PKIX Working Group S. Chokhani (CygnaCom Solutions, Inc.)
Internet Draft W. Ford (VeriSign, Inc.)

expires in six months June 1997

Certificate Policy and Certification Practice Statement Framework

<draft-chokhani-cps-00.txt>

Status of this Memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of 6 months and may be updated, replaced, or may become obsolete by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as work in progress.

To learn the current status of any Internet-Draft, please check the 1id-abstracts.txt listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za(Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

Abstract

This document presents an initial draft of a framework to assist the writers of X.509 certificate policies or certification practice statements for certification authorities and public key infrastructures. In particular, the framework identifies a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in an X.509 certificate policy or a certification practice statement.

1. INTRODUCTION

1.1 BACKGROUND

An X.509 public key certificate (henceforth termed a certificate) binds an entity to the entity's public key. The degree to which a certificate user (a certificate user is typically a signature verifier or a key token generator) can trust this binding depends on several factors. These factors include the Certification Authority (CA) policy and procedures for authentication of end entities, CA operating policy, procedures and security controls,

end entity policy and procedures for handling private keys, etc. The liability assumed by certificate issuers and end entities also plays a role in the degree of trust.

Version 3 X.509 certificates may contain certificate policies [8]. A certificate policy allows the users of a certificate to decide how much trust to place in the certificate, i.e., in the binding of the entity's identity and the entity's public key. According to X.509, version 3, a certificate policy is "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."

A detailed description of how certificate policies are implemented by a particular CA is called a Certification Practice Statement (CPS). According to the American Bar Association (ABA), "a CPS is a statement of the practices which a certification authority employs in issuing certificates." When negotiating a cross certification, CAs examine and compare each other's CPS.

1.2 PURPOSE

The purpose of this document is to present a framework that identifies the elements that may need to be considered in formulating a certificate policy or a CPS, to assist the writers of certificate policies or CPSs with their task. The purpose is not to define particular certificate policies or CPSs per se.

1.3 SCOPE

There are many classes of policies, such as organization security policy, system security policy, data labeling policy, etc. The scope of this document is limited to defining the aspects and elements of a certificate policy (as described and intended in the X.509, version 3 certificate standard and ABA digital signature guidelines). While the certificate policy and certification practices statement framework presented here was motivated by the X.509 version 3 certificate standard, the framework can be used by other public key certificate standards.

This document does not define a specific certificate policy or CPS. Instead, it describes what types of information should be included in a certificate policy (and documented in a CPS). This document does not provide specific values or specific mechanisms to choose those values. Specific security policy and the mechanisms that implement them are the scope of a detailed document, a CPS.

This document's scope is limited to provide a comprehensive framework. It does not contain any guidance on how to write sound certificate policies or CPS.

This certificate policy and CPS framework contains many topics. It is not necessary for a policy or a CPS to define something concrete for each topic. A tangible statement, "none", and "not applicable" are all acceptable values. Addressing each and every topic ensures that the policy and CPS writers have not omitted anything. Addressing each and every topic in the defined sequence also facilitates comparison of policies and certification practice statements for the purpose of equivalency mapping (as described in Section 3).

1.4 AUDIENCE

The audience for this document are the designers and policy-makers of certificate infrastructures using version 3 X.509 certificates.

1.5 DOCUMENT ORGANIZATION

This document contains seven main sections. This section has provided an introduction. Section 2 contains definitions of key terms used in this document. Section 3 further explains certificate policy and CPS related terms and Section 4 provides a list of references and related work. Section 5 provides an overview of the certificate policy and certification practices framework. Section 6 contains the details of the certificate policy and CPS framework. Section 7 provides an outline format for a certificate policy and certification practice statement.

2. DEFINITIONS

In this section, we define terms used in the development of certificate policy and CPS. These terms are closely related, but have subtle differences. The definitions are intended to clarify those subtle differences.

Certificate Policy - 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 certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range. The certificate policy should be used by the user of the certificate to decide whether or not to accept the binding between the subject (of the certificate) and the

public key. A subset of the components in the certificate policy and certification practices statement framework are given concrete values to define a certificate policy. The certificate policy is represented by a registered object identifier in the X.509, version 3 certificate. The object owner also registers a textual description of the policy and makes it available to the certificate users.

The certificate policy object identifier can be included in the following extensions in the X.509, version 3 certificates: certificate policies, policy mappings, and policy constraints. The object identifier(s) may appear in none, some, or all of these fields. These object identifiers may be the same (referring to the same certificate policy) or may be different (referring to different certificate policies).

Element of Policy - A topic that may need to be covered in a certificate policy or in a certification practice statement.

Certification Path - A set of certificates that provides a chain of trust from the relying party's trusted CA to the entity whose public key is required by the relying party.

Certificate Policy and Certificate Practice Statement (CPS) Framework - A comprehensive set of security and liability related components that can be used to define a certificate policy or a CPS. A subset of the components in the certificate policy and CPS framework are given concrete values to define a certificate policy or a CPS.

Certification Practice Statement (CPS) - A statement of the practices which a certification authority employs in issuing certificates.

Issuing Certification Authority (CA) - A CA who has elected to apply a policy to itself and its subjects (CA and end entities).

Policy Qualifier - Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

Registration Authority (RA) - An entity who is responsible for identification and authentication of subjects of certificate, but is not a CA, and hence does not sign or issue certificates.

Subject CA - A CA that is certified by the issuing CA and hence complies with the certificate policy of the issuing CA.

Subject RA - See Registration Authority (RA).

3. CERTIFICATE POLICY AND CPS RELATED CONCEPTS

This section contains a detailed explanation of a certificate policy and a certification practice statement.

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 a particular entity (the certificate subject). But to what extent can the certificate user rely on that statement by the certification authority? Different certificates are issued following different practices and procedures, and may be suitable for different applications and/or purposes.

The term certificate policy derives from the X.509 standard [8]. Certificate policy refers to the way an X.509 certificate indicates to a certificate user whether or not the certificate is suitable for use for a particular application. A certificate policy needs to be recognized by both the issuer and user of the certificate. Any individual certificate will typically be associated with a single certificate policy or, possibly, be issued consistent with a small number of different policies.

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

A certificate policy is registered and assigned a globally unique ISO/IEC/ITU object identifier (OID). This registration process follows the procedures specified in ISO/IEC/ITU standards.

3.2 CERTIFICATE POLICY EXAMPLES

An organization can be expected to support a number of different certificate policies. For example, a certain organization might support two different certificate policies. One might govern how certificates are issued for confidentiality (encryption) applications, while the second might deal with how certificates are issued for non-repudiation (digital signature) applications.

For the purposes of this example, call this organization ACME research, and call the two policies the ACME Electronic Mail policy, and the ACME Purchase policy. The ACME Electronic Mail policy is used by the ACME employees for protecting routine information (e.g., causal electronic mail) and for authenticating

connections from the World Wide Web browsers to the corporate Web servers. The Certified key pairs may be generated, stored, and managed using low-cost software-based systems. Under this policy, a certificate is automatically issued to anybody identified in the corporate directory who submits a signed certificate request form to a network administrator.

The ACME Purchase policy is used to protect financial transactions. Under this policy, ACME requires that certified key pairs be generated and stored in approved cryptographic hardware tokens. A certificate and token is provided to employees with disbursement authority. These authorized individual are required to present themselves to a special security office, and show a valid identification badge before a token is issued.

3.3 X.509 CERTIFICATE FIELDS RELATING TO CERTIFICATE POLICIES

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

* Certificate Policies extension
* Policy Mappings extension
* Policy Constraints extension

3.3.1 Certificate Policies Extension

The Certificate Policies extension has two variants - one with the field flagged non-critical and one with the field flagged critical. The purpose of the field is slightly different in the two cases.

