PKIX Working Group
Internet Draft

S. Chokhani (CygnaCom Solutions, Inc.)
W. Ford (VeriSign, Inc.)
R. Sabett (Cooley Godward LLP)
C. Merrill (McCarter & English, LLP)
S. Wu (Infoliance, Inc.)

Expires in six months from January 3, 2002

Internet X.509 Public Key Infrastructure

Certificate Policy and Certification Practices Framework

< draft-ietf-pkix-ipki-new-rfc2527-01.txt >

Status of this Memo

Abstract

This document presents a framework to assist the writers of certificate policies or certification practice statements for participants within public key infrastructures, such as certification authorities, policy authorities, and communities of interest that wish to rely on certificates. In particular, the framework provides a comprehensive list of topics that potentially

(at the writer's discretion) need to be covered in a certificate policy or a certification practice statement. This document is being submitted to the RFC Editor with a request for publication as an Informational RFC that will supercede RFC 2527 [CPF].

TABLE OF CONTENTS

---

1. INTRODUCTION

1.1 BACKGROUND

In general, a public-key certificate (hereinafter "certificate") binds a public key held by an entity (such as person, organization, account, device, or site) to a set of information that identifies the entity associated with use of the corresponding private key. In most cases involving identity certificates, this entity is known as the "subject" or "subscriber" of the certificate. Two exceptions, however, include devices (in which the subscriber is usually the individual or organization controlling the device) and anonymous

---

certificates (in which the identity of the individual or organization is not available from the certificate itself). Other types of certificates bind public keys to attributes of an entity other than the entity's identity, such as a role, a title, or creditworthiness information.

A certificate is used by a "certificate user" or "relying party" that needs to use, and rely upon the accuracy of, the binding between the subject public key distributed via that certificate and the identity and/or other attributes of the subject contained in that certificate. A relying party is frequently an entity that verifies a digital signature from the certificate's subject where the digital signature is associated with an email, web form, electronic document, or other data. Other examples of relying parties can include a sender of encrypted email to the subscriber, a user of a web browser relying on a server certificate during a secure sockets layer (SSL) session, and an entity operating a server that controls access to online information using client certificates as an access control mechanism. In summary, a relying party is an entity that uses a public key in a certificate (for signature verification and/or encryption). The degree to which a relying party can trust the binding embodied in a certificate depends on several factors. These factors can include the practices followed by the certification authority (CA) in authenticating the subject;

the CA's operating policy, procedures, and security controls; the scope of the subscriber's responsibilities (for example, in protecting the private key); and the stated responsibilities and liability terms and conditions of the CA (for example, warranties, disclaimers of warranties, and limitations of liability).

A Version 3 X.509 certificate may contain a field declaring that one or more specific certificate policies apply to that certificate [ISO1]. According to X.509, a certificate policy (CP) is "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements." A CP may be used by a relying party to help in deciding whether a certificate, and the binding therein, are sufficiently trustworthy and otherwise appropriate for a particular application. The CP concept is an outgrowth of the policy statement concept developed for Internet Privacy Enhanced Mail [PEM1] and expanded upon in [BAU1].

A more detailed description of the practices followed by a CA in issuing and otherwise managing certificates may be contained in a certification practice statement (CPS) published by or referenced by the CA. According to the American Bar Association Information Security Committee's Digital Signature Guidelines (hereinafter "DSG")(1) and the Information Security Committee's PKI Assessment Guidelines (hereinafter "PAG")(2), "a CPS is a statement of the practices which a certification authority employs in issuing certificates." [ABA1, ABA2] In general, CPSs also describe practices relating to all certificate lifecycle services (e.g., issuance, management, revocation, and renewal or re-keying), and CPSs provide details concerning other business, legal, and technical matters.

The terms contained in a CP or CPS may or may not be binding upon a PKI's participants as a contract. A CP or CPS may itself purport to be a contract. More commonly, however, an agreement may incorporate a CP or CPS by reference and therefore attempt to bind the parties of the agreement to some or all of its terms. For example, some PKIs may utilize a CP or (more commonly) a CPS that is incorporated by reference in the agreement between a subscriber and a CA or RA (called a "subscriber agreement") or the agreement between a relying party and a CA (called a "relying party agreement" or "RPA"). In other cases, however, a CP or CPS has no contractual significance at all. A PKI may intend these CPs and CPSs to be strictly informational or disclosure documents.

1.2 PURPOSE

The purpose of this document is twofold. First, the document aims

to explain the concepts of a CP and a CPS, describe the differences between these two concepts, and describe their relationship to subscriber and relying party agreements. Second, this document aims to present a framework to assist the writers and users of certificate policies or CPSs in drafting and understanding these documents. In particular, the framework identifies the elements that may need to be considered in formulating a CP or a CPS. The purpose is not to define particular certificate policies or CPSs, per se. Moreover, this document does not aim to provide legal advice or recommendations as to particular requirements or practices that should be contained within CPs or CPSs. (Such recommendations, however, appear in [ABA2].)

1.3 SCOPE

The scope of this document is limited to discussion of the topics that can be covered in a CP (as defined in X.509) or CPS (as defined in the DSG and PAG). In particular, this document describes the types of information that should be considered for inclusion in a CP or a CPS. While the framework as presented generally assumes use of the X.509 version 3 certificate format for the purpose of providing assurances of identity, it is not intended that the material be restricted to use of that certificate format or identity certificates. Rather, it is intended that this framework be adaptable to other certificate formats and to certificates providing assurances other than identity that may come into use.

The scope does not extend to defining security policies generally (such as organization security policy, system security policy, or data labeling policy). Further, this document does not define a specific CP or CPS. Moreover, in presenting a framework, this document should be viewed and used as a flexible tool presenting topics that should be considered of particular relevance to CPs or CPSs, and not as a rigid formula for producing CPs or CPSs.

This document assumes that the reader is familiar with the general concepts of digital signatures, certificates, and public-key infrastructure (PKI), as used in X.509, the DSG, and the PAG.

---

2. DEFINITIONS

This document makes use of the following defined terms:

Activation data - Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share).

Authentication - The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization. This process corresponds to the second process involved with identification, as shown in the definition of "identification" below. Authentication can also refer to a security service that provides assurances that individuals, organizations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the message's sender.

CA-certificate - A certificate for one CA's public key issued by another CA.

Certificate policy (CP) - A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.

Certification path - An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification Practice Statement (CPS) - A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.

CPS Summary (or CPS Abstract) - A subset of the provisions of a complete CPS that is made public by a CA.

Identification - The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. In the context of a PKI, identification refers to two processes: (1) establishing that a given name of an individual or organization corresponds to a real-world identity of an individual or organization, and (2) establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or organization. A person

---

seeking identification may be a certificate applicant, an applicant

for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems.

Issuing certification authority (issuing CA) - In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority).

Participant - An individual or organization that plays a role within a given PKI as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity.

PKI Disclosure Statement (PDS) - An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS.

Policy qualifier - Policy-dependent information that may accompany a CP identifier in an X.509 certificate. Such information can include a pointer to the URL of the applicable CPS or relying party agreement. It may also include text (or number causing the appearance of text) that contains terms of the use of the certificate or other legal information.

Registration authority (RA) - An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). [Note: The term Local Registration Authority (LRA) is sometimes used in other documents for the same concept.]

Relying party - A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

Relying party agreement (RPA) - An agreement between a certification authority and relying party that typically establishes the rights and responsibilities between those parties regarding the verification of digital signatures or other uses of certificates.

Set of provisions - A collection of practice and/or policy statements, spanning a range of standard topics, for use in

expressing a CP or CPS employing the approach described in this framework.

Subject certification authority (subject CA) - In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate (see also Issuing certification authority).

Subscriber - A subject of a certificate who is issued a certificate.

Subscriber Agreement - An agreement between a CA and a subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates.

Validation - The process of identification of certificate applicants. "Validation" is a subset of "identification" and refers to identification in the context of establishing the identity of certificate applicants.

3. CONCEPTS

This section explains the concepts of CP and CPS, and describes their relationship with other PKI documents, such as subscriber agreements and relying party agreements. Other related concepts are also described. Some of the material covered in this section and in some other sections is specific to certificate policies extensions as defined X.509 version 3. Except for those sections, this framework is intended to be adaptable to other certificate formats that may come into use.

3.1 CERTIFICATE POLICY

When a certification authority issues a certificate, it is providing a statement to a certificate user (i.e., a relying party) that a particular public key is bound to the identity and/or other attributes of a particular entity (the certificate subject, which is usually also the subscriber). The extent to which the relying party should rely on that statement by the CA, however, needs to be assessed by the relying party or entity controlling or coordinating the way relying parties or relying party applications use certificates. Different certificates are issued following different practices and procedures, and may be suitable for different applications and/or purposes.

The X.509 standard defines a CP as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security

requirements" [ISO1]. An X.509 Version 3 certificate may identify a specific applicable CP, which may be used by a relying party to decide whether or not to trust a certificate, associated public key, or any digital signatures verified using the public key for a particular purpose.

CPs typically fall into two major categories. First, some CPs "indicate the applicability of a certificate to a particular community" [ISO1]. These CPs set forth requirements for certificate usage and requirements on members of a community. For instance, a CP may focus on the needs of a geographical community,

---

such as the ETSI policy requirements for CAs issuing qualified certificates [ETS]. Also, a CP of this kind may focus on the needs of a specific vertical-market community, such as financial services [IDT].

The second category of typical CPs "indicate the applicability of a certificate to a . . . class of application with common security requirements." These CPs identify a set of applications or uses for certificates and say that these applications or uses require a certain level of security. They then set forth PKI requirements that are appropriate for these applications or uses. A CP within this category often makes sets requirements appropriate for a certain "level of assurance" provided by certificates, relative to certificates issued pursuant to related CPs. These levels of assurance may correspond to "classes" or "types" of certificates.

For instance, the Government of Canada PKI Policy Management Authority (GOC PMA) has established eight certificate policies in a single document [GOC], four policies for certificates used for digital signatures and four policies for certificates used for confidentiality encryption. For each of these applications, the document establishes four levels of assurances: rudimentary, basic, medium, and high. The GOC PMA described certain types of digital signature and confidentiality uses in the document, each with a certain set of security requirements, and grouped them into eight categories. The GOC PMA then established PKI requirements for each of these categories, thereby creating eight types of certificates, each providing rudimentary, basic, medium, or high levels of assurance. The progression from rudimentary to high levels corresponds to increasing security requirements and corresponding increasing levels of assurance.

