PKI Model Certificate Policy

A White Paper

NECCC
E-SIGN INTEROPERABILITY WORK GROUP
December, 2001

1.1 National Electronic Commerce Coordinating Council

1.2 The National Electronic Commerce Coordinating Council (**NECCC**) was established in 1997 to promote electronic government based on emerging issues and best practices through an alliance of national associations. The Alliance is comprised of the National Association of State Auditors, Comptrollers and Treasurers (**NASACT**), The National Association of Chief Information Officers (**NASCIO**), the National Association of State Procurement Officials (**NASPO**), the National Association of Secretaries of State (**NASS**). In addition, there are six non-voting affiliated members: the Information Technology Association of American (**ITAA**), the National Automated Clearing House Association (**NACHA**), the National Association of State Chief Administrators (**NASCA**), the National Governors Association (**NGA**). The National Association of Government Archive and Records Administrators (**NAGARA**), and the National Association of State Treasurers (**NAST**) became Council members in October 2001. The ITAA and NACHA specifically represent private information technology companies and the financial services and technology industries.

NECCC 2001 EXECUTIVE BOARD

Chair: **Carolyn Purcell**, NASCIO, CIO, State of Texas
Vice Chair: **Hon. J. Kenneth Blackwell**, NASS, Secretary of State, Ohio
Secretary/Treasurer: **Richard Thompson**, NASPO, Director, Maine Division of Purchases
Immediate Past Chair: **Hon. J. D. Williams,** NASACT, Idaho State Controller

NECCC 2001 BOARD

NASCIO	**David Lewis,** Massachusetts Chief Information Officer
	Aldona Valicenti, Kentucky Chief Information Officer
NASPO	**Dave Ancell** Director, Office of Purchasing, Michigan Department of Management & Budget
	Denise Lea, Director, Office of State Purchasing, Louisiana
NASS	**Hon. Mary Kiffmeyer** Minnesota Secretary of State
	Hon. Elaine Marshall North Carolina Secretary of State
NASACT	**Hon. Ralph Campbell,** State Auditor, North Carolina
	Hon. Jack Markell, State Treasurer, Delaware
ITAA	**Basil Nikas** CEO, iNetPurchasing.Com
NACHA	**William Kilmartin** Strategic Alliance Director, Accenture
NASCA	**Pam Ahrens** Director, Idaho Department of Administration
NGA	**Thom Rubel** National Governors Association
NAGARA	**Terry Ellis**, Salt Lake City Records Manager
NAST	**Hon. Jack Markell**, Delaware State Treasurer

NECCC STAFF

Eveanna Barry • ebarry@nasact.org
Scott Etter • setter@nasact.org
web: www.ec3.org

Model Certificate Policy

Based on Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

1. **INTRODUCTION**

This document defines four certificate policies for use in the _____(name of state) Public Key Infrastructure (___ PKI): one for Confidentiality/Encryption, two representing different assurance levels for Digital Signatures and one for Electronic Notary Signatures. These policies contain the rules governing the issuance and use of certificates by those parties authorized to participate in the ___ PKI. The Policy Specification portion of the document follows and complies with the Internet Engineering Task Force Public Key Infrastructure X.509 (IETF PKIX) Part 4 Certificate Policy and Certification Practice Statement Framework.

This document uses several technical concepts associated with PKI technology. To become familiar with the terminology used, we strongly recommend that you read the Electronic and Digital Signature Definitions and Acronyms document before reading this one and then refer to it as needed while reading this.

The security mechanisms provided by the ___ PKI are intended for use in combination with one or more additional security conventions to give protection appropriate to sensitive information.

1.1 Overview

This document defines Certificate Policies intended for use by Government Entities in the State of _____. Four policies are defined: two for Digital Signature certificates, one for Notary Digital Signatures and one for Confidentiality/Encryption certificates. For the convenience of the reader, all four policies have been combined into one document, which will be referred to as "the policy," "the policies," or "CP." When referring to a specific certificate policy, that policy will be mentioned by name and capitalized (e.g., "Confidentiality/Encryption Certificate Policy").

Digital Signature certificate policies are for the management and use of certificates containing public keys used for verification, authentication, integrity, and signing. For instance, the certificates issued under such policies could be used for verifying the identity of electronic mail correspondents, for providing remote access to a computer system, for verifying the identity of citizens or other legal entities, for protecting the integrity of software and documents, or for signing a document.

The Confidentiality/Encryption Certificate Policy contained herein is for the management and use of certificates containing public keys used for encryption key establishment, including key transfer. The certificates issued under this policy are suitable for providing confidentiality/encryption for applications such as electronic mail or Web communications.

Each Certificate Policy herein also represents a different level of "assurance." "Assurance," in this CP, means how well a Relying Party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate. In addition, it also reflects how well the Relying Party can be certain that the individual whose subject name is cited in the

certificate is controlling the use of the private key that corresponds to the public key in the certificate. The term "assurance" is not intended to convey any representation or warranty as to 100% availability of CA services offered under the ___ PKI. Such availability may be affected by system maintenance, system repair or factors outside the control of the CA. The State of _____ does not represent or warrant 100% availability offered under the ___ PKI.

The laws of the State of _____ without regard to the conflicts of laws principles thereof concerning the enforceability, construction, interpretation and validity of this Certificate Policy will govern a CA operating under this Policy, as well as any disputes arising from the use of the certificates issued by such CAs.

The State of _____ reserves the right not to enter into a cross certification agreement with a Certification Authority external to the ___ PKI.

1.1.1 Policy overview

The Policy Object Identifier Designation for these Policies is _____.

The policies are designed for use in certain situations, and identify specific roles and responsibilities for Certificate Authorities (CA) issuing certificates under the ___ PKI and for Registration Authorities (RAs), Local Registration Authorities (LRAs), Certificate Manufacturing Authority (CMA), Subscribers and Relying Parties under the ____ PKI; all have specific obligations outlined in this policy.