Each Certificate Policy may define one or more purposes for which certificates issued on the policy may be used. A non-critical Certificate Policies field lists certificate policies that the certification authority declares are applicable, however, use of the certificate is not restricted to the purposes indicated by the applicable policies. Using the example of the "Electronic Mail" and the "Purchase" policies defined in Section 3.2 above, the certificates issued to the organization's regular employees will contain the object identifier for certificate policy for the Electronic Mail policy. The certificates issued to the employees with disbursement authority will contain the object identifiers for both the Electronic Mail policy and the Purchase policy. The Certificate Policies field may also optionally convey qualifier values for each identified policy; use of qualifiers is discussed below in Section 3.4.

The non-critical Certificate Policies field is designed to be used by applications as follows. Each application is pre-configured to know what policy it requires. Using the example in Section 3.2, electronic mail applications and Web servers will be configured to require the Electronic Mail policy. The corporate financial applications will be configured to require the Purchase policy for validating financial transactions.

When processing a certification path, a certificate policy that is acceptable to the certificate-using application must be present in every certificate in the path, i.e., in certification authority 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. 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 not be used for any purpose other than those identified by the certificate policies. This field is intended, first and foremost, to protect the certification authority against damage claims by some party who has used the certificate for a purpose not defined in the applicable policies.

For example, the government might issue certificates to taxpayers for the purpose of protecting tax filings. The government understands and can accommodate the risks of accidentally issuing a bad certificate, e.g., to a wrongly-authenticated person. However, suppose someone used a government tax-filing certificate as the basis for encrypting multi-million-dollar-value proprietary secrets which subsequently fell into the wrong hands because of an error in issuing the government certificate. Would it not be possible for the damaged party to sue the government for issuing a bad certificate? It is this type of situation that the critical-flagged Certificate Policies extension is intended to avert. To provide protection against this type of situation, the extension field should always be set critical in a certificate, i.e., any application using the certificate must use the certificate only for the purpose(s) defined by the policies in the field.

3.3.2 Policy Mapping Extension

The next policy related extension field is the Policy Mappings extension. This extension may only be used in CA-certificates, i.e., certificates for certification authorities issued by other certification authorities. 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 the ACE Corporation establishes an agreement with the ABC Corporation to cross-certify each others' public-key infrastructures for the purposes of mutually protecting electronic data interchange. 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 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. Another solution, which is much 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).

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 explicit certificate policy to be present in all subsequent certificates in a certification path. Certificates at the start of a certification path may be considered by a certificate user to be part of a trusted domain, i.e., certification authorities are trusted for all purposes so no particular certificate policy is needed in the Certificate Policies extension. Whenever a certification authority in the trusted domain certifies outside the domain, it should activate the requirement for explicit policy in subsequent certificates.

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. Unless special requirements arise, it would be prudent to always disable policy mapping when certifying outside the domain. This will eliminate the increase in security risk due to transitive trust. i.e., a domain A trusts domain B, domain B trusts domain C, and hence domain A trusts domain C even though domain A does not wish to trust any other domain except domain B.

3.4 POLICY QUALIFIERS

The Certificate Policies extension field has a provision for conveying, along with each certificate policy 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.

In practice, policy qualifiers will not be particularly useful unless agreement is reached, outside the standard, on the purposes for which they will be used and on the syntax for representing them. A collection of common qualifier types will likely emerge.

Some important purposes currently envisaged for qualifiers are:

a. for providing a solid link back to a location from which a copy of the full certification practice statement (see next section) can be retrieved; the qualifier will convey a World Wide Web URL and a digest field to enable a user to check that the document has been retrieved uncorrupted; and

b. for conveying textual information comprising appropriate legal text, e.g., disclaimer of limitation of liability, for display to certificate users whenever certificates are used.

It is anticipated that the IETF PKIX Working Group will standardize these qualifier types.

3.5 CERTIFICATION PRACTICE STATEMENT

The term certification practice statement derives from the American Bar Association (ABA) Digital Signature Guidelines [10]. (E1) A certification practice statement is defined to be:

A statement of the practices which a certification authority employs in issuing certificates.

In the 1995 draft of the ABA guidelines, 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, or it may be a statute or regulation applicable to the certification authority and covering similar subject matter. It may also be part of the contract between the certification authority and the subscriber. A certification practice statement may also be comprised of multiple documents, a combination of public law, private contract, and/or declaration.
>
> Certain forms for legally implementing certification practice statements lend themselves to particular relationships. For example, when the legal relationship between a certification authority and subscriber is consensual, a contract would ordinarily be the means of giving effect to a certification practice statement. The certification authority's duties to a relying person are generally based on the certification authority's representations, which may include a certification practice statement.
>
> Whether a certification practice statement is binding on a relying person depends on whether the relying person has knowledge or notice of the certification practice statement. A relying person has knowledge or at least notice of the contents of the certificate used by the relying person to verify a digital signature, including documents incorporated into the certificate by reference. It is therefore advisable to incorporate a certification practice statement into a certificate by reference.
>
> > NOTE: When the legal relationship is regulatory, for example, between a government and its citizens, a statute may be the means of giving effect to a certification practice statement.
>
> As much as possible, a certification practice statement should indicate any of the widely recognized standards to which the certification authority's practices conform. Reference to widely recognized standards may indicate concisely the suitability of the certification authority's practices for another person's purposes, as well as the potential technological compatibility of the certificates issued by the certification authority with repositories and other systems.

3.6 RELATIONSHIP BETWEEN CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT

The concepts of certificate policy and certification practice statement come from different sources and were developed for different reasons. However, they are interrelated. This section describes the relationship between the two.

A certification practice statement is a detailed statement by a certification authority as to its practices, that potentially needs to be understood and consulted by subscribers and certificate users (relying parties). A certificate policy is a mutually understood indicator from certification authority to certificate user as to suitable applications and purposes for a particular certificate. A certification authority with a single certification practice statement may support multiple certificate policies (used by different certificate user communities). Also, multiple different certification authorities, with non-identical certification practice statements, may support the same certificate policy.

For example, the Government of Canada might define a government-wide certificate policy for handling confidential human resources information. The certificate policy definition will be a broad statement of the general characteristics of that certificate policy, and an indication of the types of applications for which it is suitable for use. Different departments or agencies that operate certification authorities with different certification practice statements might support this certificate policy. At the same time, such certification authorities may support other certificate policies.

In addition to populating the certificate policies field with the certificate policy 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 certificate policy qualifier, is described in Section 3.4.

3.7 CA DISCLOSURE RECORD

A CA Disclosure Record [9] is a body of textual information, intended to convey information about a particular certification authority that may be of some help to a certificate user in evaluating the suitability of a certificate issued by that certification authority.

The following excerpt from the Utah Administrative Code has the following recommendations for the contents of a certification

authority disclosure record:

1. an indication that the certification authority disclosure record is provided and maintained by this state;

2. the name, street address, and voice telephone number of the certification authority;

3. the telephone number of the certification authority's facsimile transmission machine, if the certification authority has such a machine;

4. the electronic mail or other address by which the certification authority may be contacted electronically;

5. the distinguished name of the certification authority;

6. the current public key or keys of the certification authority by which its digital signatures on published certificates may be verified;

7. the restrictions, if any, placed on the certification authorities license pursuant to section 201(3);

8. if the certification authority's license has been revoked or is currently suspended, the data of revocation or suspension and the grounds for revocation or suspension;

9. the amount of the certification authority's suitable guaranty;

10. the total amount of all claims filed with the division for payment from the suitable guaranty filed by the certification authority;

11. a brief description of any limit known to the division and applicable to the certification authority's liability or legal capacity to pay damages in tort or for breach of a duty prescribed in this document; unless the limitation is specified in this document;

12. the categorization pursuant to section 202(2) of the certification authority's compliance with this document and resulting from the most recent performance audit of the certification authority's activities, and the data of the most recent performance audit;

13. any event which substantially affects the certification

authority's ability to conduct its business or the validity of a certificate published in the repository provided by the Division or in a recognized repository;

14. if a certificate containing the public key required to verify one or more certificates issued by the certification authority has been revoked or is currently suspended, the date of its revocation or suspension; and

15. if the certification authority has a material, primary certification practice statement, indications of its location, the method or procedure by which it may be retrieved, its form and structure, its authorship, and its date, as prescribed in rule 302.