A CP is represented in a certificate by a unique number called an "Object Identifier" (OID). That OID, or at least an "arc", can be registered. An "arc" is the beginning of the numerical sequence of

an OID and is assigned to a particular organization. The registration process follows the procedures specified in ISO/IEC and ITU standards. The party that registers the OID or arc also can publish the text of the CP, for examination by relying parties. Any one certificate will typically declare a single CP or, possibly, be issued consistent with a small number of different policies. Such declaration appears in the Certificate Policies extension of a X.509 Version 3 certificate. When a CA places multiple CPs within a certificate's Certificate Policies extension, the CA is asserting that the certificate is appropriate for use in accordance with any of the listed CPs.

CPs also constitute a basis for an audit, accreditation, or another assessment of a CA. Each CA can be assessed against one or more certificate policies or CPSs that 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 an assessment with respect to the certificate policies involved). The assessed set of

certificate policies is then indicated by the issuing CA in the CA-certificate. The X.509 certification path processing logic employs these CP indications in its well-defined trust model.

3.2 CERTIFICATE POLICY EXAMPLES

For example purposes, suppose that the International Air Transport Association (IATA) undertakes to define some certificate policies for use throughout the airline industry, in a PKI operated by IATA in combination with PKIs operated by individual airlines. Two CPs might be defined - the IATA General-Purpose CP, and the IATA Commercial-Grade CP.

The IATA General-Purpose CP could be used by industry personnel for protecting routine information (e.g., casual electronic mail) and for authenticating connections from World Wide Web browsers to servers for general information retrieval purposes. The key pairs may be generated, stored, and managed using low-cost, software-based systems, such as commercial browsers. Under this policy, a certificate may be automatically issued to anybody listed as an employee in the corporate directory of IATA or any member airline who submits a signed certificate request form to a network administrator in his or her organization.

The IATA Commercial-Grade CP could be used to protect financial transactions or binding contractual exchanges between airlines. Under this policy, IATA could require that certified key pairs be

generated and stored in approved cryptographic hardware tokens. Certificates and tokens could be provided to airline employees with disbursement authority. These authorized individuals might then be required to present themselves to the corporate security office, show a valid identification badge, and sign a subscriber agreement requiring them to protect the token and use it only for authorized purposes, as a condition of being issued a token and a certificate.

3.3 X.509 CERTIFICATE FIELDS

The following extension fields in an X.509 certificate are used to support CPs:

* Certificate Policies extension;
* Policy Mappings extension; and
* Policy Constraints extension.

3.3.1 Certificate Policies Extension

A Certificate Policies field lists CPs that the certification authority declares are applicable. Using the example of the IATA General-Purpose and Commercial-Grade policies defined in Section 3.2, the certificates issued to regular airline employees would contain the object identifier for General-Purpose policy. The certificates issued to the employees with disbursement authority would contain the object identifiers for both the General-Purpose policy and the Commercial-Grade policy. The inclusion of both

---

object identifiers in the certificates means that they would be appropriate for either the General-Purpose or Commercial-Grade policies. The Certificate Policies field may also optionally convey qualifier values for each identified policy; the use of qualifiers is discussed in Section 3.4.

When processing a certification path, a CP that is acceptable to the relying party application must be present in every certificate in the path, i.e., in CA-certificates as well as end entity certificates.

If the Certificate Policies field is flagged critical, it serves the same purpose as described above but also has an additional role. Specifically, it indicates that the use of the certificate is restricted to one of the identified policies, i.e., the certification authority is declaring that the certificate must only be used in accordance with the provisions of at least one of the listed CPs. This field is intended to protect the certification authority against claims for damages asserted by a relying party who

has used the certificate for an inappropriate purpose or in an inappropriate manner, as stipulated in the applicable CP.

For example, the Internal Revenue Service might issue certificates to taxpayers for the purpose of protecting tax filings. The Internal Revenue Service understands and can accommodate the risks of erroneously issuing a bad certificate, e.g., to an imposter. Suppose, however, that someone used an Internal Revenue Service tax-filing certificate as the basis for encrypting multi-million-dollar-value proprietary trade secrets, which subsequently fell into the wrong hands because of a cryptanalytic attack by an attacker who is able to decrypt the message. The Internal Revenue Service may want to defend itself against claims for damages in such circumstances by pointing to the criticality of the Certificate Policies extension to show that the subscriber and relying party misused the certificate. The critical-flagged Certificate Policies extension is intended to mitigate the risk to the CA in such situations.

3.3.2 Policy Mappings Extension

The Policy Mappings extension may only be used in CA-certificates. This field allows a certification authority to indicate that certain policies in its own domain can be considered equivalent to certain other policies in the subject certification authority's domain.

For example, suppose that for purposes of facilitating interoperability, the ACE Corporation establishes an agreement with the ABC Corporation to cross-certify the public keys of each others' certification authorities for the purposes of mutually securing their respective business-to-business exchanges. Further, suppose that both companies have pre-existing financial transaction protection policies called ace-e-commerce and abc-e-commerce, respectively. One can see that simply generating cross-certificates between the two domains will not provide the necessary interoperability, as the two companies' applications are configured

---

with, and employee certificates are populated with, their respective certificate policies. One possible solution is to reconfigure all of the financial applications to require either policy and to reissue all the certificates with both policies appearing in their Certificate Policies extensions. Another solution, which may be easier to administer, uses the Policy Mapping field. If this field is included in a cross-certificate for the ABC Corporation certification authority issued by the ACE Corporation certification authority, it can provide a statement that the ABC's financial transaction protection policy (i.e., abc-e-commerce) can be considered equivalent to that of the ACE Corporation (i.e., ace-

e-commerce). With such a statement included in the cross-certificate issued to ABC, relying party applications in the ACE domain requiring the presence of the object identifier for the ace-e-commerce CP can also accept, process, and rely upon certificates issued within the ABC domain containing the object identifier for the abc-e-commerce CP.

3.3.3 Policy Constraints Extension

The Policy Constraints extension supports two optional features. The first is the ability for a certification authority to require that explicit CP indications be present in all subsequent certificates in a certification path. Certificates at the start of a certification path may be considered by a relying party to be part of a trusted domain, i.e., certification authorities are trusted for all purposes so no particular CP is needed in the Certificate Policies extension. Such certificates need not contain explicit indications of CP. When a certification authority in the trusted domain, however, certifies outside the domain, it can activate the requirement that a specific CP's object identifier appear in subsequent certificates in the certification path.

The other optional feature in the Policy Constraints field is the ability for a certification authority to disable policy mapping by subsequent certification authorities in a certification path. It may be prudent to disable policy mapping when certifying outside the domain. This can assist in controlling risks due to transitive trust, e.g., a domain A trusts domain B, domain B trusts domain C, but domain A does not want to be forced to trust domain C.

3.3.4 Policy Qualifiers

The Certificate Policies extension field has a provision for conveying, along with each CP identifier, additional policy-dependent information in a qualifier field. The X.509 standard does not mandate the purpose for which this field is to be used, nor does it prescribe the syntax for this field. Policy qualifier types can be registered by any organization.

The following policy qualifier types are defined in PKIX RFC 2459 [PKI1]:

(a) The CPS Pointer qualifier contains a pointer to a CPS, CPS Summary, RPA, or PDS published by the CA. The pointer is in the

---

form of a uniform resource identifier (URI).

(b) The User Notice qualifier contains a text string that is to be displayed to subscribers and relying parties prior to the use of the certificate. The text string may be an IA5String or a BMPString - a subset of the ISO 100646-1 multiple octet coded character set. A CA may invoke a procedure that requires that the relying party acknowledge that the applicable terms and conditions have been disclosed and/or accepted.

Policy qualifiers can be used to support the definition of generic, or parameterized, CPs. Provided the base CP so provides, policy qualifier types can be defined to convey, on a per-certificate basis, additional specific policy details that fill in the generic definition.

3.4 CERTIFICATION PRACTICE STATEMENT

The term certification practice statement (CPS) is defined by the DSG and PAG as: "A statement of the practices which a certification authority employs in issuing certificates." [ABA1, ABA2] As stated above, a CPS establishes practices concerning lifecycle services in addition to issuance, such as certificate management (including publication and archiving), revocation, and renewal or re-keying. In the DSG, the ABA expands this definition with the following comments:

"A certification practice statement may take the form of a declaration by the certification authority of the details of its trustworthy system and the practices it employs in its operations and in support of issuance of a certificate . . . ." This form of CPS is the most common type, and can vary in length and level of detail.

Some PKIs may not have the need to create a thorough and detailed statement of practices. For example, the CA may itself be the relying party and would already be aware of the nature and trustworthiness of its services. In other cases, a PKI may provide certificates providing only a very low level of assurances where the applications being secured may pose only marginal risks if compromised. In these cases, an organization establishing a PKI may only want to write or have CAs use a subscriber agreement, relying party agreement, or agreement combining subscriber and relying party terms, depending on the role of the different PKI participants. In such a PKI, that agreement may serve as the only "statement of practices" used by one or more CAs within that PKI. Consequently, that agreement may also be considered a CPS and can be entitled or subtitled as such.

Likewise, since a detailed CPS may contain sensitive details of its system, a CA may elect not to publish its entire CPS. It may instead opt to publish a CPS Summary (or CPS Abstract). The CPS Summary would contain only those provisions from the CPS that the CA considers to be relevant to the participants in the PKI (such as the

responsibilities of the parties or the stages of the certificate lifecycle). A CPS Summary, however, would not contain those

sensitive provisions of the full CPS that might provide an attacker with useful information about the CA's operations. Throughout this document, the use of "CPS" includes both a detailed CPS and a CPS Summary (unless otherwise specified).

CPSs do not automatically constitute contracts and do not automatically bind PKI participants as a contract would. Where a document serves the dual purpose of being a subscriber or relying party agreement and CPS, the document is intended to be a contract and constitutes a binding contract to the extent that a subscriber or relying party agreement would ordinarily be considered as such. Most CPSs, however, do not serve such a dual purpose. Therefore, in most cases, a CPS's terms have a binding effect as contract terms only if a separate document creates a contractual relationship between the parties and that document incorporates part or all of the CPS by reference. Further, if a particular PKI employs a CPS Summary (as opposed to the entire CPS), the CPS Summary could be incorporated into any applicable subscriber or relying party agreement.