[commentary - This Certificate Policy may be the total policy framework for a state's electronic signature and confidentiality/encryption uses, in that case the term "___ PKI" is sufficient. If this Certificate Policy is part of a larger policy framework for a state's electronic signature and confidentiality/encryption uses or if there are reasons to describe particular communities or processes, then the term "ESI" (Electronic Signature Infrastructure) might be useful to describe a particular framework established for a specific community or class of applications. This document occasionally uses the term ESI, if that is not appropriate (e.g. this Certificate Policy covers all communities and applications) then it can be replaced with ____ PKI.]

A CA must associate itself with and use one or more Certificate and one or more CRL repository. Certificates must be made available to Subscribers.

The use of confidentiality/encryption keys is appropriate for the confidentiality/encryption of designated information.

The use of Certificate Policy Digital Signatures Medium Assurance is appropriate for all transactions with Government Entities in _____(state) that require authentication and / or a signature. The use of Certificate Policy Digital Signatures High Assurance is appropriate for all transactions with Government Entities in _____(state) that require authentication and /or a signature that require a high-level of assurance. The use of Certificate Policy Notary Digital Signatures is appropriate for all electronic notarizations in _____(state).

The State of _____ disclaims all liability for any use of a certificate issued by a CA in accordance with this policy and the ___ PKI.

Any disputes concerning key or certificate management under this policy are to be brought in the courts of the State of _____ and governed by the statutes and laws of the State of _____, without regard to conflicts of laws principles thereof. [**Commentary** - a state may, as appropriate, specify that any disputes concerning key or certificate management under this policy are to be resolved by the Parties concerned using an appropriate dispute settlement mechanism (i.e. through negotiation, mediation or arbitration).]

Certificates may be issued under this policy following authentication of a Subscriber's identity. Identification will be in the manner set out in this policy.

A CA will revoke certificates in the circumstances enumerated in this policy.

A CA is required to maintain records or information logs in the manner described in this policy.

A CA should ensure the separation of critical CA functions between at least three individuals assigned to distinct trusted roles.

Only Subscriber may posses, backup, or otherwise store Subscribers' Digital Signature private keys. Keys may have a validity period as indicated in this policy.

Confidentiality/Encryption private keys issued by a CA may be backed-up to protect against data loss or data corruption.

Applications that require recoverable encrypted messaging will employ Confidentiality/Encryption Certificate Policy, which defines confidentiality with key recovery for the encryption signature use. Such applications may also use a Digital Signature Certificate Policy, but only for a separate authentication signature and as long as there is no mingling of the two types of Certificates in a repository. Certificates based on the Digital Signature Certificate Policy rely on the Subscriber's sole possession to assert the right of Non-Repudiation and must not be mingled with any Certificates that allow recovery and thereby break the criteria of sole possession.

No information provided by a Subscriber to a CA shall be disclosed without the Subscriber's consent, unless required by law or court order.

CA activities are subject to inspection by the Policy Management Authority (PMA) or its agents at the discretion of the PMA.

1.2 Identification

The Policy Object Identifier Designation for this Policy is registered under the Policy Management Authority arc (e.g. for Arizona's basic digital signature, it is: { joint-iso-ccitt (2) country (16) us (840) state (3) AZ (04) EB (01) Secretary of State (002) DO (02) Policy Authority (999)} as OO (00) id-AESIpki-certpcy-sign-2 (002)). This policy has been designed for use in certain situations

and identifies specific roles to implement them. Certificate Authorities (CA), Registration Authorities (RAs), Local Registration Authorities (LRAs), Certificate Manufacturing Authority (CMA), the party responsible for the Repository, Subscribers and Relying Parties all have specific obligations which are outlined in this policy.

1.3 Community and Applicability

These certificate policies have been designed to satisfy general public key certificate requirements of the State of _____.

CAs participating in the ___ PKI are not obligated to issue, recognize or support all of the ___ PKI policies. They are also not limited to issuing certificates only in accordance with these policies. Any CA participating in the ___ PKI may issue, recognize or support additional certificate policies outside the scope of the ___ PKI.

A CA may subrogate responsibilities defined in this policy and other CA responsibilities to a third party who agrees to be bound by this policy. The CA remains responsible for subrogee performance in accord with this policy.

1.3.1 Certification Authorities (CAs)

The CA that issues certificates in accordance with this policy:

- Creates, signs, distributes and revokes Certificates binding the X.500 Distinguished Name of Subscribers and Registration Authorities with their respective signature verification key and their public encryption key;
- Promulgates certificate status through certificate revocation lists (CRLs) and, as appropriate, via the Online Certificate Status Protocol (OCSP) ;
- Has designed, implemented, and operated its certification practices to reasonably achieve the requirements of this Policy.

Specific CA practices and procedures implementing the requirements of this Policy shall be set forth by the CA in a certification practice statement ("CPS") or other publicly available document.

A cross-certification must be in accordance with requirements determined by the PMA. All cross-certification between Issuing CAs and CAs not participating in the ___ PKI will be done pursuant to instructions from the PMA.

An Issuing CA may issue cross certificates to other Issuing CAs where expressly authorized by the PMA.

1.3.2 Registration Authorities (RAs)

An RA operating under these certificate policies is responsible for all duties assigned to it by the Issuing CA.

An RA operating under these policies may perform duties on behalf of more than one CA, provided that the RA satisfies all the requirements of this CP for each CA. An Approved CA may subcontract Registration Authority functions to third party RAs who agree to be bound by this Policy, but the Approved CA remains responsible for the performance of those services in accordance with this Policy.

1.3.3 Local Registration Authorities (LRAs)

An LRA may perform duties on behalf of one or more CA, providing that in doing so it satisfies all the requirements of this CP.

