multi-person control

6.2.3 Private key escrow

6.2.4 Private key backup

6.2.5 Private key archival

6.2.6 Private key entry into cryptographic module

6.2.7 Method of activating private key

6.2.8 Method of deactivating private key

6.2.9 Method of destroying private key

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

6.3.2 Usage periods for the public and private keys

6.4 Activation Data

6.4.1 Activation data generation and installation

6.4.2 Activation data protection

6.4.3 Other aspects of activation data

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

6.5.2 Computer security rating

6.6 Life Cycle Technical Controls

6.6.1 System development controls

6.6.2 Security management controls

6.6.3 Life cycle security ratings

6.7 Network Security Controls

6.8 Cryptographic Module Engineering Controls

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version number(s)

7.1.2 Certificate extensions

Editor's Notes

History