In the future, a court or applicable statutory or regulatory law may declare that a certificate itself is a document that is capable of creating a contractual relationship, to the extent its mechanisms designed for incorporation by reference (such as the Certificate Policies extension and its qualifiers) indicate that terms of its use appear in certain documents. In the meantime, however, some subscriber agreements and relying party agreements may incorporate a CPS by reference and therefore make its terms binding on the parties to such agreements.

3.5 RELATIONSHIP BETWEEN CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT

The CP and CPS address the same set of topics that are of interest to the relying party in terms of the degree to and purpose for which a public key certificate should be trusted. Their primary difference is in the focus of their provisions. A CP sets forth the requirements and standards imposed by the PKI with respect to the various topics. In other words, the purpose of the CP is to establish what participants must do. A CPS, by contrast, states how a CA and other participants in a given domain implement procedures and controls to meet the requirements stated in the CP. In other words, the purpose of the CPS is to disclose how the participants perform their functions and implement controls.

An additional difference between a CP and CPS relates the scope of coverage of the two kinds of documents. Since a CP is a statement of requirements, it best serves as the vehicle for communicating minimum operating guidelines that must be met by interoperating PKIs. Thus, a CP generally applies to multiple CAs, multiple organizations, or multiple domains. By contrast, a CPS applies only to a single CA or single organization and is not generally a vehicle to facilitate interoperation.

A CA with a single CPS may support multiple CPs (used for different application purposes and/or by different relying party communities). Also, multiple CAs, with non-identical CPSs, may support the same CP.

For example, the Federal Government might define a government-wide CP for handling confidential human resources information. The CP will be a broad statement of the general requirements for participants within the Government's PKI, and an indication of the types of applications for which it is suitable for use. Each department or agency wishing to operate a certification authority in this PKI may be required to write its own certification practice statement to support this CP by explaining how it meets the requirements of the CP. At the same time, a department's or agency's CPS may support other certificate policies.

An additional difference between a CP and CPS concerns the level of detail of the provisions in each. Although the level of detail may vary among CPSs, a CPS will generally be more detailed than a CP. A CPS provides a detailed description of procedures and controls in place to meet the CP requirements, while a CP is more general.

The main differences between CPs and CPSs can therefore be summarized as follows:

(a) A PKI uses a CP to establish requirements that state what participants within it must do. A single CA or organization can use a CPS to disclose how it meets the requirements of a CP or how it implements its practices and controls.

(b) A CP facilitates interoperation through cross-certification, unilateral certification, or other means. Therefore, it is intended to cover multiple CAs. By contrast, a CPS is a statement of a single CA or organization. Its purpose is not to facilitate interoperation (since doing so is the function of a CP).

(c) A CPS is generally more detailed than a CP and specifies how

the CA meets the requirements specified in the one or more CPs under which it issues certificates.

In addition to populating the certificate policies extension with the applicable CP object identifier, a certification authority may include, in certificates it issues, a reference to its certification practice statement. A standard way to do this, using a CP qualifier, is described in Section 3.4.

3.6 RELATIONSHIP AMONG CPs, CPSs, AGREEMENTS, AND OTHER DOCUMENTS

CPs and CPSs play a central role in documenting the requirements and practices of a PKI. Nonetheless, they are not the only documents relevant to a PKI. For instance, subscriber agreements and relying party agreements play a critical role in allocating responsibilities to subscribers and relying parties relating to the use of certificates and key pairs, and establish the terms and conditions

under which certificates are issued, managed, and used. The term subscriber agreement is defined by the PAG as: "An agreement between a CA and a subscriber that establishes the right and obligations of the parties regarding the issuance and management of certificates." [ABA2] The PAG defines a relying party agreement as: "An agreement between a certification authority and relying party that typically establishes the rights and obligations between those parties regarding the verification of digital signatures or other uses of certificates." [ABA2]

As mentioned in Section 3.5, a subscriber agreement, relying party agreement, or an agreement that combines subscriber and relying party terms may also serve as a CPS. In other PKIs, however, a subscriber or relying party agreement may incorporate some or all of the terms of a CP or CPS by reference. Yet other PKIs may distill from a CP and/or CPS the terms that are applicable to a subscriber and place such terms in a self-contained subscriber agreement, without incorporating a CP or CPS by reference. They may use the same method to distill relying party terms from a CP and/or CPS and place such terms in a self-contained relying party agreement. Creating such self-contained agreements has the advantage of creating documents that are easier for consumers to review. In some cases, subscribers or relying parties may be deemed to be "consumers" under applicable law, who are subject to certain statutory or regulatory protections. Under the legal systems of civil law countries, incorporating a CP or CPS by reference may not be effective to bind consumers to the terms of an incorporated CP or CPS.

CPs and CPSs may be incorporated by reference in other documents, including:
* Interoperability agreements (including agreements between CAs for cross-certification, unilateral certification, or other forms of interoperation),
* Vendor agreements (under which a PKI vendor agrees to meet standards set forth in a CP or CPS), or
* A PDS.
See [ABA2]

A PDS serves a similar function to a CPS Summary. It is a relatively short document containing only a subset of critical details about a PKI or CA. It may differ from a CPS Summary, however, in that its purpose is to act as a summary of information about the overall nature of the PKI, as opposed to simply a condensed form of the CPS. Moreover, its purpose is to distill information about the PKI, as opposed to protecting security sensitive information contained in an unpublished CPS, although a PDS could also serve that function.

Just as writers may wish to refer to a CP or CPS or incorporate it by reference in an agreement or PDS, a CP or CPS may refer to other documents when establishing requirements or making disclosures. For instance, a CP may set requirements for certificate content by referring to an external document setting forth a standard

---

certificate profile. Referencing external documents permits a CP or CPS to impose detailed requirements or make detailed disclosures without having to reprint lengthy provisions from other documents within the CP or CPS. Moreover, referencing a document in a CP or CPS is another useful way of dividing disclosures between public information and security sensitive confidential information (in addition to or as an alternative to publishing a CPS Summary). For example, a PKI may want to publish a CP or CPS, but maintain site construction parameters for CA high security zones as confidential information. In that case, the CP or CPS could reference an external manual or document containing the detailed site construction parameters.

Documents that a PKI may wish to refer to in a CP or CPS include:
* A security policy,
* Training, operational, installation, and user manuals (which may contain operational requirements),
* Standards documents that apply to particular aspects of the PKI (such as standards specifying the level of protection offered by any hardware tokens used in the PKI or standards applicable to the site construction),

* Key management plans,
* Human resource guides and employment manuals (which may describe some aspects of personnel security practices), and
* E-mail policies (which may discuss subscriber and relying party responsibilities, as well as the implications of key management, if applicable).
See [ABA2]

3.7 SET OF PROVISIONS

A set of provisions is a collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a CP or CPS employing the approach described in this framework by covering the topic appearing in Section 5 below, which are described in detail in Section 4 below.

A CP can be expressed as a single set of provisions.

A CPS can be expressed as a single set of provisions with each component addressing the requirements of one or more certificate policies, or, alternatively, as an organized collection of sets of provisions. For example, a CPS could be expressed as a combination of the following:

(a) a list of certificate policies supported by the CPS;

(b) for each CP in (a), a set of provisions that contains statements responding to that CP by filling in details not stipulated in that policy or expressly left to the discretion of the CA (in its CPS) ; such statements serve to state how this particular CPS implements the requirements of the particular CP; or

---

(c) a set of provisions that contains statements regarding the certification practices on the CA, regardless of CP.

The statements provided in (b) and (c) may augment or refine the stipulations of the applicable CP, but generally must not conflict with any of the stipulations of such CP. In certain cases, however, a policy authority may permit exceptions to the requirements in a CP, because certain compensating controls of the CA are disclosed in its CPS that allow the CA to provide assurances that are equivalent to the assurances provided by CAs that are in full compliance with the CP.

This framework outlines the contents of a set of provisions, in terms of nine primary components, as follows:

1. Introduction
2. Publication and Repository
3. Identification and Authentication
4. Certificate Life-Cycle Operational Requirements
5. Facilities, Management, and Operational Controls
6. Technical Security Controls
7. Certificate, CRL, and OCSP Profile
8. Compliance audit
9. Other Business and Legal Matters

PKIs can use this simple framework of nine primary components to write a simple CP or CPS. Moreover, a CA can use this same framework to write a subscriber agreement, relying party agreement, or agreement containing subscriber and relying party terms. If a CA uses this simple framework to construct an agreement, it can use paragraph 1 as an introduction or recitals, it can set forth the responsibilities of the parties in paragraphs 2-8, and it can use paragraph 9 to cover the business and legal issues described in more detail in, and using the ordering of, Section 4.9 below (such as representations and warranties, disclaimers, and liability limitations). The ordering of topics in this simple framework and the business and legal matters Section 4.9 is the same as (or similar to) the ordering of topics in a typical software or other technology agreement. Therefore, a PKI can establish a set of core documents (with a CP, CPS, subscriber agreement, and relying party agreement) all having the same structure and ordering of topics, thereby facilitating comparisons and mappings among these documents and among the corresponding documents of other PKIs.

This simple framework may also be useful for agreements other than subscriber agreements and relying party agreements. For instance, a CA wishing to outsource certain services to an RA or certificate manufacturing authority (CMA) may find it useful to use this framework as a checklist to write a registration authority agreement or outsourcing agreement. Similarly, two CAs may wish to use this simple framework for the purpose of drafting a cross-certification, unilateral certification, or other interoperability agreement.

In short, the primary components of the simple framework (specified above) may meet the needs of drafters of short CPs, CPSs, subscriber agreements, and relying party agreements. Nonetheless, this framework is extensible, and its coverage of the nine components is flexible enough to meet the needs of drafters of comprehensive CPs and CPSs. Specifically, components appearing above can be further divided into subcomponents, and a subcomponent may comprise multiple elements. Section 4 provides a more detailed description of the contents of the above components, and their

subcomponents. Drafters of CPs and CPSs are permitted to add additional levels of subcomponents below the subcomponents described in Section 4 for the purpose of meeting the needs of the drafter's particular PKI.

4. CONTENTS OF A SET OF PROVISIONS

This section expands upon the contents of the simple framework of provisions, as introduced in Section 3.7. The topics identified in this section are, consequently, candidate topics for inclusion in a detailed CP or CPS.