4. REFERENCES

This document is based on the certificate taxonomy developed by CygnaCom and documented in [1]. References 2 through 7 have been used to refine the framework.

1. Technical Specifications for Federal Public Key Infrastructure-Annex D: Interoperability Profiles, (Appendix E), CygnaCom Solutions, Inc., December, 1995.

2. Technical Specifications for Federal Public Key Infrastructure-Annex B: Technical Security Policy, National Institutes of Standards and Technology, December, 1995.

3. Statement of Work Federal Public Key Infrastructure Pilot, (Appendix A-Technical Specifications), Solicitation No. 52SBN5C8535, National Institutes of Standards and Technology, October, 1994.

4. Information System Security Policy and Certification Practice Statement, National Security Agency, March 12, 1996.

5. Government of Canada PKI - Certificate Policy and Certification Practices Statement Framework, November 12, 1996.

6. MISSI Policy Analysis, Booz, Allen and Hamilton, March 1996.

7. Recommendation X.509 and ISO 9594-8, Information Processing System - Open Systems Interconnection - The Directory - Authentication Framework, 1988.

8. Final Text of Draft Amendment DAM 4 to ISO/IEC 9594-2, DAM 2 to ISO/IEC 9594-6, DAM 1 to ISO/IEC 9594-7, and DAM 1 to ISO/IEC

9594-8 on Certificate Extensions, June 1996.

9. Utah Administrative Code.

10. American Bar Association, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Electronic Commerce, Draft 1995.

11. Baum, Michael S., Federal Certification Authority Liability and Policy, NIST-GCR-94-654, June 1994.

12. Certification Practices Statement, Verisign, 1996.

13. Privacy Enhanced Mail, Internet RFC 1421-23, 1994

5. CERTIFICATE POLICY AND CERTIFICATION PRACTICES FRAMEWORK: OVERVIEW

This section provides a brief overview of the certificate policy components. Section 6 provides a complete refinement of the components. Both the certificate policy and the CPS are composed of components described in this section and further refined in Section 6. Components can be further divided into subcomponents. Subcomponents can be divided into elements. Elements can be divided into subelements.

A certificate policy or CPS consists of the following components:

* Community and Applicability

* Identification and Authentication Policy

* Key Management Policy

* Local Security Policy

* Technical Security Policy

* Operations Policy

* Legal Provisions

* Certificate and CRL Profile

* Policy Administration

Each of these components is described below.

5.1 COMMUNITY AND APPLICABILITY

Under this component, the following are described:

* types of subject CA certified (e.g., subordinate banks, peer banks, regional offices, etc.) (2)

* types of subject Registration Authority (RA) certified (e.g., regional offices)

* types of end entities certified (e.g., employees, contractors, subscribers, customers, etc.) (3)

* applications for which the policy is suitable for, is restricted to, or must not be used in conjunction with.

5.2 IDENTIFICATION AND AUTHENTICATION (I&A) POLICY

This component is used to describe the various I&A policies. The I&A policies are fundamental to ensuring that the bindings between the public keys and the individuals are correct. The I&A policies may be the same or different for the subject CA, subject Registration Authority (RA), and subject end entities. For each class of subject (CA, RA, or end entity), the I&A policy may be different for the various interactions with the parent CA. The interactions include, initial registration, rekey, rekey after revocation, and revocation request. The component also describes if and how the trademarks are recognized (authenticated). The component also describes if and how name disputes are resolved.

5.3 KEY MANAGEMENT POLICY

This component is used to define the security measures taken by the CA to protect its cryptographic keys and critical security parameters (e.g., Personal Identification Number or PIN). This component may also be used to impose constraints on subject CAs and end entities to protect their cryptographic keys and critical security parameters. For the sake of completeness, for each type of entity (issuer CA, subject CA, RA, and end entity), and for each type of keying material (private key, parameters, public key, and critical security parameters) this element addresses the entire key life-cycle from generation, through storage and usage, to archival and destruction.

Secure key management is critical to ensure that all secret and private keys and critical security parameters are protected and used only by authorized personnel.

5.4 LOCAL SECURITY POLICY

This component is used to define the non-technical security controls used by the CA to perform CA functions securely. The CA functions include key generation, user authentication, certificate registration, certificate revocation, audit, and archival. The non-technical security controls include physical, personnel, and procedural controls.

This component is also used to define non-technical security controls on subject CAs, RAs, and end entities. The non technical security controls for the subject CAs, RAs, and end entities could be the same, similar, or quite different. In most cases they are envisioned to be quite different with tighter controls on the subject CAs and RAs due to the sensitivity of the functions they perform.

The security controls are critical to trusting the public key certificates since lack of security may compromise CA operations, resulting in creation of certificates or CRLs with erroneous information or even the compromise of the CA private key.

5.5 TECHNICAL SECURITY POLICY

This component is used to define the technical security controls used by the CA to perform CA functions securely. The CA functions include key generation, user authentication, certificate registration, certificate revocation, audit, and archival. The technical controls include life-cycle security controls (including software development environment security, trusted software development methodology) and operational security controls.

This component is also used to define technical security controls on subject CAs, RAs, and end entities. The technical security controls for the subject CAs, RAs, and end entities could be the same, similar, or quite different. In most cases they are envisioned to be quite different with tighter controls on the subject CAs and RAs due to the sensitivity of the roles they perform.

The security controls are critical to trusting the public key certificates since lack of security may compromise CA operations, resulting in the creation of certificates or CRLs with erroneous information or even the compromise of the CA private key.

5.6 OPERATIONS POLICY

This component is used to describe the frequency of routine Certificate Revocation List (CRL) issuance, frequency of special CRL issuance (e.g., key compromise CRL), and frequency for CA key changeover. It also describes how the CA operations are periodically audited by another entity and the CA's relationship with that entity. This component is also used to define who can revoke certificates under what circumstances.

This component is used to describe periodic compliance audits the CA performs on the subject CAs, RAs, and end entities. Periodic compliance audit on subject CAs and RAs is recommended to ensure compliance and to maintain trustworthiness of the whole infrastructure. Periodic compliance audit of subject end entities is also desirable, but not as critical as the subject CAs.

This component is also used to define the frequency of routine CRL issuance, frequency of special CRL issuance (e.g., key compromise CRL), and frequency for key changeover for the subject CAs. This component is also used to define the typical validity period for subject end entity certificates. These validity periods could be different based on key usage (e.g., signature, key establishment, etc.)

This component is also used to describe the CA, subject CAs, subject RAs, and subject end entities archival policies.

This component is also used to describe the procedures for recovering from CA and RA failure and compromise.

This component is also used to define the confidentiality policy for the information that the CA and RA hold.

This component is relevant for certificate policy, since a compliance audit policy increases the overall trustworthiness of the infrastructure entities. The CRL issuance frequency allows the users of the certificate to develop appropriate caching strategies. The key changeover period in conjunction with key size directly relate to the security offered by the cryptosystem.

5.7 LEGAL PROVISIONS

This component describes the liability policy including disclaimers of warranty and limitations on liability.