1.3.4 Certificate Manufacturing Authorities (CMAs)

A Certificate Manufacturing Authority (CMA) may perform duties on behalf of more than one CA, provided that the RA satisfies all the requirements of this CP for each CA. An Approved CA may subcontract CMA functions to third party CMAs who agree to be bound by this Policy, but the Approved CA remains responsible for the performance of those services in accordance with this Policy.

1.3.3 Repositories

An Issuing CA shall perform the role and functions of the Repository. An Issuing CA may subcontract performance of the Repository functions to a third party Repository who agrees to be bound by this Policy, but an Issuing CA remains responsible for the performance and audit of those services in accordance with this Policy.

1.3.4 Subscribers

Subscribers for Digital Signature Certificates may be issued certificates for assignment to devices, organizational roles, or applications provided that responsibility and accountability for the certificate is attributable to an individual. See Section 3.1.10.

Subscribers for Confidentiality/Encryption Certificates may be issued certificates for assignment to devices, groups, organizational roles or applications provided that responsibility and accountability for the certificate is attributable to an individual or an organization.

Certificates in the ___ PKI may be issued after request or authorization for issuance from one or more Sponsors. Such certificates may be issued to employees, citizens, organizations or others with whom the Sponsor has a relationship.

Eligibility for a certificate is at the sole discretion of the Issuing CA. The CA may administer any number of Subscribers.

1.3.5 Relying Parties

A Relying Party may be either a Subscriber of the ___ PKI or a Subscriber of a PKI that has signed a cross-certification agreement with the ___ PKI.

By accepting a certificate issued pursuant to the provisions of this policy, including but not limited to, Section 2.1.4 and its subsections, a Relying Party agrees to be bound by the provisions of this policy.

1.3.6 Policy applicability

The policy applicability of each certificate is described below. The PMA will provide further clarification and guidance on the applicability of certificates for Government Entity use.

Confidentiality/Encryption Certificate Policy	Suitable for certificate uses such as confidentiality/encryption key establishment for information exchanged with Government Entities.
Digital Signature Medium and High Assurance Certificate Policies	Suitable for the integrity and authentication of government transactions that are satisfied by the authentication process as defined in Section 3.1.9 and key generation as defined in Section 6.1.8.

1.4 Contact Details

The _____ State PKI Policy Management Authority administers this certificate policy.
The contact person is:

PMA Administrator, _____ State PKI Policy Management Authority
(location)
Fax:
E-mail:

2. GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA obligations

The CA is responsible for all aspects of the issuance and management of a certificate, including control over the application and enrollment process, the identification and authentication process, the actual certificate manufacturing process, publication of the certificate, suspension and revocation of the certificate, and renewal of the certificate, and for ensuring that all aspects of the CA Services and CA operations and infrastructure related to certificates issued under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy.

The CA will operate in accordance with its CPS, this Certificate Policy, and the laws of _____ when fulfilling these obligations. The CA will take all reasonable measures to ensure that Subscribers and Relying Parties are aware of their respective rights and obligations with respect to the operation and management of any keys, Certificates or End-Entity hardware and software used within the framework established by this CP.

2.1.1.1 Representations By CA

By issuing a certificate that references this Policy, the CA certifies to the subscriber, and to all Relying Parties who reasonably and in good faith rely on the information contained in the certificate during its operational period and in accordance with this Policy, that:

(a) The CA has issued, and will manage, the certificate in accordance with this Policy, any applicable PMA regulations and any applicable state statute or regulations and that the certificate meets all material requirements of this Policy and the CA's CPS
(b) operate in accordance with its CPS, this CP, and the laws of the State of _____ when issuing and managing the keys provided to RAs and Subscribers under this CP;
(c) ensure that all CAs, Ras, LRAs, Repositories and Certificate Manufacturing Authorities operating on its behalf are aware of, and agree to abide by the stipulations in this policy that apply to them;
(d) have in place mechanisms and procedures that include written agreements (Subscriber agreements and Relying Party agreements) as approved by the PMA to ensure that Subscribers and Relying Parties (collectively known as End-Entities) are aware of, and agree to abide with, the stipulations in this policy that apply to them and their respective rights, obligations and liabilities, if any, with respect to the operation and management of any keys, certificates or End-Entity hardware and software connected with the PKI;
(e) There are no misrepresentations of fact in the certificate known to the CA, and the CA has taken reasonable steps to verify additional information in the certificate unless otherwise noted in its CPS
(f) Information provided by the subscriber in the certificate application for inclusion in the certificate has been accurately transcribed to the certificate
(g) maintain a statement in compliance with identified state statute reciting the CA's statutory obligation to maintain the confidentiality of personal information in accordance with the provisions of such statute.

The written agreements required by this section must include written notice to Subscribers and Relying Parties of any liability limitations relating to the CA's participation and performance in the ___ PKI. Such liability limitations must be stipulated to by the PMA. Such notice must, at a minimum, be provided within the CPS published by the CA and be accessible by Subscribers and Relying Parties. Notice of liability limitations may also be published in the Certificate either through a private Certificate extension or the use of the user Notice field within the Certificate as defined by PKIX. Because of space limitations within a Certificate, such notice may be limited to the following language: "Limited Liability. See CPS".

The written Subscriber agreements required by this section stipulate the series of events and their respective time periods necessary to issue a certificate to a subscriber.

CA personnel associated with PKI roles (e.g. PKI Administrators, PKI Master Users, and PKI Officers) must be individually accountable for actions they perform. "Individually accountable" means that there must be evidence that attributes an action to the person performing the action.

2.1.1.2 Notification of certificate issuance and revocation

An Issuing CA must make CRLs available to a Subscriber or Relying Party in accordance with 4.4. An Issuing CA must notify a Subscriber when a certificate bearing the Subscriber's DN is issued, suspended, reinstated, or revoked.

2.1.1.3 Accuracy of representations

When an Issuing CA publishes a certificate it certifies that it has issued a certificate to a Subscriber and that the information stated in the certificate was verified in accordance with this CP. Publication of the certificate in a repository, to which the Subscriber has access, constitutes notice of such verification.