While many topics are identified, it is not necessary for a CP or a CPS to include a concrete statement for every such topic. Rather, a particular CP or CPS may state "no stipulation" for a component, subcomponent, or element on which the particular CP or CPS imposes no requirements or makes no disclosure. In this sense, the list of topics can be considered a checklist of topics for consideration by the CP or CPS writer.

It is recommended that each and every component and subcomponent be included in a CP or CPS, even if there is "no stipulation"; this will indicate to the reader that a conscious decision was made to include or exclude a provision concerning that topic. This drafting style protects against inadvertent omission of a topic, while facilitating comparison of different certificate policies or CPSs, e.g., when making policy mapping decisions.

In a CP, it is possible to leave certain components, subcomponents, and/or elements unspecified, and to stipulate that the required information will be indicated in a policy qualifier, or the document to which a policy qualifier points. Such CPs can be considered parameterized definitions. The set of provisions should reference or define the required policy qualifier types and should specify any applicable default values.

4.1 INTRODUCTION

This component identifies and introduces the set of provisions, and indicates the types of entities and applications for which the document (either the CP or the CPS being written) is targeted.

4.1.1 Overview

This subcomponent provides a general introduction to the document being written. This subcomponent can also be used to provide a

synopsis of the PKI to which the CP or CPS applies. For example, it may set out different levels of assurance provided by certificates within the PKI. Depending on the complexity and scope of the particular PKI, a diagrammatic representation of the PKI might be useful here.

4.1.2 Document Name and Identification

This subcomponent provides any applicable names or other identifiers, including ASN.1 object identifiers, for the document. An example of such a document name would be the US Federal Government Policy for Secure E-mail.

4.1.3 PKI Participants

This subcomponent describes the identity or types of entities that fill the roles of participants within a PKI, namely:

* Certification authorities, i.e., the entities that issue certificates. A CA is the issuing CA with respect to the certificates it issues and is the subject CA with respect to the CA certificate issued to it. CAs may be organized in a hierarchy in which an organization's CA issues certificates to CAs operated by subordinate organizations, such as a branch, division, or department within a larger organization.

* Registration authorities, i.e., the entities that establishment enrollment procedures for end-user certificate applicants, perform identification and authentication of certificate applicants, initiate or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of a CA. Subordinate organizations within a larger organization can act as RAs for the CA serving the entire organization, but RAs may also be external to the CA.

* Subscribers. Examples of subscribers who receive certificates from a CA include employees of an organization with its own CA, banking or brokerage customers, organizations hosting e-commerce sites, organizations participating in a business-to-business exchange, and members of the public receiving certificates from a CA issuing certificates to the public at large.

* Relying parties. Examples of relying parties include employees of an organization having its own CA who receive digitally signed e-mails from other employees, persons buying goods and services from e-commerce sites, organizations participating in a business-to-business exchange who receive bids or orders from other participating organizations, and individuals and organizations doing business with subscribers who have received their certificates from a CA issuing certificates to the public. Relying parties may or may

not also be subscribers within a given PKI.

* Other participants, such as certificate manufacturing authorities, providers of repository services, and other entities providing PKI-related services.

4.1.4 Certificate usage

This subcomponent contains:

* A list or the types of applications for which the issued certificates are suitable, such as electronic mail, retail transactions, contracts, and a travel order, and/or

* A list or the types of applications for which use of the issued certificates is prohibited.

In the case of a CP or CPS describing different levels of assurance, this subcomponent can describe applications or types of applications that are appropriate or inappropriate for the different levels of assurance.

4.1.5 Policy Administration

This subcomponent includes the name and mailing address of the organization that is responsible for the drafting, registering, maintaining, and updating of this CP or CPS. It also includes the name, electronic mail address, telephone number, and fax number of a contact person. As an alternative to naming an actual person, the document may name a title or role, an e-mail alias, and other generalized contact information. In some cases, the organization may state that its contact person, alone or in combination with others, is available to answer questions about the document.

Moreover, when a formal or informal policy authority is responsible for determining whether a CA should be allowed to operate within or interoperate with a PKI, it may wish to approve the CPS of the CA as being suitable for the policy authority's CP. If so, this subcomponent can include the name or title, electronic mail address (or alias), telephone number, fax number, and other generalized information of the entity in charge of making such a determination. Finally, in this case, this subcomponent also includes the procedures by which this determination is made.

4.1.6 Definitions and acronyms

This subcomponent contains a list of definitions for defined terms used within the document, as well as a list of acronyms in the

document and their meanings.

4.2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

This component contains any applicable provisions regarding:
* An identification of the entity or entities that operate repositories within the PKI, such as a CA, certificate manufacturing authority, or independent repository service provider;

*The responsibility of a PKI participant to publish information regarding its practices, certificates, and the current status of such certificates, which may include the responsibilities of making the CP or CPS publicly available using various mechanisms and of

identifying components, subcomponents, and elements of such documents that exist but are not made publicly available, for instance, security controls, clearance procedures, or trade secret information due to their sensitivity;

* When information must be published and the frequency of publication; and

* Access control on published information objects including CPs, CPS, certificates, certificate status, and CRLs.

4.3 IDENTIFICATION AND AUTHENTICATION

This component describes the procedures used to authenticate the identity and/or other attributes of an end-user certificate applicant to a CA or RA prior to certificate issuance. In addition, the component sets forth the procedures for authenticating the identity and the criteria for accepting applicants of entities seeking to become CAs, RAs, or other entities operating in or interoperating with a PKI. It also describes how parties requesting re-key or revocation are authenticated. This component also addresses naming practices, including the recognition of trademark rights in certain names.

4.3.1 Naming

This subcomponent includes the following elements regarding naming and identification of the subscribers:

* Types of names assigned to the subject, such as X.500 distinguished names; RFC-822 names; and X.400 names;

* Whether names have to be meaningful or not;(3)

* Whether or not subscribers can be anonymous or pseudonymous, and, if they can, what names are assigned to or can be used by anonymous subscribers;

* Rules for interpreting various name forms, such as the X.500 standard and RFC-822;

* Whether names have to be unique; and

* Recognition, authentication, and role of trademarks.

4.3.2 Initial Identity Validation

This subcomponent contains the following elements for the identification and authentication procedures for the initial registration for each subject type (CA, RA, subscriber, or other participant):

* If and how the subject must prove possession of the companion private key for the public key being registered, for example, a digital signature in the certificate request message;(4)

---

* Identification and authentication requirements for organizational identity of subscriber or participant (CA; RA; subscriber (in the case of certificates issued to organizations or devices controlled by an organization), or other participant), for example, consulting the database of a service that identifies organizations or inspecting an organization's articles of incorporation;

* Identification and authentication requirements for an individual subscriber or a person acting on behalf of an organizational subscriber or participant (CA, RA, in the case of certificates issued to organizations or devices controlled by an organization, the subscriber, or other participant),(5) including:

* Type of documentation and/or number of identification credentials required;
* How a CA or RA authenticates the identity of the organization or individual based on the documentation or credentials provided;
* If the individual must present personally to the authenticating CA or RA;
* How an individual as an organizational person is authenticated, such as by reference to duly signed authorization documents or a corporate identification badge.

* List of subscriber information that is not verified (called "non-verified subscriber information") during the initial registration;

* Validation of authority involves a determination of whether a person has specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a certificate; and

* In the case of applications by a CA wishing to operate within, or interoperate with, a PKI, this subcomponent contains the criteria by which a PKI, CA, or policy authority determines whether or not the CA is suitable for such operations or interoperation. Such interoperation may include cross-certification, unilateral certification, or other forms of interoperation.

4.3.3 Identification and Authentication for Re-key Requests

This subcomponent addresses the following elements for the identification and authentication procedures for re-key for each subject type (CA, RA, subscriber, and other participants):

* Identification and authentication requirements for routine re-key, such as a re-key request that contains the new key and is signed using the current valid key; and

* Identification and authentication requirements for re-key after certificate revocation. One example is the use of the same process as the initial identity validation.

4.3.4 Identification and Authentication for Revocation Requests

---

This subcomponent describes the identification and authentication procedures for a revocation request by each subject type (CA, RA, subscriber, and other participant). Examples include a revocation request digitally signed with the private key whose companion public key needs to be revoked and a digitally signed request by the RA.

4.4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

This component is used to specify requirements imposed upon issuing CA, subject CAs, RAs, subscribers, or other participants with respect to the life-cycle of certificate.

Within each subcomponent, separate consideration may need to be given to subject CAs, RAs, subscribers, and other participants.

4.4.1 Certificate Application

This subcomponent is used to address the following requirements regarding subject certificate application:

* Who can submit a certificate application, such as a certificate subject or the RA; and

* Enrollment process used by subjects to submit certificate applications and responsibilities in connection with this process. An example of this process is where the subject generates the key pair and sends a certificate request to the RA. The RA validates and signs the request and sends it to the CA. A CA or RA may have the responsibility to establish an enrollment process in order to receive certificate applications. Likewise, certificate applicants may have the responsibility to provide accurate information on their certificate applications.

4.4.2 Certificate Application Processing

This subcomponent is used to describe the procedure for processing certificate applications. For example, the issuing CA and RA may perform identification and authentication procedures to validate the certificate application. Following such steps, the CA or RA will either approve or reject the certificate application, perhaps upon the application of certain criteria. Finally, this subcomponent sets for the time in which a CA and/or RA must act on and process a certificate application.

4.4.3 Certificate Issuance

This subcomponent is used to describe the following certificate issuance related elements:

* Actions performed by the CA during the issuance of the certificate, for example a procedure whereby the CA validates the RA signature and RA authority and generates a certificate; and

* Notification mechanisms, if any, used by the CA to notify the subscriber of the issuance of the certificate; an example is a procedure under which the CA e-mails the certificate to the subscriber or the RA or e-mails information permitting the subscriber to download the certificate from a web site.

4.4.4 Certificate Acceptance

This subcomponent addresses the following:

* The conduct of an applicant that will be deemed to constitute acceptance of the certificate. Such conduct may include affirmative steps to indicate acceptance, actions implying acceptance, or a failure to object to the certificate or its content. For instance, acceptance may be deemed to occur if the CA does not receive any notice from the subscriber within a certain time period; a subscriber may send a signed message accepting the certificate; or a subscriber may send a signed message rejecting the certificate where the message includes the reason for rejection and identifies the fields in the certificate that are incorrect or incomplete.

* Publication of the certificate by the CA. For example, the CA may post the certificate to an X.500 or LDAP repository.