This component also defines the obligations of the subscribers (subject CA, RA, and end entities) and those of the certificate

users (relying parties).

It also describes applicable laws and regulations and dispute resolution procedures.

5.8 CERTIFICATE AND CRL PROFILE

This component is used to define the certificate and CRL versions and extensions supported (populated) by the CA and the criticality of the extensions. This component describes typical values of the following fields within the policy constraints extension: require explicit policy, and inhibit policy mapping.

This component is also used to define the certificate and CRL versions and extensions supported (populated) by the subject CAs and the criticality of the extensions. This component describes typical values of the following fields within the policy constraints extension: require explicit policy, and inhibit policy mapping.

The certificate profile could be different for different key usage such as signature, key management, certificate signing, CRL signing, etc.

5.9 POLICY ADMINISTRATION

This component is used to define the authority that is responsible for the registration, maintenance and interpretation of the policy. The information includes the name and address of the organization, and the name and the telephone number of a contact person.

This component also describes how the policy change is administered and how various notices are published and distributed.

This component also describes how the compliance of a specific CPS with the policy is determined.

6. **CERTIFICATE** POLICY AND CERTIFICATION PRACTICES FRAMEWORK: DESCRIPTION

In this section, we provide a complete refinement of the certificate policy and certification practices statement framework.

6.1 COMMUNITY AND APPLICABILITY

This component consists of the following subcomponents:

* Subject CAs

* Subject RAs

* Subject End Entities

* Applicability

This component describes the various types of certificate subscribers, and applications and standards.

The following sections describe these subcomponents.

6.1.1 Subject CAs

This subcomponent contains a brief description of the types of entities that are certified as subject CAs. (4)

6.1.2 Subject RAs

This subcomponent contains a brief description of the types of entities that are certified as subject RAs. (5)

6.1.3 Subject End Entities

This subcomponent contains a brief description of the types of entities that are certified as end entities. (6)

6.1.4 Applicability

This subcomponent contains:

* A list of applications for which the issued certificates are suitable

* A list of applications that the issued certificates are restricted to. (This list implicitly prohibits all other uses for the certificates.)

* A list of applications that the issued certificates are prohibited from being used for

6.2 IDENTIFICATION AND AUTHENTICATION (I&A) POLICY

This component contains the I&A policies for subject CAs, subject RAs, and subject end entities. These policies could be the same or different for each of these entities.

* Initial Registration

* Routine Rekey

* Rekey After Revocation

* Revocation Request

6.2.1 Initial Registration

This subcomponent contains the following:

* Identification and authentication policy for each subject type (CA, RA, and end entity) for initial registration

* Types of names assigned to the subject (7)

* Whether names have to be meaningful or not (8)

* Rules for interpreting various name forms

* Whether names have to be unique

* How name claim disputes are resolved

* Whether trademarks are recognized or not

* How trademarks are authenticated

* What role trademarks play in naming and identification and authentication

* If and how the subject must prove that (s)he possesses the companion private key for the public key being registered (9)

* Authentication requirements for organizational identity of subject (CA, RA, or end entity) (10)

* Authentication requirements for a person acting on behalf of subject (CA, RA, or end entity) (11)

* Number of identifications required

* How a CA or RA validates the identification cards provided

* If the person must present himself to the authenticating CA or RA

* How an individual as an organizational person is authenticated (12)

6.2.2 Routine Rekey

This subcomponent contains the I&A policy for routine rekey for each subject type (CA, RA, and end entity). (13)

6.2.3 Rekey After Revocation -- No Key Compromise

This subcomponent is used to describe the I&A policy for rekey for each subject type (CA, RA, and end entity) after the subject certificate has been revoked. (14)

6.2.4 Revocation Request

This subcomponent is used to describe the I&A policy for revocation request by each subject type (CA, RA, and end entity). (16)

6.3 KEY MANAGEMENT POLICY

This component consists of the key management policies for the following entities: issuing CA, subject CAs, subject RAs, and subject end entities. These four sets of policies could be the same or different.

6.3.1 Public and Private Key Pair

The key management policies for the issuing CA, subject CAs, Subject RAs, and subject end entities address the entire life-cycle of the public and private key pair from generation through archival and destruction. For each of these types of entities (issuing CA, subject CA, subject RA, subject end entity) the following questions should be answered:

6.3.1.1 Key Pair Generation and Installation

1. Who generates the entity public, private key pair?

2. How is the private key provided securely to the

entity?

3. How is the entity's public key provided securely to the certificate issuer?

4. If the entity is a CA (issuing or subject) how is the entity's public key provided securely to the users?

5. What are the key sizes?

6. Who generates the public key parameters?

7. Is the quality of the parameters checked during key generation?

8. Is the key generation performed in hardware or software?

9. For what purposes may the key be used (these purposes should be same as the key usage flags in the Version 3, X.509 certificates)?

10. For what purposes may the key must be restricted to(these purposes should be same as the key usage flags in the Version 3, X.509 certificates and the key usage field must be marked criical)?

11. What standards, if any, are required for the module used to generate the keys? For example, are the keys certified by the infrastructure required to be generated using modules complaint with the US FIPS 140-1? If yes, what is the security level of the module?

6.3.1.2 Private Key Protection

1. Is the private key under n out of m multi-person control?(18) If yes, provide n and m (two person control is a special case of n out of m, where n = m = 2)?

2. Is the private key escrowed? (19) 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?

3. 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?

4. 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?

5. Who enters the private key in the cryptographic module? In what form (i.e., plaintext, encrypted, or split key)?

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

7. 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?

8. Who can deactivate the private key and how? Example of how include, logout, power off, remove token/key, automatic, time expiration, etc.

9. Who can destroy the private key and how? Examples of how include token surrender, token destruction, key overwrite, etc.

6.3.1.3 Other Aspects of Key Pair Management

1. Is the public key archived? If so, who is the archival agent and what are the security controls on the archival system? The archival system should provide integrity controls other than digital signatures since: the archival period may be greater than the cryptanalysis period for the key and the archive requires tamper protection, which is not provided by digital signatures.

2. What are the validity periods for the public and the private key respectively?

6.3.2 Critical Security Parameters (20)

The key management policies for the issuing CA, subject CAs, Subject RAs, and subject end entities address the entire life-cycle of the critical security parameters from generation through archival and destruction. For each of these types of entities (issuing CA, subject CA, subject RA, subject end entity) the following questions should be answered:

6.3.2.1 Critical Security Parameter Generation and Installation

1. Who generates the initial critical security parameters?

2. How are the critical security parameters provided securely to the entity?

3. What are the size requirements on the parameters (e.g., PIN size, password size, etc.)?

6.3.2.2 Critical Security Parameter Protection

1. Are the parameters stored in a token (e.g., crypto ignition key)?

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

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

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

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

6.3.2.3 Other Aspects of Critical Security Parameters

1. Who enters the parameters in the cryptographic module?

In what form (i.e., plaintext, encrypted, or split key)?

2. How are the parameters used in the module (e.g., for authentication and private key activation, private key decryption and activation, etc.)?

3. What is the recommended life for the parameters?

4. Who can change the parameters?

6.4 LOCAL SECURITY POLICY

This component consists of four security policies for the four types of entities: one for the issuer CA, one for subject CAs, one for the subject RAs, and one for subject end-entities. The following sections describe the items required for these four security policies:

* Physical Controls

* Procedural Controls

* Personnel Controls

6.4.1 Physical Controls

The physical controls on the facility housing the entity systems are described.(21)

6.4.2 Procedural Controls

The procedural controls for the entity are described. These controls include the description of various trusted roles and responsibilities for each of the roles.(22)

For each of these roles, n out m rules should be defined, i.e. define how many people are required to perform the task. Identification and authentication requirements for each role must also be defined.