The CA will provide to each Subscriber notice of the Subscriber's rights, obligations and liabilities, if any, under this Certificate Policy. Such notice will be in the form of an agreement as specified by the PMA. Such agreements will include, but not be limited to, a description of the allowed uses of certificates issued under this CP; the Subscriber's obligations concerning key protection; and procedures for communication between the Subscriber and the CA or RA, including communication of changes in service delivery or changes to this policy. Subscribers should also be notified as to procedures for dealing with suspected key compromise, certificate or key renewal, service cancellation, and dispute resolution.

The CA will ensure that any notice of the Subscriber's rights, obligations and liabilities, if any, under this Certificate Policy includes a description of a Relying Party's obligations with respect to use, verification and validation of certificates.

2.1.1.4 Time between certificate request and issuance

There is no stipulation for the period between the receipt of an application for a Certificate and the generation of the Entity's key material. The Issuing CA must ensure that the period for which the Entity has to complete its initialization process is no longer than _____ working days.
[**Commentary** – current practices vary, each state will need to evaluate their signing processes and define an appropriate time frame.]

2.1.1.5 Certificate revocation and renewal

The Issuing CA must ensure that any procedures for the expiration, revocation and renewal of a certificate will conform to the relevant provisions of this CP and will be expressly stated in the Subscriber Agreement and any other applicable document outlining the terms and conditions of the certificate use. The Issuing CA must ensure that the key changeover procedures are in accordance with 4.7. The Issuing CA will also ensure that notice of revocation of a certificate will be posted to the CRL within the time limits stated in 4.4.4 and 4.4.9. The address of the CRL must be defined in the certificate.

2.1.1.6 Protection of private keys

All Entities must ensure that their private keys and activation data are protected in accordance with 4 and 6 herein.

2.1.1.7 Restrictions on Issuing CA's private key use

An Issuing CA must ensure that its certificate signing private key is used only to sign certificates and CRLs. Such CA may issue certificates to Subscribers, CA and RA personnel, devices and applications. The CA may issue cross-certificates in accordance with 1.3.1.

An Issuing CA must ensure that private keys issued to its personnel to access and operate CA applications are used only for such purposes. If required, its personnel could be issued sets of Subscriber keys and certificates to be used for purposes other than CA use.

2.1.2 Repository Obligations

Certificates and CRLs must be available to Relying Parties in accordance with the requirements of 4.4.9.

2.1.3 Registration Authorities (RA) and Certificate Manufacturing Authorities (CMA) Obligations

The CA shall be responsible for performing all identification and authentication functions and all certificate manufacturing and issuing functions. However, the CA may delegate these functions to an identified Registration Authority (RA) and/or Certificate Manufacturing Authority (CMA) provided that the CA remains primarily responsible for the performance of those services by such third parties in a manner consistent with the requirements of this Policy.

2.1.4 LRA obligations (LRA duties)

Should the PMA allow a CA to use LRAs, the CA must ensure that all its LRAs comply with the provisions of this CP and the CA's CPS. The CA shall continue to be responsible for any matters delegated to an LRA.

A CA is responsible through its LRA personnel to bring to the attention of Subscribers all relevant information pertaining to the rights and obligations of the CA, LRA and Subscriber contained in this CP, the Subscriber agreement, if applicable, and any other relevant document outlining the terms and conditions of use.

LRA Administrators must be individually accountable for actions performed on behalf of the CA. (There must be evidence that attributes an action to the person performing the action for it to be individually accountable.) Records of all actions carried out in performance of LRA duties must identify the individual who performed the particular duty.

The LRA is not required to notify a Relying Party of the issuance or revocation of a certificate.

2.1.5 Subscriber Obligations

In all cases, the CA shall require the Subscriber to enter into an enforceable contractual commitment for the benefit of Relying Parties obligating the Subscriber to:

(a) Any information required to be submitted to an Issuing CA or RA in connection with a certificate must be complete and accurate.
(b) activate a key pair using a trustworthy system, and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key;
(c) acknowledge that by accepting the Certificate the Subscriber is warranting that all information and representations made by the Subscriber that are included in the Certificate are true;
(d) use the Certificate exclusively for authorized and legal purposes, consistent with this Policy;
(e) request the CA to revoke the Certificate promptly upon any actual or suspected compromise of the Subscribers private key.

2.1.6 Relying Party Obligations

A Relying Party has a right to rely on a Certificate that references this Policy only if the Certificate is used and relied upon for lawful purposes and under circumstances where:

(a) the reliance was reasonable and in good faith in light of all the circumstances known to the Relying Party at the time of reliance;
(b) the certificate is used for an appropriate purpose according to this policy;
(c) the Relying Party checked the status of the Certificate prior to reliance and it was valid. Reliance in the case of an inability to check the status shall be governed by any contract between the parties and by applicable statute.

2.1.7 Policy Management Authority Obligations

The Policy Authority is responsible for the terms of this Policy and its administration.

2.2 Certification Authority Liability

[**Commentary** – each state will need to define this section to fit their laws and the framework they intend to establish.]

An issuing CA will ensure that its practices and actions (including certification and repository services, issuance and revocation of certificates, and issuance of CRLs) are in accordance this CP. It will take reasonable efforts to ensure that all LRAs and Subscribers will know and follow the requirements of this policy when dealing with any certificates containing this policy's OID or the associated keys.

A CA is responsible to Relying Parties for direct damages suffered by such Relying Parties that are caused by the failure of the CA to comply with the terms of this Policy, and sustained by such Relying Parties as a result of reliance on a Certificate in accordance with this Policy, but only to the

extent that the damages result from the use of Certificates for a suitable applications listed as defined in this CP.

Except as expressly provided in this Policy and in its CPS, CA disclaims all other warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided.