* Notification of certificate issuance by the CA to other entities. As an example, the CA may send the certificate to the RA.

4.4.5 Key Pair and Certificate Usage

This subcomponent is used to describe the responsibilities relating to the use of keys and certificates, including:

* Subscriber responsibilities relating to use of the subscriber's private key and certificate. For example, the subscriber may be required to use a private key and certificate only for appropriate applications as set forth in the CP and consistent with applicable certificate content (e.g., key usage field), use of a private key and certificate are subject to the terms of the subscriber agreement, the use of a private key is permitted only after the subscriber has accepted the corresponding certificate, or subscriber must discontinue use of the private key following expiration or revocation of the certificate.

* Relying party responsibilities relating to the use of a subscriber's public key and certificate. For instance, a relying party may be obligated to rely on certificates only for appropriate applications as set forth in the CP and consistent with applicable certificate content (e.g., key usage field), successfully perform public key operations as a condition of relying on a certificate, responsibility to check the status of certificate using one of the required or permitted mechanisms set forth in the CP/CPS (see Section 4.4.9 below), and assent to the terms of the applicable relying party agreement as a condition of relying on the certificate.

4.4.6 Certificate Renewal

This subcomponent is used to describe the following elements related to certificate renewal. Certificate renewal means issuance of a new certificate to the subscriber without changing the subscriber or other participant's public key or any other information in the certificate:

* Circumstances under which certificate renewal takes place, such as where the certificate life has expired, but the policy permits the same key pair to be reused;

* Who may request certificate renewal, for instance, the subscriber, RA, or the CA may automatically renew an end-user subscriber certificate;

* A CA or RA's procedures to process renewal requests to issue the new certificate, for example, the use of a token, such as a password, to re-authenticate the subscriber, or procedures that are the same as the initial certificate issuance;

* Notification of the new certificate to the subscriber;

* Conduct constituting acceptance of the certificate;

* Publication of the certificate by the CA; and

* Notification of certificate issuance by the CA to other entities.

4.4.7 Certificate Re-key

This subcomponent is used to describe the following elements related to a subscriber or other participant generating a new key pair and applying for the issuance of new certificate that certifies the new public key:

* Circumstances under which certificate re-key can or must take place, such as after a certificate is revoked for the reasons of key compromise or after a certificate has expired and the usage period of the key pair has also expired;

* Who may request certificate re-key, for example, the subscriber;

* A CA or RA's procedures to process re-keying requests to issue the new certificate, such as procedures that are the same as the initial certificate issuance;

* Notification of the new certificate to the subscriber;

* Conduct constituting acceptance of the certificate;

* Publication of the certificate by the CA; and

* Notification of certificate issuance by the CA to other entities.

4.4.8 Certificate Modification

This subcomponent is used to describe the following elements related to issuance of a new certificate (6) due to changes in the information in the certificate other than the subscriber public key:

* Circumstances under which certificate modification can take place, such as name change, role change, reorganization resulting a change in the DN;

* Who may request certificate modification, for instance, subscribers, human resources personnel, or the RA;

* A CA or RA's procedures to process modification requests to issue the new certificate, such as procedures that are the same as the initial certificate issuance;

* Notification of the new certificate to the subscriber;

* Conduct constituting acceptance of the certificate;

* Publication of the certificate by the CA; and

* Notification of certificate issuance by the CA to other entities.

4.4.9 Certificate Revocation and Suspension

This subcomponent addresses the following:

* Circumstances under which a certificate may be and circumstances under which it must be revoked, for instance, in cases of subscriber employment termination, loss of cryptographic token, or suspected compromise of the private key;

* Who can request the revocation of the participant's certificate, for example, the subscriber, RA, or CA in the case of an end-user subscriber certificate.

* Procedures used for certificate revocation request, such as a digitally signed message from the RA, a digitally signed message from the subscriber, or a phone call from the RA;

* The grace period available to the subscriber, within which the subscriber must make a revocation request;

* The time within which CA must process the revocation request;

* The mechanisms, if any, that a relying party may use or must use in order to check the status of certificates on which they wish to rely;

---

* If a CRL mechanism is used, the issuance frequency;

* If a CRL mechanism is used, maximum latency between the generation of CRLs and posting of the CRLs to the repository (in other words, the maximum amount of processing- and communication-related delays in posting CRLs to the repository after the CRLs are generated);

* On-line revocation/status checking availability, for instance, OCSP and a web site to which status inquiries can be submitted;

* Requirements on relying parties to perform on-line revocation/status checks;

* Other forms of revocation advertisements available;

* Any variations on the above stipulations when the suspension or revocation is the result of private key compromise (as opposed to other reasons for suspension or revocation).

* Circumstances under which a certificate may be suspended;

* Who can request the suspension of a certificate, for example, the subscriber, human resources personnel, a supervisor of the subscriber, or the RA in the case of an end-user subscriber certificate;

* Procedures to request certificate suspension, such as a digitally signed message from subscriber or RA, or a phone call from RA; and

* How long the suspension may last.

4.4.10 Certificate Status Services

This subcomponent addresses the certificate status checking services available to the relying parties, including:

* The operational characteristics of certificate status checking services;

* The availability of such services, and any applicable policies on unavailability; and

* Any optional features of such services.

4.4.11 End of Subscription

This subcomponent addresses procedures used by the subscriber to end subscription to the CA services, including:

* The revocation of certificates at the end of subscription (which may differ, depending on whether the end of subscription was due to expiration of the certificate or termination of the service).

4.4.12 Key Escrow and Recovery

This subcomponent contains the following elements to identify the policies and practices relating to the escrowing, and/or recovery of private keys where private key escrow services are available (through the CA or other trusted third parties):

* Identification of the document containing private key escrow and recovery policies and practices or a listing of the such policies and practices; and

* Identification of the document containing session key encapsulation and recovery policies and practices or a listing of such policies and practices.

4.5 MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

This component describes non-technical security controls (that is, physical, procedural, and personnel controls) used by the issuing CA to perform securely the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival.

This component can also be used to define non-technical security controls on repository, subject CAs, RAs, subscribers, and other participants. The non-technical security controls for the subject CAs, RAs, subscribers, and other participants could be the same, similar, or very different.

These non-technical security controls are critical to trusting the certificates since lack of security may compromise CA operations resulting, for example, in the creation of certificates or CRLs with erroneous information or in the compromise of the CA private key.

Within each subcomponent, separate consideration will, in general, need to be given to each entity type, that is, issuing CA, repository, subject CAs, RAs, subscribers, and other participants.

4.5.1 Physical Security Controls

In this subcomponent, the physical controls on the facility housing the entity systems are described. Topics addressed may include:

* Site location and construction, such as the construction requirements for high-security zones and the use of locked rooms, cages, safes, and cabinets;

* Physical access, i.e., mechanisms to control access from one area of the facility to another or access into high-security zones, such as locating CA operations in a secure computer room monitored by guards or security alarms and requiring movement from zone to zone to be accomplished using a token, biometric readers, and/or access control lists;

* Power and air conditioning;

---

* Water exposures;

* Fire prevention and protection;

* Media storage, for example, requiring the storage of backup media in a separate location that is physically secure and protected from fire and water damages;

* Waste disposal; and

* Off-site backup.

4.5.2 Procedural Controls

In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role. Examples of trusted roles include system administrators, security officers, and system auditors.

For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule). Identification and authentication requirements for each role may also be defined.

This components also includes the separation of duties in terms of the roles that cannot be performed by the same individuals.

4.5.3 Personnel Security Controls

This subcomponent addresses the following:

* Qualifications, experience, and clearances that personnel must have as a condition of filling trusted roles or other important roles. Examples include credentials, job experiences, and official government clearances that candidates for these positions must have before being hired;

* Background checks and clearance procedures that are required in connection with the hiring of personnel filling trusted roles or perhaps other important roles, such as requirements that trusted personnel undergo checks of their criminal records, references, and additional clearances that a participant undertakes after a decision has been made to hire a particular person;

* Training requirements and training procedures for each role following the hiring of personnel;

* Any retraining period and retraining procedures for each role after completion of initial training;

* Frequency and sequence for job rotation among various roles;

* Sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of entity

---

systems for the purpose of imposing accountability on a participant's personnel;

* Controls on personnel that are independent contractors rather than employees of the entity; examples include:

- Bonding requirements on contract personnel;
- Contractual requirements including indemnification for damages due to the actions of the contractor personnel;
- Audit and monitoring of contractor personnel; and
- Other controls on contracting personnel.

* Documentation to be supplied to personnel, during initial training, retraining, or otherwise.

4.5.4 Audit Logging Procedures

This subcomponent is used to describe event logging and audit systems, implemented for the purpose of maintaining a secure environment. Elements include the following:

* Types of events recorded, such as certificate lifecycle operations, attempts to access the system, and requests made to the system;

* Frequency with which audit logs are processed or archived, for example, weekly, following an alarm or anomalous event, or when ever the audit log is n% full;

* Period for which audit logs are kept;

* Protection of audit logs:

- Who can view audit logs, for example only the audit administrator;
- Protection against modification of audit log, for instance a requirement that no one may modify or delete the audit records or that only an audit administrator may delete the audit file as part of rotating the audit file; and
- Protection against deletion of audit log.

* Audit log back up procedures;

* Whether the audit log accumulation system is internal or external to the entity;

* Whether the subject who caused an audit event to occur is notified of the audit action; and

* Vulnerability assessments, for example, where audit data is run through a tool that identifies potential attempts to breach the security of the system.

4.5.5 Records Archival

This subcomponent is used to describe general records archival (or

records retention) policies, including the following:

* Types of records that are archived, for example, all audit data, certificate application information, and documentation supporting certificate applications;

* Retention period for archive;

* Protection of archive:

- Who can view the archive, for example, a requirement that only the audit administrator may view the archive;
- Protection against modification of archive, such as securely storing the data on a write once medium;
- Protection against deletion of archive;
- Protection against deterioration of the media on which the archive is stored, such as a requirement for data to be migrated periodically to fresh media; and
- Protection against obsolescence of hardware, operating systems, and other software, by, for example, retaining as part of the archive the hardware, operating systems, and/or other software in order to permit access to and use of archived records over time.

* Archive backup procedures;

* Requirements for time-stamping of records;

* Whether the archive collection system is internal or external; and

* Procedures to obtain and verify archive information, such as a requirement that two separate copies of the archive data be kept under the control of two persons, and that the two copies be compared in order to ensure that the archive information is accurate.