6.4.3 Personnel Controls

This subcomponent contains the following:

* Background checks and clearance procedures required for the personnel filling the trusted roles (23)

* Background checks and clearance procedures requirements for other personnel (24)

* Training requirements and training procedures for each role

* Any retraining period and retraining procedures for each role

* 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 (25)

* Controls on the contracting personnel for operating the entity system and facility

  - 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

  - Other controls on contracting personnel

6.5 TECHNICAL SECURITY POLICY

This component consists of four technical security policies for the four types of entities: one for the issuer CA, one for subject CAs, one for the subject RAs, and one for subject end- entities. The following sections describe the items required for these four technical security policies:

* Computer Security Controls

* Life-Cycle Security Controls

* Network Security Controls

* Cryptographic Module Engineering Controls

* Computer Security Assurance

* Life-Cycle Assurance

* Cryptographic Assurance

6.5.1 Computer Security Controls

This subcomponent is used to describe computer security controls. Examples of computer security controls are: trusted computing base concept, discretionary access control, labels, mandatory access controls, object reuse, audit, identification and authentication, trusted path, security testing, penetration testing, etc.

6.5.2 Life Cycle Security Controls

This subcomponent is used to describe 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 Fail-Safe design techniques, use of Fail-Safe 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.

6.5.3 Network Security Controls

This subcomponent is used to describe network security related controls for the system. Examples of network security controls are: firewalls, guards, etc.

6.5.4 Cryptographic Module Engineering Controls (26)

This subcomponent contains the following aspects of the cryptographic module: 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, key management, and self tests.

6.5.5 Computer Security Assurance

This subcomponent is used to describe the computer security rating for the computer system. The rating could be based on the Trusted System Evaluation Criteria (TCSEC), Canadian Trusted Products Evaluation Criteria, European Information Technology Security Evaluation Criteria, or the Common Criteria.

This subcomponent is also used to describe the evaluation analysis, testing, profiling, certification, and/or accreditation related activity undertaken.

6.5.6 Life-Cycle Assurance

This subcomponent is used to describe the life-cycle security controls rating such as the Trusted Software Development Methodology (TSDM) level, IV&V, independent life-cycle security controls audit, and Software Engineering Institute's Capability Maturity Model (SEI-CMM).

6.5.7 Cryptographic Assurance

This subcomponent is used to describe the cryptographic module's compliance with applicable standards (e.g., US FIPS 140-1). (27)

6.6 OPERATIONS POLICY

The operations policy is used to describe the operating procedures for the issuing CA, subject CAs, subject RAs, and subject end entities. Each operations policy consists of the following subcomponents:

* revocation policy

* key compromise policy

* audit policy

* archive policy

* key changeover policy

* recovery procedures

* compliance audit

* non-disclosure policy. The subject end entity policy does not contains the non-disclosure policy subcomponent.

6.6.1 Revocation Policy

This subcomponent contains the following:

* Circumstances under which the entity certificate may be revoked

* Who can request the revocation of the entity certificate

* Procedures used for certificate revocation request

* Revocation request grace period available to the entity

* Circumstances under which the entity certificate may be suspended (held)

* Who can request the suspension (hold) of the entity certificate

* Procedures used for certificate suspension (hold) request

* How long the suspension may last

* CRL issuance frequency by the entity

* Requirements on the entity to check CRLs

* On-line revocation checks available

* Requirements on the entity to perform on-line revocation checks

* Other forms of revocation advertisements available

* Requirements on the entity to checks other forms of revocation advertisements

6.6.2 Key Compromise Policy

This subcomponent is used to describe the following:

* Procedures used by the entity to report key compromise

* Key compromise notification grace period available to the entity

* Key compromise CRL issuance frequency by the entity

* Requirements on the entity to check key compromise CRL

6.6.3 Audit Policy

This subcomponent is used to describe the following:

* Types of events the entity audits (28)

* Frequency with which each event is audited

* Period for which audit logs are kept

* Protection of audit logs

  - Who can view the audit log

  - Protection against modification of audit log

  - Protection against deletion of audit log

* Audit log back up procedures

* Whether the audit collection system is internal or external to the entity

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

6.6.4 Archive Policy

This subcomponent is used to describe the following:

* Types of event to be archived (29)

* Retention period for archive

* Protection of archive

  - Who can view the archive

  - Protection against modification of archive

  - Protection against deletion of archive

* Archive back up procedures

* Whether the archive collection system is internal or external to the entity

* Archive custodian in case of entity termination

* Procedures to obtain and verify archive information

6.6.5 Key Changeover

This subcomponent contains the following:

* Entity public key validity period

* Procedures to provide the new entity public key to the users

6.6.6 Recovery Procedures

This subcomponent is used to describe the disaster recovery procedures for the entity.

This subcomponent also contains the recovery procedures used by the entity under each of the following circumstances:

* The recovery procedures used if the entity computing resources, software, and/or data are corrupted or suspected to be corrupted. These procedures describe how a secure environment is reestablished, which certificates and CRL are revoked, whether the entity key is revoked, how the new entity public key is provided to the users, and how the

subjects are recertified.

* The recovery procedures used if the entity public key is revoked. 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 recertified.

* 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 recertified.

6.6.7 Compliance Audit

This subcomponent contains the following:

* Frequency of compliance audit for the entity

* Identity of the audit entity

* Auditing entity's relationship to the entity being audited (30)

* List of topics covered under the compliance audit(31)

* Actions taken as a result of a deficiency found during compliance audit (32)

* Compliance audit results: who are they shared with (e.g., subject CA, RA, and/or end entities), who provides them (e.g., entity being audited, or auditor), how are they provided, i.e., communication mechanism

6.6.8 Non-disclosure Policy

This subcomponent contains the following:

* Information that must be kept confidential by the entity

* Who is entitled to know what in terms of the reasons for revocation and suspension of the certificates issued by the entity

* Who is entitled to know what in terms of the reasons for revocation and suspension requested by the entity

* Information that can be revealed to the law enforcement

personnel

* Information that can be revealed as part of civil discovery

* List of other mitigating circumstances under which confidential information may be disclosed

6.7 LEGAL PROVISIONS

The legal provisions include the following subcomponents for each of the four types of the entities (issuing CA, subject CAs, subject RAs, and subject end entities):

* Entity Liability Policy

* Entity Obligations

* Certificate User (Relying Party) Obligations

* Financial Responsibility

* Laws and Procedures

* Fees

The subject end entities only contain the following subcomponents: entity liability policy, entity obligations.

6.7.1 Entity Liability Policy

This subcomponent contains the following:

* Warranties and disclaimers of warranties

* Liabilities and limitations on liabilities

6.7.2 Entity Obligations

This subcomponent contains the following:

* Entity's obligations in terms of accuracy of representation

* Obligations of the entity to protect the private key

* Purpose for which the entity's private key is constrained to be used for

* Entity's obligations for notification of issuance of a certificate to the subscriber who is the subject of the certificate being issued

* Entity's general obligations for notification of issuance of a certificate to others than the subject of the certificate

* Entity's obligations for notification of revocation of a certificate to the subscriber whose certificate is being revoked

* Entity's general obligations for notification of revocation of a certificate to others than the subject whose certificate is being revoked

* Entity's obligations for notification of suspension of a certificate to the subscriber whose certificate is being suspended

* Entity's general obligations for notification of suspension of a certificate to others than the subject whose certificate is being suspended

6.7.3 Certificate User (Relying Party) Obligations

This subcomponent contains the following elements:

* Purposes for which a relying party may use the certificates issued by the entity

* Certificate verification responsibilities of the relying parties

* Revocation and suspension checking responsibilities of the relying parties

6.7.4 Financial Responsibility

This subcomponent contains the following elements:

* Indemnification clause for the entity by the certificate users

* Fiduciary relationship of the entity with subscribers and entities in the infrastructure

6.7.5 Laws and Procedures

This subcomponent contains the following elements:

* Statement about applicable laws and regulations

* Dispute resolution procedures

6.7.6 Fees

This subcomponent contains the following elements:

* Certificate issuance fee

* Certificate access fee

* Revocation information access fee

* Fee for other services such as the certificate status, policy information, etc.