2.3 Financial Responsibility

An Issuing CA and RA's shall provide the following financial assurances:

- An Issuing CA shall obtain and maintain a bond from a surety, in a form and amount as required by the PMA.
- An RA shall maintain adequate financial assurance in the form of a bond, guaranty or irrevocable letter of credit, in the form and amount deemed appropriate by the issuing CA.
- An Issuing CA shall maintain insurance coverage, naming the State of ____ as an additional insured, which will cover the Issuing CA, the State of _____, and their employees, officers, agents, subcontractors, designees, etc., including coverage for professional liability errors and omissions and crime coverage, in amounts as deemed appropriate by the PMA.

This insurance shall also cover any assessment of charges for the transfer and continuation of services (e.g. Repositories) not covered by the surety bond should the Certification Authority or any agent be unable to continue providing any service as required by this Certificate Policy or any related agreement. All coverages, conditions, limits and endorsements shall remain in full force and effect as required to act as an approved Certification Authority.

An Issuing CA may require that an RA maintain professional liability error and omissions and crime coverage insurance in adequate amounts and under terms consistent with the policy terms applicable to an Issuing CA, from an insurance company satisfactory to an Issuing CA.

The failure of an Issuing CA or RA to continuously maintain a required bond or insurance coverage may be the basis for revocation or suspension of its approval to issue certificates and may also be the basis for revocation of suspension or certificates previously issued.

2.3.1 Fiduciary Relationships

Nothing in this CP shall confer on any CA, RA, Subscriber, Relying Party, or any other third party, any authority to act for, bind, or create or assume any obligation or responsibility, or make any representation on behalf of the State. Issuance of certificates in accordance with this policy does not make an Issuing CA or any RA an agent, fiduciary, trustee or other representative of Subscribers or Relying Parties.

2.4 Interpretation and Enforcement

2.4.1 Governing law

The laws of the State of _____, excluding its conflict of laws rules and any applicable treaties, shall govern the construction, validity, interpretation, enforceability and performance of this CP, all Subscription Agreements and all Relying Party Agreements. Any dispute in respect to this CP or in respect to certificates Issued under this CP by an Issuing CA or any services provided by an Issuing CA in respect to certificates, shall be brought in the courts of the State of _____, and each person, entity, or organization hereby agrees that such courts shall have personal and exclusive jurisdiction over such disputes.

2.4.2 Severability, survival, merger, notice

A CA must ensure that any agreements by that CA relating to its operation within the ___ PKI will contain provisions governing severability, survival, merger and notice as approved by the PMA.

2.5 Fees

The PMA will determine the fees, if any, for any and all ___ PKI services.

CA shall not impose any fees on the reading of this Policy or the CA's CPS.

2.6 Publication and Repositories

An Issuing CA must:

- include within any certificate it issues the URL of a web site maintained by, or on behalf of, the CA;
- ensure the publication of this CP and its CPS, digitally signed by an authorized representative of the CA, on a web site maintained by, or on behalf, of the CA, the location of which must be indicated in compliance with 8;
- ensure, directly or through agreement with a repository, that operating system and repository access controls will be configured so that only authorized CA personnel can write or modify the online version of this CP and its CPS;
- provide a full text version of its CPS when necessary for the purposes of any audit, inspection, accreditation or cross-certification; and
- provide to the public the final opinion letter resulting from any audit performed and used to establish compliance with PMA audit requirements.

[**Commentary** – additional thoughts are included in an endnote[i]]

All information to be published in the Repository shall be published promptly after such information is available to the CA. Certificates issued by the CA that reference this Policy will be published promptly upon acceptance of such Certificate by the Subscriber.

2.7 Compliance Audit

A compliance audit determines whether a CA's performance meets the standards established in its CPS and satisfies the requirements of the CPs it supports.

The Policy Authority shall outline specific requirements for a compliance audit. These requirements will conform to any statutory or regulatory requirements of the State of _____.

Before initial approval as an Approved CA, and thereafter as deemed necessary by the PMA, the CA (and each RA, CMA, and Repository Services Provider [RSP], as applicable) shall submit to a compliance audit by an independent nationally recognized security audit firm that is approved by the Policy Authority as being qualified to perform such an audit and that has significant experience in the application of PKI and cryptographic technologies. The purpose of such audit shall be to verify that the CA and its delegated parties have a system in place:

- to assure the quality of the CA services provided,
- that the CA complies with all of the requirements of this Policy and its CPS, and
- that assures the CA's CPS is consistent with the requirements of this Policy and any related agreement with the PMA.

2.7.2 Identity/qualifications of CA auditor

Any person or entity, seeking to perform a compliance audit must be certified by a audit standards body with an audit process commonly recognized as appropriate for CA operations audit (e.g. a certified public accountant or firm) and possess significant experience with PKI and cryptographic technologies as well as the operation of relevant PKI software, as defined by the PMA.

2.7.3 Auditor's relationship to audited CA

The auditor must be independent of the CA.

2.7.4 Topics covered by audit

The compliance audit must comply with the commonly accepted industry requirements [**Commentary** – suggested framework is to specify one or both of these:

1. AICPA/CICA *WebTrust Program for Certification Authorities*;
2. Federal Information Processing Standards 140-1 "Security: Cryptographic Modules" Level 2 and TSEC (The Orange Book) C2 criteria or comply with contemporary Certification Authority security criteria as expressed in terms of the "Common Criteria" – ISO 15408-1:1999.]

2.7.5 Actions taken as a result of audit

The audit results must be submitted to the PMA. If irregularities are found, the CA must submit a report to the PMA as to any action the CA will take in response to the audit report. Where a CA fails to take appropriate action in response to the audit report, the PMA may:

- indicate the irregularities, but allow the CA to continue operations until the next programmed audit; or
- allow the CA to continue operations for a maximum of thirty days pending correction of any problems prior to revocation; or

- downgrade the assurance level of any cross-certificates; or
- revoke the CA's participation in the ___ PKI.