4.5.6 Key Changeover

This subcomponent describes the procedures to provide a new public key to a CA's users following a re-key by the CA. These procedures may be the same as the procedure for providing the current key. Also, the new key may be certified in a certificate signed using the old key.

4.5.7 Compromise and Disaster Recovery

This subcomponent describes requirements relating to notification and recovery procedures in the event of compromise or disaster. Each of the following may need to be addressed separately:

* Identification or listing of the applicable incident and compromise reporting and handling procedures.

* The recovery procedures used if computing resources, software,

and/or data are corrupted or suspected to be corrupted. These procedures describe how a secure environment is reestablished, which

certificates are revoked, whether the entity key is revoked, how the new entity public key is provided to the users, and how the subjects are re-certified.

* The recovery procedures used if the entity key is compromised. These procedures describe how a secure environment is reestablished, how the new entity public key is provided to the users, and how the subjects are re-certified.

* The entity's capabilities to ensure business continuity following a natural or other disaster. Such capabilities may include the availability of a remote hot-site at which operations may be recovered. They may also include procedures for securing its facility during the period of time following a natural or other disaster and before a secure environment is reestablished either at the original site or at a remote site. For example, procedures to protect against theft of sensitive materials from an earthquake-damaged site.

4.5.8 CA or RA Termination

This subcomponent describes requirements relating to procedures for termination and for termination notification of a CA or RA, including the identity of the custodian of CA and RA archival records.

4.6 TECHNICAL SECURITY CONTROLS

This component is used to define the security measures taken by the issuing CA to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares). This component may also be used to impose constraints on repositories, subject CAs, subscribers, and other participants to protect their private keys, activation data for their private keys, and critical security parameters. Secure key management is critical to ensure that all secret and private keys and activation data are protected and used only by authorized personnel.

This component also describes other technical security controls used by the issuing CA to perform securely the functions of key generation, user authentication, certificate registration, certificate revocation, audit, and archival. Technical controls include life-cycle security controls (including software development environment security, trusted software development methodology) and

operational security controls.

This component can also be used to define other technical security controls on repositories, subject CAs, RAs, subscribers, and other participants.

4.6.1 Key Pair Generation and Installation

Key pair generation and installation need to be considered for the

---

issuing CA, repositories, subject CAs, RAs, and subscribers. For each of these types of entities, the following questions potentially need to be answered:

1. Who generates the entity public, private key pair? Possibilities include the subscriber, RA, or CA. Also, how is the key generation performed? Is the key generation performed in hardware or software?

2. How is the private key provided securely to the entity? Possibilities include a situation where the entity has generated it and therefore already has it, handing the entity the private key physically, mailing a token containing the private key securely, or delivering it in a SSL session.

3. How is the entity's public key provided securely to the certification authority? Some possibilities are in an online SSL session or in a message signed by the RA.

4. In the case of issuing CAs, how is the CA's public key provided securely to potential relying parties? Possibilities include handing the public key to the relying party securely in person, physically mailing a copy securely to the relying party, or delivering it in a SSL session.

5. What are the key sizes? Examples include a 1,024 bit RSA modulus and a 1,024 bit DSA large prime.

6. Who generates the public key parameters, and is the quality of the parameters checked during key generation?

7. For what purposes may the key be used, or for what purposes should usage of the key be restricted? For X.509 certificates, these purposes should map to the key usage flags in X.509 Version 3 certificates.

4.6.2 Private Key Protection and Cryptographic Module Engineering Controls

Requirements for private key protection and cryptographic module need to be considered for the issuing CA, repositories, subject CAs, RAs, and subscribers. For each of these types of entity, the following questions potentially need to be answered:

1. What standards, if any, are required for the cryptographic module used to generate the keys? A cryptographic module can be composed of hardware, software, firmware, or any combination of them. For example, are the keys certified by the infrastructure required to be generated using modules compliant with the US FIPS 140-1? If so, what is the required FIPS 140-1 level of the module? Are there any other engineering or other controls relating to a cryptographic module, such as the identification of the cryptographic module boundary, input/output, roles and services, finite state machine, physical security, software security, operating system security, algorithm compliance, electromagnetic

compatibility, and self tests.

2. Is the private key under n out of m multi-person control?(7) If yes, provide n and m (two person control is a special case of n out of m, where n = m = 2)?

3. Is the private key escrowed?(8) If so, who is the escrow agent, what form is the key escrowed in (examples include plaintext, encrypted, split key), and what are the security controls on the escrow system?

4. Is the private key backed up? If so, who is the backup agent, what form is the key backed up in (examples include plaintext, encrypted, split key), and what are the security controls on the backup system?

5. Is the private key archived? If so, who is the archival agent, what form is the key archived in (examples include plaintext, encrypted, split key), and what are the security controls on the archival system?

6. Under what circumstances, if any, can a private key be transferred into or from a cryptographic module? Who is permitted to perform such a transfer operation? In what form is the private key during the transfer (i.e., plaintext, encrypted, or split key)?

7. How is the private key stored in the module (i.e., plaintext, encrypted, or split key)?

8. Who can activate (use) the private key? What actions must be performed to activate the private key (e.g., login, power on, supply PIN, insert token/key, automatic, etc.)? Once the key is activated, is the key active for an indefinite period, active for one time, or active for a defined time period?

9. Who can deactivate the private key and how? Examples of methods of deactivating private keys include logging out, turning the power off, removing the token/key, automatic deactivation, and time expiration.

10. Who can destroy the private key and how? Examples of methods of destroying private keys include token surrender, token destruction, and overwriting the key.

11. Provide the capabilities of the cryptographic module in the following areas: identification of the cryptographic module boundary, input/output, roles and services, finite state machine, physical security, software security, operating system security, algorithm compliance, electromagnetic compatibility, and self tests. Capability may be expressed through reference to compliance with a standard such as U.S. FIPS 140-1, associated level, and rating.

4.6.3 Other Aspects of Key Pair Management

Other aspects of key management need to be considered for the issuing CA, repositories, subject CAs, RAs, subscribers, and other participants. For each of these types of entity, the following questions potentially need to be answered:

1. Is the public key archived? If so, who is the archival agent and what are the security controls on the archival system? Also, what software and hardware need to be preserved as part of the archive to permit use of the public key over time? Note: this subcomponent is not limited to requiring or describing the use of digital signatures with archival data, but rather can address integrity controls other than digital signatures when an archive requires tamper protection. Digital signatures do not provide tamper protection or protect the integrity of data; they merely verify data integrity. Moreover, the archival period may be greater than the cryptanalysis period for the public key needed to verify any digital signature applied to archival data.

2. What is the operational period of the certificates issued to the subscriber. What are the usage periods, or active lifetimes, for the subscriber's key pair?

4.6.4 Activation Data

Activation data refers to data values other than whole private keys that are required to operate private keys or cryptographic modules containing private keys, such as a PIN, passphrase, or portions of a private key used in a key-splitting scheme. Protection of activation data prevents unauthorized use of the private key, and potentially needs to be considered for the issuing CA, subject CAs, RAs, and subscribers. Such consideration potentially needs to address the entire life-cycle of the activation data from generation through archival and destruction. For each of the entity types (issuing CA, repository, subject CA, RA, subscriber, and other participants) all of the questions listed in 4.6.1 through 4.6.3 potentially need to be answered with respect to activation data rather than with respect to keys.

4.6.5 Computer Security Controls

This subcomponent is used to describe computer security controls such as: use of the trusted computing base concept, discretionary access control, labels, mandatory access controls, object reuse, audit, identification and authentication, trusted path, security testing, and penetration testing. Product assurance may also be addressed.

A computer security rating for computer systems may be required. The rating could be based, for example, on the Trusted System Evaluation Criteria (TCSEC), Canadian Trusted Products Evaluation Criteria, European Information Technology Security Evaluation Criteria (ITSEC), or the Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408:1999. This subcomponent can also

address requirements for product evaluation analysis, testing, profiling, product certification, and/or product accreditation related activity undertaken.

4.6.6 Life Cycle Security Controls

This subcomponent addresses system development controls and security management controls.

System development controls include development environment security, development personnel security, configuration management security during product maintenance, software engineering practices, software development methodology, modularity, layering, use of failsafe design and implementation techniques (e.g., defensive

programming) and development facility security.

Security management controls include execution of tools and procedures to ensure that the operational systems and networks adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.

This subcomponent can also address life-cycle security ratings based, for example, on the Trusted Software Development Methodology (TSDM) level IV and V, independent life-cycle security controls audit, and the Software Engineering Institute's Capability Maturity Model (SEI-CMM).

4.6.7 Network Security Controls

This subcomponent addresses network security related controls, including firewalls.

4.6.8 Time-stamping

This subcomponent addresses requirements or practices relating to the use of timestamps on various data. It may also discuss whether or not the time-stamping application must use a trusted time source.

4.7 CERTIFICATE AND CRL PROFILES

This component is used to specify the certificate format and, if CRLs and/or OCSP are used, the CRL and/or OCSP format. This includes information on profiles, versions, and extensions used.

4.7.1 Certificate Profile

This subcomponent addresses such topics as the following (potentially by reference to a separate profile definition, such as the one defined in IETF PKIX RFC 2459):

* Version number(s) supported;

* Certificate extensions populated and their criticality;

---

* Cryptographic algorithm object identifiers;

* Name forms used for the CA, RA, and subscriber names;

* Name constraints used and the name forms used in the name constraints;

* Applicable CP OID(s);

* Usage of the policy constraints extension;

* Policy qualifiers syntax and semantics; and

* Processing semantics for the critical CP extension.

4.7.2 CRL Profile

This subcomponent addresses such topics as the following (potentially by reference to a separate profile definition, such as the one defined in IETF PKIX RFC 2459):

* Version numbers supported for CRLs; and

* CRL and CRL entry extensions populated and their criticality.

4.7.3 OCSP Profile

This subcomponent addresses such topics as the following (potentially by reference to a separate profile definition, such as the IETF RFC 2560 profile):

* Version of OCSP that is being used as the basis for establishing an OCSP system; and

* OCSP extensions populated and their criticality.

4.8 COMPLIANCE AUDIT AND OTHER ASSESSMENT

This component addresses the following:

* The list of topics covered by the assessment and/or the assessment methodology used to perform the assessment; examples include WebTrust for CAs (9) and SAS 70 (10).