* Refund policy for the various services

6.8 CERTIFICATE AND CRL PROFILES

This component is used to define the certificate and CRL versions and extensions supported (populated) by the issuing CA and the subject CAs. This component contains the following information:

* Certificate Profile

* CRL Profile

6.8.1 Certificate Profile

This subcomponent has the following information: certificate version, naming, policy related information.

6.8.1.1 Certificate Version

This subcomponent has the following elements:

* A list of version numbers supported for the certificate

* A list of certificate profiles (e.g., PKIX, Federal PKI, or ANSI X9.57, etc.)

* Certificate extensions populated and their criticality.

* Signature, key management, and other cryptographic algorithms object identifiers

6.8.1.2 Naming

This subcomponent has the following elements:

* Name forms used for the CA, RA, and end entity names

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

6.8.1.3 Policy

This subcomponent has the following elements:

* Applicable policy OID for this policy

* Typical values for the following fields within the policy constraints extension: require explicit policy and inhibit policy mapping

* Policy qualifiers syntax, semantics, and their processing semantics

* Processing semantics for the critical certificate policy extension

6.8.2 CRL Profile

This subcomponent has the following elements:

* A list of the version numbers supported for CRLs

* CRL and CRL entry extensions populated and their criticality

6.9 POLICY ADMINISTRATION

This component is used to define the authority that is responsible for the registration, maintenance, and interpretation of the policy.

6.9.1 Contact Information

This subcomponent includes the name, mailing address of the organization, and the name, electronic mail address, telephone number, and fax number of a contact person. It also describes who performs the analysis of a CPS to determine its suitability as an implementation vehicle for the policy.

6.9.2 Policy Definition and Practice Statement Change Procedures

It will occasionally be necessary to change certificate policies and Certification Practice Statements. Some of these changes will not change the assurance that a certificate policy or its implementation provide, and will be judged by the policy administrator as not changing the acceptability of certificates asserting the policy for the purposes for which they have been used. Such changes to security policies and Certification Practice Statements need not require a change in the policy Object Identifier (OID). Changes to other policy components (or their implementations) will change the acceptability of certificates for specific purposes, and these changes will require changes to the OID representing the changed policy.

This subcomponent contains the following information:

* a list of policy or CPS components, subcomponents, and elements that can be changed without notification and without changes to the policy OID.

* a list of the policy or CPS components, subcomponents, and elements that may change following a notification period without changing the policy OID. The procedures to be used to notify interested parties (relying parties, certification authorities, etc.) of the policy or CPS changes is described. The description of notification procedures includes the notification mechanism, notification period for comments, mechanism to receive, review and incorporate the comments, mechanism for final changes to the policy, and the period before final changes become effective.

* a list of components, subcomponents, and elements changes to which require a change in the policy object identifier.

6.9.3 Publication and Notification Policies

This subcomponent contains the following elements:

* list of components, subcomponents, and elements that are not published in the CPS(33)

* descriptions of mechanisms used to distribute the policy, CPS, certificates, certificate status, and CRLs

* access control on information objects including the policy, CPS, certificates, certificate status, and CRLs

* notification procedures for the security breaches of CA and RA

* procedures for termination and for termination notification of the CA and RA, including the identity of the custodian of CA and RA archival records

7. CERTIFICATE POLICY AND CPS OUTLINE

This appendix contains a possible outline for a certificate policy or a CPS. With further development, it is intended to evolve to a standard template suitable for use by certificate policy or CPS writers. Such a common format will facilitate:

1. ease in comparing two policies during cross-certification (for the purpose of equivalency mapping).

2. ease in comparing a CPS with a policy to ensure that the CPS faithfully implements the policy.

3. ease in comparing two CPS for equivalency.

Following is the proposed outline for a certificate policy or CPS. Since a certificate policy and a CPS both address the same issues (a CPS is a detailed description of how a policy is implemented), we expect that they both should be able to use the same outline.

It is proposed that the upper two levels of this outline form the basis of a certificate policy or CPS template. Lower level items constitute a useful checklist for the certificate or CPS writer, but would not form part of the template.

COMMUNITY AND APPLICABILITY

Types of CAs certified

Types of RAs certified

Types of end entities certified

Applicability

List of suitable applications

List of approved applications

List of prohibited applications

IDENTIFICATION AND AUTHENTICATION (34)

Initial registration

Types of names

Need for names to be meaningful

Rules for interpreting various name forms

Uniqueness of names

Name claim dispute resolution procedure

Recognition, authentication and role of trademarks in I&A

Method to prove possession of private key

Authentication of organization identity

Authentication of individual identity

Number of identifications required

Authentication confirmation procedure

Need to present in person

Routine Rekey

Authentication method

Method to prove possession of private key

Rekey after revocation

Authentication method

Method to prove possession of private key

Revocation Request

Authentication method

KEY MANAGEMENT (34)

Key Pair Generation and Installation

Key pair generating entity

Method for private key delivery to entity

Method for public key delivery to certificate issuer

Method for CA public key delivery to users

Key sizes

Public key parameters generating entity

Parameter quality checking

Hardware/software key generation

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

Key usage restrictions (as per X.509 v3 critical key usage field)

Standards for cryptographic module

Private Key Protection

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

Private key escrow

Private key backup

Private key archival

Private key entry into cryptographic module

Storage form of the private key in the module

Method of activating private key

Method of deactivating private key

Method of destroying private key

Other Aspects of Key Pair Management

Public key archival

Usage periods for the public and private keys

Critical Security Parameters Generation and Installation

Critical security parameter generating entity

Method for delivery of critical security parameters

Critical security parameter sizes

Critical Security Parameter Protection

Storage medium for critical security parameters

Critical security parameters under (n out of m) multi-person control

Critical security parameters escrow

Critical security parameters backup

Critical security parameters archival

Other Aspects of Critical Security Parameters

Critical security parameters entry into cryptographic module

Critical security parameters purpose

Usage periods for critical security parameters

Changes to critical security parameters

LOCAL SECURITY POLICY (34)

Physical controls

Procedural controls

- Separation of duties
- n out of m rule for each role
- I&A requirement for each role

Personnel Controls

- Clearance procedures
- Training requirements
- Retraining period and requirements
- Job rotation frequency and sequence
- Sanctions for unauthorized use
- Contracting personnel
  - Bonding requirements
  - Indemnification for damages due to contractor
  - Audit and monitoring of contractor personnel
  - Other controls

TECHNICAL SECURITY POLICY (34)

Computer security controls

- Trusted Computing Base
- Identification and Authentication
- Discretionary Access Controls
- Labels
- Mandatory Access Controls
- Object Reuse
- Audit
- Trusted Path

- Security Testing
- Penetration Testing

Life cycle technical controls

- System development controls
  - Development environment security
  - Development personnel security
  - Configuration management
  - Development facility physical controls
  - Software engineering practices
  - Software development methodology
  - Modularity
  - Layering
  - Fail-Safe Design
  - Fail-Safe Implementation
- Security management controls
  - Procedures
  - Tools
  - Software Integrity
  - Firmware Integrity
  - Hardware Integrity

Network security controls

- firewalls and guard
- firewall and guard policy
- firewall and guard security rating