Any decision regarding which of these actions to take will be based on the severity of the irregularities.

2.7.6 Communication of results

CAs participating in the ___ PKI must provide the PMA with a copy of the results of the compliance audit. These full results will not be made public unless required by law. However, the final opinion letter resulting from an audit performed shall be made available to the public.

2.8 Confidentiality Policy

Information regarding subscribers that is submitted on applications for Certificates will be kept confidential by the CA and shall not be released without the prior consent of the Subscriber, unless otherwise required by law. This does not apply, however, to information appearing on certificates.

2.9 Intellectual Property Rights

The private key shall be treated as the sole property of the legitimate holder of the corresponding Public Key identified in a certificate. This CP and its OID are the property of the state of _____ and may be used by a CA participating in the ___ PKI as provided in this CP. Any other use of this CP and its OID without the express written permission of the PMA is expressly prohibited.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of names

Each Entity must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate Subject Name field and in accordance with PKIX Part 1. Each Entity may use an alternative name via the Subject Alternate Name field, which must also be in accordance with PKIX Part 1. The DN must be in the form of a X.501 printable String and must not be blank.

3.1.2 Need for names to be meaningful

The contents of each certificate Subject and Issuer name fields must have an association with the authenticated name of the Entity. In the case of individuals the Relative Distinguished Name (RDN) should be a combination of first name, surname, and optionally initials. In the case of other entities the RDN will reflect the authenticated legal name of the Entity. A certificate issued for a device or application must include within the DN the name of the person or organization responsible for that device or application.

3.1.3 Rules for interpreting various name forms

No stipulation.

3.1.4 Uniqueness of names

The subject name listed in a Certificate shall be unambiguous and unique for all certificates issued by the CA. and conform to X.500 standards for name uniqueness. If necessary, additional numbers or letters may be appended to the real name to ensure the name's uniqueness within the domain of certificates issued by the CA.

3.1.5 Name claim dispute resolution procedure

The CA reserves the right to make all decisions regarding Entity names in all assigned certificates. A party requesting a certificate must demonstrate its right to use a particular name. Where there is a dispute about a name in a repository not under its control, a CA must ensure that there is a name claim dispute resolution procedure in its agreement with that repository.

3.1.6 Recognition, authentication and roles of trademarks

The use of trademarks will be reserved to registered trademark holders.

3.1.7 Method to prove possession of private key

Prior to the issuance of a verification certificate the Issuing CA and End-Entity will confirm their respective identities through the use of a shared secret. The key transfer protocol described in PKIX Certificate Management Protocol is suitable for this requirement.

3.1.8 Authentication of organization identity

Confidentiality/Encryption Certificate	An individual or an organization authorized to act on behalf of the prospective Subscriber, may make an application for an organization to be a Subscriber. Identification and authentication of the prospective Subscriber must be through one of the following means: • the CA or RA must examine documentation providing evidence of the existence of the organization; • if a Government Entity has previously established the identity of the organization using a process that satisfies the PMA, and there have been no changes in the

	information presented, then the CA or RA and the prospective Subscriber may utilize privately shared information. The CA or RA must also verify the identity and authority of the individual or organization acting on behalf of the prospective Subscriber and their authority to receive the keys on behalf of that organization. The CA or RA must keep a record of the type and details of identification used.
Digital Signature Medium Assurance and High Assurance Certificates	Are **not** intended for use by organizations. Where the technology does not permit the independent generation of Digital Signature and Confidentiality/Encryption key pairs, the Digital Signature key pair shall not be used.

3.1.9 Authentication of individual identity

Another person or organization authorized to act on behalf of the prospective Subscriber may make an application for an individual to be a Subscriber. Identification and authentication of the individual must be through the following means:

Confidentiality/Encryption Certificate	• the CA or RA will compare the identity of the individual with two original pieces of identification. At least one of these must be government issued identification containing a photograph (e.g., driver's license, non-driver identification, passport); or • if the sponsoring Government Entity has previously established the identity of an individual using a process that satisfies the PMA, and there have been no changes in the information presented, then the CA or RA and the individual may utilize this privately shared information. The CA or RA must keep a record of the type and details of identification used.
Digital Signature Medium Assurance Certificate	• the CA or RA will compare the identity of the individual with two pieces of

	identification (certified copies or originals). At least one of these must be government issued identification containing a photograph (e.g., driver's license, non-driver identification, passport); or • . if the sponsoring Government Entity has previously established the identity of an individual using a process that satisfies the PMA, and there have been no changes in the information presented, then the CA or RA and the individual may utilize this privately shared information. The CA or RA must keep a record of the type and details of identification used.
Digital Signature High Assurance Certificate	• the CA or RA in the presence of the individual will compare the identity of the individual with two pieces of identification (certified copies or originals). At least one of these must be government identification containing a photograph (e.g., driver's license, non-driver identification, passport). The CA or RA must keep a record of the type and details of identification used.
Electronic Notary Digital Signature	• same requirements as for a Digital Signature High Assurance Certificate AND proof of appropriate notary commission

3.1.10 Authentication of devices or applications

An application for a device or application to be an End-Entity may be made by an individual or organization to which the device's or application's signature is attributable for the purposes of accountability and responsibility.

Identification and authentication of the applicant must follow 3.1.8 or 3.1.9 as if that individual or organization was applying for the certificate on its own behalf.

The CA or RA must also verify the identity of the individual or organization making the application and its authority to receive the keys for that device or application.

The CA or RA must keep a record of the type and details of identification used.

The CA shall establish that the applicant is in possession of the private key corresponding to the public key submitted with the application in accordance with an appropriate secure protocol, such as that described in the IETF PKIX Certificate Management Protocol.

3.2 Routine Rekey

Within three months prior to the scheduled expiration of the operational period of a Certificate issued following authentication under this Policy, a Subscriber may request issuance of a new Certificate for a new key pair from the CA that issued the original Certificate, provided the original Certificate has not been suspended or revoked. Such a request may be made electronically via a digitally signed message based on the old key pair in the original Certificate.