* Frequency of compliance audit or other assessment for each entity that must be assessed pursuant to a CP or CPS, or the circumstances that will trigger an assessment; possibilities include an annual audit, pre-operational assessment as a condition of allowing an entity to being operations, or investigation following a possible or actual compromise of security.

* The identity and/or qualifications of the personnel performing the audit or other assessment.

* The relationship between the assessor and the entity being

assessed, including the degree of independence of the assessor.

* Actions taken as a result of deficiencies found during the assessment; examples include a temporary suspension of operations until deficiencies are corrected, revocation of certificates issued to the assessed entity, changes in personnel, triggering special investigations or more frequent subsequent compliance assessments, and claims for damages against the assessed entity.

* Who is entitled to see results of an assessment (e.g., assessed entity, other participants, the general public), who provides them (e.g., the assessor or the assessed entity), and how they are communicated.

4.9 OTHER BUSINESS AND LEGAL MATTERS

This component covers general business and legal matters. Sections 9.1 and 9.2 of the framework discuss the business issues of fees to be charged for various services and the financial responsibility of participants to maintain resources for ongoing operations and for paying judgments or settlements in response to claims asserted against them. The remaining sections are generally concerned with legal topics.

Starting with Section 9.3 of the framework, the ordering of topics is the same as or similar to the ordering of topics in a typical software licensing agreement or other technology agreement. Consequently, this framework may not only be used for CPs and CPSs, but also associated PKI-related agreements, especially subscriber agreements and relying party agreements. This ordering is intended help lawyers review CPs, CPSs, and other documents adhering to this framework.

With respect to many of the legal subcomponents within this component, a CP or CPS drafter may choose to include in the document terms and conditions that apply directly to subscribers or relying parties. For instance, a CP or CPS may set forth limitations of liability that apply to subscribers and relying parties. The inclusion of terms and conditions is likely to be appropriate where the CP or CPS is itself a contract or part of a contract.

In other cases, however, the CP or CPS is not a contract or part of a contract; instead, it is configured so that its terms and conditions are applied to the parties by separate documents, which may include associated agreements, such as subscriber or relying party agreements. In that event, a CP drafter may write a CP so as to require that certain legal terms and conditions appear (or not appear) in such associated agreements. For example, a CP might include a subcomponent stating that a certain limitation of

liability term must appear in a CA's subscriber and relying party agreements. Another example is a CP that contains a subcomponent prohibiting the use of a subscriber or relying party agreement containing a limitation upon CA liability inconsistent with the provisions of the CP. A CPS drafter may use legal subcomponents to disclose that certain terms and conditions appear in associated

subscriber, relying party, or other agreements in use by the CA. A CPS might explain, for instance, that the CA writing it uses an associated subscriber or relying party agreement that applies a particular provision for limiting liability.

4.9.1 Fees

This subcomponent contains any applicable provisions regarding fees charged by CAs, repositories, or RAs, such as:

* Certificate issuance or renewal fees;

* Certificate access fees;

* Revocation or status information access fees;

* Fees for other services such as providing access to the relevant CP or CPS; and

* Refund policy.

4.9.2 Financial Responsibility

This subcomponent contains requirements or disclosures relating to the resources available to CAs, RAs, and other participants providing certification services to support performance of their operational PKI responsibilities, and to remain solvent and pay damages in the event they are liable to pay a judgment or settlement in connection with a claim arising out of such operations. Such provisions include:

* A statement that the participant maintains a certain amount of insurance coverage for its liabilities to other participants;

* A statement that a participant has access to other resources to support operations and pay damages for potential liability, which may be couched in terms of a minimum level of assets necessary to operate and cover contingencies that might occur within a PKI, where examples include assets on the balance sheet of an organization, a surety bond, a letter of credit, and a right under an agreement

to an indemnity under certain circumstances; and

* A statement that a participant has a program that offers first-party insurance or warranty protection to other participants in connection with their use of the PKI.

4.9.3 Confidentiality of Business Information

This subcomponent contains provisions relating to the treatment of confidential business information that participants may communicate to each other, such as business plans, sales information, trade secrets, and information received from a third party under a nondisclosure agreement. Specifically, this subcomponent addresses:

* The scope of what is considered confidential information,

---

* The types of information that are considered to be outside the scope of confidential information, and

* The responsibilities of participants that receive confidential information to secure it from compromise, and refrain from using it or disclosing it to third parties.

4.9.4 Privacy of Personal Information

This subcomponent relates to the protection that participants, particularly CAs, RAs, and repositories, may be required to afford to personally identifiable private information of certificate applicants, subscribers, and other participants. In specific, this subcomponent addresses the following, to the extent pertinent under applicable law:

* The designation and disclosure of the applicable privacy plan that applies to a participant's activities, if required by applicable law or policy;

* Information that is or is not considered private within the PKI;

* Any responsibility of participants that receive private information to secure it, and refrain from using it and from disclosing it to third parties;

* Any requirements as to notices to, or consent from individuals regarding use or disclosure of private information; and

* Any circumstances under which a participant is entitled or required to disclose private information pursuant to judicial,

administrative process in a private or governmental proceeding, or in any legal proceeding.

4.9.5 Intellectual Property Rights

This subcomponent addresses the intellectual property rights, such as copyright, patent, trademarks, or trade secrets, that certain participants may have or claim in a CP, CPS, certificates, names, and keys, or are the subject of a license to or from participants.

4.9.6 Representations and Warranties

This subcomponent can include representations and warranties of various entities that are being made pursuant to the CP or CPS. For example, a CPS that serves as a contract might contain a CA's warranty that information contained in the certificate is accurate. Alternatively, a CPS might contain a less extensive warranty to the effect that the information in the certificate is true to the best of the CA's knowledge after performing certain identity authentication procedures with due diligence. This subcomponent can also include requirements that representations and warranties appear in certain agreements, such as subscriber or relying party agreements. For instance, a CP may contain a requirement that all

CAs utilize a subscriber agreement, and that a subscriber agreement must contain a warranty by the CA that information in the certificate is accurate. Participants that may make representations and warranties include CAs, RAs, subscribers, relying parties, and other participants.

4.9.7 Disclaimers of Warranties

This subcomponent can include disclaimers of express warranties that may otherwise be deemed to exist in an agreement, and disclaimers of implied warranties that may otherwise be imposed by applicable law, such as warranties of merchantability or fitness for a particular purpose. The CP or CPS may directly impose such disclaimers, or the CP or CPS may contain a requirement that disclaimers appear in associated agreements, such as subscriber or relying party agreements.

4.9.8 Limitations of Liability

This subcomponent can include limitations of liability in a CP or CPS or limitations that appear or must appear in an agreement associated with the CP or CPS, such as a subscriber or relying party agreement. These limitations may fall into one of two categories:

limitations on the elements of damages recoverable and limitations on the amount of damages recoverable, also known as liability caps. Often, contracts contain clauses preventing the recovery of elements of damages such as incidental and consequential damages, and sometimes punitive damages. Frequently, contracts contain clauses that limit the possible recovery of one party or the other to an amount certain or to an amount corresponding to a benchmark, such as the amount a vendor was paid under the contract.

4.9.9 Indemnities

This subcomponent includes provisions by which one party makes a second party whole for losses or damage incurred by the second party, typically arising out of the first party's conduct. They may appear in a CP, CPS, or agreement. For example, a CP may require that subscriber agreements contain a term under which a subscriber is responsible for indemnifying a CA for losses the CA sustains arising out of a subscriber's fraudulent misrepresentations on the certificate application under which the CA issued the subscriber an inaccurate certificate. Similarly, a CPS may say that a CA uses a relying party agreement, under which relying parties are responsible for indemnifying a CA for losses the CA sustains arising out of use of a certificate without properly checking revocation information or use of a certificate for purposes beyond what the CA permits.

4.9.10 Term and Termination

This subcomponent can include the time period in which a CP or a CPS remains in force and the circumstances under which the document, portions of the document, or its applicability to a particular participant can be terminated. In addition or alternatively, the CP or CPS may include requirements that certain term and termination

---

clauses appear in agreements, such as subscriber or relying party agreements. In particular, such terms can include:

* The term of a document or agreement, that is, when the document becomes effective and when it expires if it is not terminated earlier.

* Termination provisions stating circumstances under which the document, certain portions of it, or its application to a particular participant ceases to remain in effect.

* Any consequences of termination of the document. For example, certain provisions of an agreement may survive its termination and

remain in force. Examples include acknowledgements of intellectual property rights and confidentiality provisions. Also, termination may trigger a responsibility of parties to return confidential information to the party that disclosed it.

4.9.11 Individual notices and communications with participants

This subcomponent discusses the way in which one participant can or must communicate with another participant on a one-to-one basis in order for such communications to be legally effective. For example, an RA may wish to inform the CA that it wishes to terminate its agreement with the CA. This subcomponent is different from publication and repository functions, because unlike individual communications described in this subcomponent, publication and posting to a repository are for the purpose of communicating to a wide audience of recipients, such as all relying parties. This subcomponent may establish mechanisms for communication and indicate the contact information to be used to route such communications, such as digitally signed e-mail notices to a specified address, followed by a signed e-mail acknowledgement of receipt.

4.9.12 Amendments

It will occasionally be necessary to amend a CP or CPS. Some of these changes will not materially reduce the assurance that a CP or

its implementation provides, and will be judged by the policy administrator to have an insignificant effect on the acceptability of certificates. Such changes to a CP or CPS need not require a change in the CP OID or the CPS pointer (URL). On the other hand, some changes to a specification will materially change the acceptability of certificates for specific purposes, and these changes may require corresponding changes to the CP OID or CPS pointer qualifier (URL).

This subcomponent may also contain the following information:

* The procedures by which the CP or CPS and/or other documents must, may be, or are amended. In the case of CP or CPS amendments, change procedures may include a notification mechanism to provide notice of proposed amendments to affected parties, such as subscribers and relying parties; a comment period; a mechanism by which comments are

received, reviewed and incorporated into the document; and a mechanism by which amendments become final and effective.

* The circumstances under which amendments to the CP or CPS would

require a change in CP OID or CPS pointer (URL).

4.9.13 Dispute Resolution Procedures

This subcomponent discusses procedures utilized to resolve disputes arising out of the CP, CPS, and/or agreements. Examples of such procedures include requirements that disputes be resolved in a certain forum or by alternative dispute resolution mechanisms.

4.9.14 Governing Law

This subcomponent sets forth a statement that the law of a certain jurisdiction governs the interpretation and enforcement of the subject CP or CPS or agreements.