- Crypto Engineering Controls
  - input/output
  - roles and services
  - finite state machine
  - physical security
  - software security
  - operating system security
  - algorithm compliance
  - electromagnetic compatibility
  - key management
  - self tests
- Computer Security Assurance
  - standard
  - rating organization
  - accreditation of rating organization
  - rating
  - Evaluation analysis
  - Security testing
  - System security profiling
  - System certification and/or accreditation
- Life-cycle Security Assurance
  - TSDM level, rating organization, and accreditation of rating organization
  - IV&V
  - Independent life-cycle security controls audit

SEI CMM level, rating organization, and accreditation of rating organization

Cryptographic Module Assurance

standard

rating organization

accreditation of rating organization

rating

OPERATIONS POLICY (34)

Revocation

When can entity (CA, RA, or end entity) certificate be revoked

Who can request revocation of entity certificate

Procedure for entity certificate revocation

Revocation request grace period

When can the entity certificate be suspended (put on hold)

Who can request the entity certificate suspension

Procedures for entity certificate suspension request

Length of suspension

CRL issuance frequency by the entity (if applicable)

CRL check requirement on the entity

On-line revocation checks available

Requirements on the entity to perform on-line revocation checks

Other forms of revocation advertisements available

Requirements on the entity to check other forms of revocation advertisements

Key compromise

Procedure used by the entity to report key compromise

Key compromise notification grace period

Key compromise CRL issuance by the entity (if applicable)

Requirement on the entity to check key compromise CRL

Audit policy

Types of event to be audited

Frequency with which each event is audited

Retention period for audit log

Protection of audit log

Who can view the audit log

Protection against modification of audit log

Protection against deletion of audit log

Audit log back up procedures

Audit collection system (internal or external to the entity)

Notification to audit causing subject

Archive policy

Types of event to be archived

Retention period for archive

Protection of archive

Who can view the archive

Protection against modification of archive

Protection against deletion of archive

Archive back up procedures

Archive collection system (internal or external to the entity)

Archive custodian in case of entity termination

Procedures to obtain and verify archive information

Key changeover

Public key validity period

Procedures to provide new key to users

Recovery procedures

Disaster recovery procedures

Recovery from entity resources corruption

Recovery from entity public key revocation (no key compromise)

Recovery from entity private key compromise

Compliance audit

Frequency of entity compliance audit

Entity's relationship to the auditor

Topic covered by the audit

Actions taken as a result of deficiency

Entities who are provided the results of compliance audit

Entity who provides the results of compliance audit

Mechanism used to provide results of compliance audit

Non-disclosure policy

Information to be kept confidential by the entity

Disclosure rules (who can be told what) for reasons of revocation/suspension of certificates

Information that can be revealed to the law enforcement personnel

Information that can be revealed as part of civil discovery

Mitigating circumstances when confidential information may be disclosed

LEGAL PROVISIONS

Certification Authority

Liability

Warranties and disclaimers of warranties

Liabilities and limitations on liabilities

CA obligations

Accuracy of representations

Protection of issuing CA private key

Restrictions on issuing CA private key use

Notification of issuance of a certificate to the subject of the certificate

Notification of issuance of a certificate to others

Notification of revocation of a certificate to the subject of the certificate

Notification of revocation of a certificate to others

Notification of suspension of a certificate to the subject of the certificate

Notification of suspension of a certificate to others

Certificate user obligations

Use of certificates for appropriate purpose

Certificate verification responsibilities

Revocation/suspension check responsibility

Financial responsibility

Indemnification of issuing CA by certificate users

Fiduciary relationships of the issuing CA

Laws and procedures

Applicable laws and regulations

Dispute resolution procedures

Fees

Certificate issuance fee

Certificate access fee

Revocation information access fee

Fee for other services such as the certificate status, policy information, etc.

Refund policy for the various services.

Registration Authority

Liability

Warranties and disclaimers of warranties

Liabilities and limitations on liabilities

Subject RA obligations

Accuracy of representations

Protection of RA private key

Restrictions on RA private key use

Certificate user obligations

Use of certificates for appropriate purpose

Certificate verification responsibilities

Revocation/suspension check responsibility

Financial responsibility

Indemnification of RA by certificate users

Fiduciary relationships of RA

Laws and procedures

Applicable laws and regulations

Dispute resolution procedures

Fees

Certificate registration fee

Certificate revocation fee

Fee for other services

Refund policy for the various services.

End entity

Liability

Warranties and disclaimers of warranties

Liabilities and limitations on liabilities

End entity obligations

Accuracy of representations

Protection of end entity private key

Restrictions on end entity private key use

CERTIFICATE AND CRL PROFILES (34)

Certificate Profile

Certificate Version

A list of version numbers supported for the certificate

A list of certificate profiles (e.g., PKIX, Federal PKI, or ANSI X9.57, etc.)

Certificate extensions populated and their criticality.

Signature, key management, and other cryptographic algorithms object identifiers

Naming

Name forms used for the CA, RA, and end entity names

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

Policy

Applicable policy OID for this policy

Typical values for the following fields within the policy constraints extension: require explicit policy and inhibit policy mapping

Policy qualifiers syntax, semantics, and their processing semantics

Processing semantics for the critical certificate policy extension

CRL Profile

A list of the version numbers supported for CRLs

CRL and CRL entry extensions populated and their criticality

POLICY ADMINISTRATION

Contact information

Name and mailing address of the policy administration organization

Name, electronic mail address, telephone number, and fax number of a contact person

Name and telephone number of person determining CPS suitability for the policy

Policy definition change procedures

List the items that can change without notification

Items that can change with notification

List of items

Notification mechanism

Comment period

Mechanism to handle comments

Period for final change notice

List of items whose change requires a new policy

Publication and notification policies

List of items not published in the CPS

Mechanisms used to distribute policy, CPS, certificates, certificate status, and CRLs.

Access control on information objects including the policy, CPS, certificates, certificate status, and CRLs

Notification procedures for security breaches of issuing CA

Notification procedures for security breaches of subject CA

Notification procedures for security breaches of subject RA

Termination procedure and notification for issuing CA

Termination procedure and notification for subject CA

Termination procedure and notification for subject RA

8. LIST OF ACRONYMS

ABA - American Bar Association

CA - Certification Authority
CC - Common Criteria
CMM - Capability Maturity Model
CPS - Certification Practice Statement
CRL - Certificate Revocation List

DAM - Draft Amendment
DAP - Directory Access Protocol

FIPS - Federal Information Processing Standard
FSDA - Fail Safe Design Analysis

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
IV&V - Independent Validation and Verification

MSP - Message Security Protocol

NIST - National Institute of Standards and Technology

OID - Object Identifier

PIN - Personal Identification Number
PKCS - Public Key Cryptography Standard
PKI - Public Key Infrastructure
PKIX - Public Key Infrastructure (X.509) (IETF Working Group)

RA - Registration Authority
RFC - Request For Comment

SEI - Software Engineering Institute
S-HTTP - Secure HyperText Transfer Protocol
S/MIME - Secure/Multipurpose Internet Mail Extension

TCP - Transmission Control Protocol
TCSEC - Trusted Computer System Evaluation Criteria
TSDM - Trusted Software Development Methodology

URL - Uniform Resource Locator
US - United States

9. GLOSSARY OF TERMS

Accreditation: A decision by the responsible official of the organization to operate a system and accept the residual risks identified by the certification activities, or to accept the risks even though no certification activities have been done or completed.

(System) Certification: A series of security engineering activities to ensure that the security requirements for a system are implemented correctly, and to identify residual risks. The certification activities typically consist of security analysis of the system architecture, design, and implementation and security testing of the system.

End Entity: A person or a computer system who is not a CA or RA.