Renewal of an affiliated individual shall require verification that the affiliation still exists. Such verification of affiliation shall be the same as what is required for a new application.

A request for rekey may only be made by the Entity in whose name the keys have been issued. The CA must authenticate all requests for rekey, and the subsequent response must be authenticated by the Entity. This may be done by an on-line method in accordance with PKIX Part 3 – Certificate Management Protocol. An Entity requesting rekey may authenticate the request for rekey using its valid Digital Signature key pair. Where the keys have expired, the request for rekey must be authenticated in the same manner as the initial registration.

3.3 Rekey After Revocation -- No Key Compromise

Where the information contained in a certificate has changed or there is a known or suspected compromise of the private key, a CA must authenticate a re-key in the same manner as for initial registration. The CA or the RA authorized to act on behalf of that CA must verify any change in the information contained in a certificate or the RA authorized to act on behalf of that CA before that certificate is issued.

3.4 Revocation Request

A CA, or RA acting on its behalf, must authenticate a request for revocation of a certificate. A CA must establish and make publicly available the process by which it addresses such requests and the means by which it will establish the validity of the request. Requests for revocation of certificates must be logged.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

A CA must ensure that all procedures and requirements with respect to an application for a certificate are set out in the CPS or a publicly available document. Only Sponsors are permitted to make bulk applications on behalf of End-Entities. A CA must ensure that each application be accompanied by:

Confidentiality/Encryption Certificates	• Proof of the End Entity's identity; • Proof of authorization for any requested certificate attributes; • In the case of employees, an acknowledgment, or in the case of other Subscribers, a signed agreement, of the applicable terms and conditions governing their use of the certificate.
Digital Signature Medium Assurance and High Assurance Certificates	• Proof of the End-Entity's identity; • Proof of authorization for any requested certificate attributes; • In the case of employees, an acknowledgment, or in the case of other Subscribers, a signed agreement, of the applicable terms and conditions governing their use of the certificate; • A public verification key generated by the End-Entity.

An application for a certificate does not oblige a CA to issue a certificate.

4.1.1 Application for a cross-certificate

The PMA will identify the necessary procedures to apply for a cross-certificate.

An application for a cross-certificate does not oblige the PMA to authorize a cross-certificate. The PMA shall review any CA's request for cross-certification and approve or deny any such request according to established procedures.

A CA requesting cross-certification will include with the application:

- its Certificate Policy;
- an external audit inspection report validating the assurance level stated in the CP;
- the public verification key generated by the CA.

4.2 Certificate Issuance

Upon successful completion of the subscriber identification and authentication process in accordance with this Policy, and complete and final approval of the certificate application, the CA shall issue the requested Certificate, notify the applicant thereof, and make the Certificate available to the applicant pursuant to a procedure whereby the certificate is initially delivered to, or available for pickup by, the Subscriber only. A CA will not issue a Certificate without the consent of the applicant and, if applicable, the applicant's sponsor.

4.3 Certificate Acceptance

The CA shall contractually require that the Subscriber expressly indicate acceptance or rejection of the Certificate following its issuance, in accordance with procedures established by the CA and specified in the CPS.

There will be a short time period when the Subscriber must act to accept, once the time has expired, the Certificate will be revoked and the Subscriber will have to begin a new application.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for revocation

A Subscriber may request revocation of their individual Certificate at any time for any reason.

A sponsoring organization may, where applicable, request revocation of an affiliated individual Certificate at any time for any reason. This includes revocation of a Notary Signature Certificate if the notary commission has expired or has been revoked.

The issuing CA may also revoke a Certificate upon failure of the Subscriber (or any sponsoring organization, where applicable) to meet its obligations under this Certificate Policy, the applicable CPS, or any other agreement, regulation, or law applicable to the Certificate that may be in force. This includes revoking a Certificate when a suspected or known compromise of the private key has occurred.

The PMA may, at its discretion, revoke a cross-certificate when a CA fails to comply with obligations set out in this CP, any agreement or any applicable law.

A certificate must be revoked:

- when any of the information in the certificate changes;
- upon suspected or known compromise of the private key;
- upon suspected or known compromise of the media holding the private key.

The CA in its discretion may revoke a certificate when an Entity fails to comply with obligations set out in this CP, the CPS, any agreement or any applicable law.

4.4.2 Who can request revocation

The revocation of a certificate may only be requested by:

- the Subscriber in whose name the certificate was issued;
- the individual or organization that made the application for the certificate on behalf of a device or application;
- the Sponsor whenever an affiliated individual is no longer affiliated with the Sponsor;

- the state agency responsible for commissioning notaries may revoke Notary Electronic Certificates;
- personnel of the Issuing CA if the CA determines that the certificate was not properly issued in accordance with this Policy and/or any applicable CPS;
- personnel of an RA associated with the Issuing CA if the CA determines that the certificate was not properly issued in accordance with this Policy and/or any applicable CPS.

The revocation of a cross-certificate may only be requested by:

- the CA on whose behalf the cross-certificate was issued;
- the PMA.

In the event that the CA ceases operations, all Certificates issued by the CA shall be revoked prior to the date that the CA ceases operations.

4.4.3 Procedure for revocation request

A CA must ensure that all procedures and requirements with respect to the revocation of a certificate are set out in the CPS or otherwise made publicly available. An authenticated revocation request, and any resulting actions taken by the CA, must be recorded and retained. In the case where a certificate is revoked, full justification for the revocation must also be documented. Where an Entity certificate is revoked, the revocation will be published in the appropriate CRL. Where a cross-certificate is revoked the revocation will be published in the ARL of the Issuing CA.

A revocation request that is submitted electronically with a digital signature based on the old private key is considered authenticated upon receipt.