4.9.15 Compliance with Applicable Law

This subcomponent relates to stated requirements that participants comply with applicable law, for example laws relating to cryptographic hardware and software that may be subject to the export control laws of a given jurisdiction. The CP or CPS could purport to impose such requirements or may require that such provisions appear in other agreements.

4.9.16 Miscellaneous Provisions

This subcomponent contains miscellaneous provisions sometimes called "boilerplate provisions" in contracts. The clauses covered in this subcomponent may appear in a CP, CPS, or agreements and include:

* An entire agreement clause, which typically identifies the document or documents comprising the entire agreement between the parties and states that such agreements supersedes all prior and contemporaneous written or oral understandings relating to the same subject matter;

* An assignment clause, which may act to limit the ability of a party to an agreement to assign its rights under the agreement to another party (such as the right to receive a stream of payments in the future) or the ability of a party to delegate its obligations under the agreement;

* A severability clause, which sets forth the intentions of the parties in the event a court or other tribunal determines that a clause within an agreement is, for some reason, invalid or unenforceable, and whose purpose is frequently to prevent the unenforceability of one clause from causing the whole agreement to be unenforceable; and

* An enforcement clause, which may state that a party prevailing in any dispute arising out of an agreement is entitled to attorneys'

fees as part of its recovery, or may state that a party's waiver of one breach of contract does not constitute a continuing waiver or a future waiver of other breaches of contract.

4.9.17 Other Provisions

This subcomponent is a "catchall" location where additional responsibilities and terms can be imposed on PKI participants that do not neatly fit within one of the other components or subcomponents of the framework. CP and CPS writers can place any provision within this subcomponent that is not covered by another subcomponent.

5. OUTLINE OF A SET OF PROVISIONS

This section contains a recommended outline for a set of provisions, intended to serve as a checklist or (with some further development) a standard template for use by CP or CPS writers. Such a common outline will facilitate:

(a) Comparison of two certificate policies during cross-certification or other forms of interoperation (for the purpose of equivalency mapping).
(b) Comparison of a CPS with a CP to ensure that the CPS faithfully implements the policy.
(c) Comparison of two CPSs.

In order to comply with the RFC, the drafters of a compliant CP or CPS are strongly advised to adhere to this outline. While use of alternate outline is discouraged, it may be accepted if a proper justification is provided for the deviation and a mapping table is provided to readily discern where each of the items described in this outline is provided.

1. INTRODUCTION

1.1 Overview

1.2 Document name and identification

1.3 PKI participants
1.3.1 Certification authorities
1.3.2 Registration authorities
1.3.3 Subscribers
1.3.4 Relying parties
1.3.5 Other participants

---

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS (11)

4.1 Certificate Application
4.1.1 Who can submit a certificate application
4.1.2 Enrollment process and responsibilities

4.2 Certificate application processing
4.2.1 Performing identification and authentication functions
4.2.2 Approval or rejection of certificate applications
4.2.3 Time to process certificate applications

4.3 Certificate issuance
4.3.1 CA actions during certificate issuance
4.3.2 Notification to subscriber by the CA of issuance of certificate

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance
4.4.2 Publication of the certificate by the CA
4.4.3 Notification of certificate issuance by the CA to other entities

4.5 Key pair and certificate usage
4.5.1 Subscriber private key and certificate usage
4.5.2 Relying party public key and certificate usage

4.6 Certificate renewal
4.6.1 Circumstance for certificate renewal
4.6.2 Who may request renewal
4.6.3 Processing certificate renewal requests
4.6.4 Notification of new certificate issuance to subscriber
4.6.5 Conduct constituting acceptance of a renewal certificate
4.6.6 Publication of the renewal certificate by the CA
4.6.7 Notification of certificate issuance by the CA to other entities

4.7 Certificate re-key
4.7.1 Circumstance for certificate re-key
4.7.2 Who may request certification of a new public key
4.7.3 Processing certificate re-keying requests
4.7.4 Notification of new certificate issuance to subscriber
4.7.5 Conduct constituting acceptance of a re-keyed certificate
4.7.6 Publication of the re-keyed certificate by the CA
4.7.7 Notification of certificate issuance by the CA to other entities

---

---

6. ACKNOWLEDGMENTS

The development of the predecessor document (RFC 2527) was supported by the Government of Canada's Policy Management Authority (PMA)

Committee, the National Security Agency, the National Institute of Standards and Technology (NIST), and the American Bar Association Information Security Committee Accreditation Working Group.

This revision effort is largely a result of constant inspiration from Michael Baum. Michael Power, Mike Jenkins, and Alice Sturgeon have also made several contributions.

7. REFERENCES

[ABA1] American Bar Association, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce, 1996.

[ABA2] American Bar Association, PKI Assessment Guidelines, v0.30, Public Draft For Comment, June 2001.

[BAU1] Michael. S. Baum, Federal Certification Authority Liability and Policy, NIST-GCR-94-654, June 1994, available at http://www.verisign.com/repository/pubs/index.html.

[ETS] European Telecommunications Standards Institute, "Policy Requirements for Certification Authorities Issuing Qualified Certificates," ETSI TS 101 456, Version 1.1.1, December 2000.

[GOC] Government of Canada PKI Policy Management Authority, "Digital Signature and Confidentiality Certificate Policies for the Government of Canada Public Key Infrastructure," v.3.02, April 1999.

[IDT] Identrus, LLC, "Identrus Identity Certificate Policy" IP-IPC Version 1.7, March 2001.

[ISO1] ISO/IEC 9594-8/ITU-T Recommendation X.509, "Information Technology - Open Systems Interconnection: The Directory:

Authentication Framework," 1997 edition. (Pending publication of 2000 edition, use 1997 edition.)

[PEM1] S. Kent, "Privacy Enhancement for Internet Electronic Mail, Part II: Certificate-Based Key Management," Internet RFC 1422, 1993.

[PKI1] R. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure, Certificate and CRL Profile," RFC 2459 1998.

[CPF] S. Chokhani and W. Ford, "Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Statement Framework," RFC 2527, April 1998.

8. AUTHORS' ADDRESSES

Santosh Chokhani
CygnaCom Solutions, Inc., an Entrust company
7927 Jones Branch Drive, Suite 100 West
McLean, VA 22102
Phone: (703) 270-3520
Fax: (703) 848-0960
EMail: chokhani@cygnacom.com

Warwick Ford
VeriSign, Inc.
401 Edgewater Place, Suite 280
Wakefield, MA 01880
Phone: (781) 245-6996 x225
Fax: (781) 245-6006
EMail: wford@verisign.com

Randy V. Sabett, J.D., CISSP
Cooley Godward LLP
One Freedom Square, Reston Town Center
11951 Freedom Drive
Reston, VA 20190-5601
Phone: (703) 456-8137
Fax: (703) 456-8100
EMail: rsabett@cooley.com

Charles (Chas) R. Merrill
McCarter & English, LLP
Four Gateway Center
100 Mulberry Street
Newark, New Jersey 07101-0652
Phone: (973) 622-4444
Fax: (973) 624-7070
EMail: cmerrill@concentric.net

Stephen S. Wu
Infoliance, Inc.
101 First St. # 725
Los Altos, CA 94022
Phone: (650) 917-8045
Fax: (650) 618-1454
EMail: swu@infoliance.com

NOTES

1 A paper copy of the ABA Digital Signature Guidelines can be purchased from the ABA. See http://www.abanet.com for ordering details. The DSG may also be downloaded without charge from the ABA website at http://www.abanet.org/scitech/ec/isc/digital_signature.html.

2 A draft of the PKI Assessment Guidelines may be downloaded without charge from the ABA website at http://www.abanet.org/scitech/ec/isc/pag/pag.html.

---

3 The term "meaningful" means that the name form has commonly understood semantics to determine identity of the person and/or organization. Directory names and RFC 822 names may be more or less meaningful.

4 The subject may not need to prove to the CA that the subject has possession of the private key corresponding to the public key being registered if the CA generates the subject's key pair on the subject's behalf.

5 Examples of means to identify and authenticate individuals include biometric means (such as thumb print, ten finger print, and scan of the face, palm, or retina), a driver's license, a credit card, a company badge, and a government badge.

6 Certificate "modification" does not refer to making a change to an existing certificate, since this would prevent the verification of any digital signatures on the certificate and cause the certificate

to be invalid. Rather, the concept of "modification" refers to a situation where the information referred to in the certificate has changed or should be changed, and the CA issues a new certificate containing the modified information. One example is a subscriber that changes his or her name, which would necessitate the issuance of a new certificate containing the new name.

7 The n out of m rule allows a private key to be split in m parts. The m parts may be given to m different individuals. Any n parts out of the m parts may be used to fully reconstitute the private key, but having any n-1 parts provides one with no information about the private key.

8 A private key may be escrowed, backed up, or archived. Each of these functions has a different purpose. Thus, a private key may go through any subset of these functions depending on the requirements. The purpose of escrow is to allow a third party (such as an organization or government) to obtain the private key without the cooperation of the subscriber. The purpose of back up is to allow the subscriber to reconstitute the key in case of the destruction or corruption of the key for business continuity purposes. The purpose of archive is to provide for reuse of the private key in future, e.g., use to decrypt a document.

9 WebTrust refers to the "WebTrust Program for Certification Authorities," from the American Institute of Certified Public Accountants, Inc., and the Canadian Institute of Chartered Accountants.

10 See <http://www.aicpa.org>.

11 All or some of the following items may be different for the various types of entities, i.e., CA, RA, and end entities.

LIST OF ACRONYMS
ABA - American Bar Association
CA - Certification Authority

CPS - Certification Practice Statement
CRL - Certificate Revocation List
DAM - Draft Amendment
FIPS - Federal Information Processing Standard
I&A - Identification and Authentication
IEC - International Electrotechnical Commission
IETF - Internet Engineering Task Force
IP - Internet Protocol
ISO - International Organization for Standardization

ITU - International Telecommunications Union
NIST - National Institute of Standards and Technology
OID - Object Identifier
PIN - Personal Identification Number
PKI - Public Key Infrastructure
PKIX - Public Key Infrastructure (X.509) (IETF Working Group)
RA - Registration Authority
RFC - Request For Comment
URL - Uniform Resource Locator
US - United States

< draft-ietf-pkix-ipki-new-rfc2527-01.txt >

Expires in six months from January 3, 2002