Entity: A CA, RA, or end entity.

Relying Party: Someone who uses a public key in a certificate to

either verify a digital signature or to encrypt keys or data.

Critical Security Parameters: security-related information (e.g., cryptographic keys, authentication data such as passwords and personal identification number (PIN))

Subject: An entity whose public key is certified in a public key certificate.

Subject End Entity: An end entity who is the subject of a certificate.

Subscriber: See subject

User: See relying party

10. ENDNOTES

1 Extracts of the ABA Digital Signature Guidelines presented in this report are taken from the 1995 draft version which was publicly released for review and comment. Later work revising the document has not been publicly released, but does not materially impact the correctness of this report.

2 Example: A bank claims that it issues CA certificates to its branches only. Now, the user of a CA certificate issued by the bank can assume that the subject CA in the certificate is a branch of the bank.

3 Example: A Government CA claims that it issues certificates to Government employees only. Now, the user of a certificate issued by the Government CA can assume that the subject of the certificate is a Government employee.

4 Examples of the types of subject CA entities are a subordinate organizations (e.g., branch, division, etc.), a US Federal Government agency, a Government of Canada agency, a state agency, a provincial department, etc.

5 Examples of the types of subject RA entities are branch and division of an organization.

6 Examples of types of subject end entities are uniformed and civilian DoD personnel, DoD contractors, Ministry of Defense employees, bank customers, telephone company subscribers, etc.

7 Examples include X.500 distinguished names, RFC 822 Internet names, URL, etc.

8 The term meaningful means that the name form has commonly understood semantics to determine identity of the person and/or organization. The directory names and RFC 822 names are examples of meaningful names.

9 Examples of proof include the issuing CA generating the key, or requiring the subject to send an electronically signed request or to sign a challenge.

10 Examples of organization identity authentication are: articles of incorporation, duly signed corporate resolutions, company seal, and notarized documents.

11 Examples of individual identity authentication are: biometrics (thumb print, ten finger print, face, palm, and retina scan), driver's license, passport, credit card, company badge, and government badge.

12 Examples include duly signed authorization papers, corporate badge, etc.

13 The identification policy for routine rekey should be the same as the one for initial registration since the same subject needs rekeying. The rekey authentication may be accomplished using the techniques for initial I&A or using digitally signed requests.

14 This I&A policy could be the same as the one for initial registration.

15 This policy could be the same as the one for initial registration.

16 The identification policy for Revocation request could be the same as the one for initial registration since the same subject certificate needs to be revoked. The authentication policy could accept a Revocation request digitally signed by subject. The authentication information used during initial registration could be acceptable for Revocation request. Other less stringent authentication policy could be defined.

17 The identification policy for key compromise notification could be the same as the one for initial registration since the same subject certificate needs to be revoked. The authentication policy could accept a Revocation request digitally signed by subject. The authentication information used during initial registration could be acceptable for key compromise notification. Other less stringent authentication policy could be defined.

18 The n out of m rule allows a 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 key, but having any n-1 parts provides one with no information about the key.

19 A key may be escrowed, backed up or archived. Each of these functions have different purpose. Thus, a 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 legally obtain the key without the cooperation of the subject. The purpose of back up is to allow the subject to reconstitute the key in case of the destruction of the key. The purpose of archive is to provide for reuse of the key in future, e.g., use the private key to decrypt a document.

20 The critical security parameters are the information other than the public and private key pair and public key parameters required to operate the module. An example of a critical security parameters is a PIN or passphrase. The public key parameters are NOT an example of critical security parameters.

21 Examples of physical controls are: monitored facility, guarded facility, locked facility, access controlled using tokens, access controlled using biometrics, access controlled through an access list, etc.

22 Examples of the roles include, system administrator, system security officer, system auditor, and crypto officer. The duties of the system administrator are to configure, generate, boot, and operate the system. The duties of the system security officer are to assign accounts and privileges. The duties of the system auditor are to set up system audit profile, perform audit file management, and audit review. The duties of the crypto officer are to hold, manage, and protect the CA keys and PINs, and to use them to operate the cryptographic devices used by the CA to sign the certificates and the CRLs.

23 The background checks may include clearance level (e.g., none, sensitive, confidential, secret, top secret, etc.) and the clearance granting authority name. In lieu of or in addition to a defined clearance, the background checks may include types of background information (e.g., name, place of birth, date of birth, home address, previous residences, previous employment, and any other information that may help determine trustworthiness). The description should also include which information was verified and how.

24 For example, the certificate policy may impose personnel security requirements on the network system administrator responsible for a CA's network access.

25 Each authorized person should be accountable for his/her actions.

26 A cryptographic module is hardware, software, or firmware or any combination of them.

27 The compliance description should be specific and detailed. For example, for each FIPS 140-1 requirement, describe the level and whether the level has been certified by an accredited laboratory.

28 Example of audit events are: request to create a certificate, request to revoke a certificate, key compromise notification, creation of a certificate, revocation of a certificate, issuance of a certificate, issuance of a CRL, issuance of key compromise CRL, establishment of trusted roles on the CA, actions of truste personnel, changes to CA keys, etc.

29 Example of archive events are: request to create a certificate, request to revoke a certificate, key compromise notification, creation of a certificate, revocation of a certificate, issuance of a certificate, issuance of a CRL, issuance of key compromise CRL, and changes to CA keys.

30 a parent CA is an example of audit relationship.

31 Example of compliance audit topics: sample check on the various I&A policies, comprehensive checks on key management policies, comprehensive checks on system security controls, comprehensive checks on operations policy, and comprehensive checks on certificate profiles,

32 The examples include, temporary suspension of operations until deficiencies are corrected, revocation of entity certificate, change in personnel, invocation of liability policy, more frequent compliance audit, etc.

33 An organization may choose not to make public some of its security controls, clearance procedures, or some others elements due to their sensitivity.

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

11. Security Considerations

This entire memo deals with security related to public key certificates.

12. Acknowledgments

We would like to thank Dave Fillingham and Jim Brandt for their inspiration, numerous valuable suggestions and inputs. We would also like to thank Edmond Van Hees for his support and inputs. We would also like to thank the Government of Canada's Policy Management Authority (PMA) Committee for their contribution and support of this work.

This document has been developed under the guidance of the International Policy Framework Working Group. The members of this working group are: Richard Bloom, US Federal Security Infrastructure Program Management Office; Santosh Chokhani (Co-Author), CygnaCom Solutions, Inc.; David W. Fillingham, National Security Agency; Warwick Ford (Co-Author); Richard Kemp, US Federal Security Infrastructure Program Management Office; Noel Nazario, National Institute of Standards and Technology; David Simonetti, Booz, Allen and Hamilton; and Edmond Van Hees, Communication Security Establishment, Government of Canada.

We would also like the following industry members for their review and input: Teresa Acevedo, A&N Associates; Michael Baum, Verisign; Patrick Cain, BBN; Michael Harrop, Government of Canada Treasury Board; John Morris, CygnaCom Solutions, Inc.; Tim Moses, Nortel; John Nicolletos, A&N Associates; Jean Petty, CygnaCom Solutions, Inc.; and Darryl Stal, Nortel.

Johnny Hsiung and Chris Miller assisted in the preparation of the manuscript.

13. Author's Address

Questions about this document can be directed to the authors:

Santosh Chokhani
CygnaCom Solutions, Inc.
Suite 100 West
7927 Jones Branch Drive
McLean, VA 22102

Phone: (703) 848-0883
Fax: (703) 848-0960
EMail: chokhani@cygnacom.com

Warwick Ford
VeriSign, Inc.

Phone: (613) 225-3487
Fax: (613) 225-6361
Email: wford@verisign.com

expires in six months June 1997