4.4.4 Revocation request grace period

Any action taken as a result of a request for the revocation of a certificate must be initiated immediately if the request is received during _____ State local business hours of the CA or within the following:

Confidentiality/Encryption Certificate	Twenty-four (24) hours of receipt
Digital Signature Medium Assurance Certificate	Twelve (12) hours of receipt
Digital Signature High Assurance Certificate	Initiated immediately upon receipt

4.4.5 Circumstances for suspension

If a CA or RA receives notification from a Subscriber or Sponsor that there is cause to revoke a certificate using the criteria stated in 4.4.1, but the authenticity of the request cannot be immediately verified by the CA or RA, the CA or RA may initiate a certificate suspension. A revocation request that is submitted electronically with a digital signature based on the old key pair is subject to prompt revocation once authenticated based on that key pair.

4.4.6 Who can request

A CA or RA may initiate a certificate suspension.

4.4.7 Procedure for suspension request

The procedures for issuing a certificate suspension request must be published in the CA's CPS.

The CA must either revoke or reinstate the suspended certificate during the suspension period and publish the status changes resulting from the suspension and its subsequent revocation or reinstatement.

4.4.8 Limits on suspension period

The suspension period may not exceed two (2) working days.

4.4.9 CRL issuance frequency

A CA must ensure that it issues an up to date CRL as follows:

Confidentiality/Encryption Certificates	At least every twenty-four hours
Digital Signature Medium Assurance Certificate	At least every twelve hours
Digital Signature High Assurance Certificate	At least every four hours

A CA must also ensure that its CRL issuance is synchronized with any directory synchronization to ensure the accessibility of the most recent CRL to Relying Parties. When a certificate is revoked due to key compromise the updated CRL must be issued immediately.

4.4.10 CRL checking requirements

A Relying Party must either check the status of all certificates in the certificate validation chain against the current CRLs and ARLs, or use an alternative method for certificate status validation as defined in this policy, prior to their use. When CRLs and ARLs are validated a Relying Party must also verify the authenticity and integrity of CRLs and ARLs.

4.4.11 On-line revocation/status checking availability

As an alternative to CRL-checking, an on-line revocation-checking transaction to a trusted server, if available, may be used in accordance with the On-line Certificate Status Protocol (OCSP) as defined in the IETF X.509 Internet Public Key Infrastructure Online Certificate Status Protocol.

Whenever an on-line Certificate status database is used as an alternative to a CRL, such database shall be updated immediately after revocation or suspension.

4.4.12 On-line revocation checking requirements

Where on-line revocation/status checking is available and used by Relying Parties as an alternative to CRL checking, a Relying Party must check the status of all certificates in the certificate validation chain prior to their use. A Relying Party must also verify the authenticity and integrity of certificate status check responses received from an OCSP responder.

4.4.13 Other forms of revocation advertisements available

No stipulation.

4.4.14 Checking requirements for other forms of revocation advertisements

Not applicable.

4.4.15 Special requirements re-key compromise

In the event of the compromise, or suspected compromise, of a CA signing key, the CA must immediately notify all CAs to whom it has issued cross-certificates and the PMA. In the event of the compromise, or suspected compromise, of any other Entity's signing key, an Entity must notify the Issuing CA immediately. An Issuing CA must ensure that its CPS or a publicly available document and appropriate agreements contain provisions outlining the means it will use to provide notice of compromise or suspected compromise.

4.5 Security Audit Procedures

4.5.1 Types of event recorded

A CA should record in audit log files all events relating to the security of the CA system. These include such events as:

- system start-up and shutdown;
- CA application start-up and shutdown;
- attempts to create, remove, set passwords or change the system privileges of the PKI Master Officer, PKI Officer, or PKI Administrator;
- changes to CA details and/or keys;
- changes to certificate creation policies e.g., validity period;
- login and logoff attempts;
- unauthorized attempts at network access to the CA system;
- unauthorized attempts to access system files;
- generation of own and subordinate Entity keys;

- creation, suspension and revocation of certificates;
- attempts to initialize remove, enable, and disable Subscribers, and update and recover their keys;
- failed read-and-write operations on the certificate and CRL directory.

All logs, whether electronic or manual, should contain the date and time of the event, and the identity of the entity which caused the event.

A CA should also collect and consolidate, either electronically or manually, security information not CA-system generated such as:

- physical access logs;
- system configuration changes and maintenance;
- personnel changes;
- discrepancy and compromise reports;
- records of the destruction of media containing key material, activation data, or personal Subscriber information.

A CA must ensure that the CPS indicates what information is logged.

To facilitate decision-making, all agreements and correspondence relating to CA services should be collected and consolidated, either electronically or manually, in a single location.

4.5.2 Frequency of audit log processing

A CA must ensure that CA personnel review its audit logs at least once every week and all significant events are explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Supporting manual and electronic logs from the CA and RA should be compared where any action is deemed suspicious. Actions taken following these reviews must be documented.

4.5.3 Retention period for audit log

A CA must retain its audit logs onsite for three database/master file backup cycles or at least two months, whichever is longer, and subsequently retain them in the manner described in 4.6.

4.5.4 Protection of audit log

The electronic audit log system must include mechanisms to protect the log files from unauthorized viewing, modification, and deletion. Manual audit information must be protected from unauthorized viewing, modification, and destruction.

4.5.5 Audit log back-up procedures

Audit logs and audit summaries must be backed up or copied if in manual form.

4.5.6 Audit collection system

A CA must identify its audit collection systems in the CPS.

4.5.7 Notification to event causing subject

Where an event is logged by the audit collection system no notice need be given to the individual, organization, device or application that caused the event.

4.5.8 Vulnerability assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. The CA must ensure that a vulnerability assessment is performed, reviewed and revised following an examination of these monitored events.

4.6 Records Archival

4.6.1 Types Of Records Archived

The following data and files must be archived by or on behalf of the CA:

- Certification Practice Statement (CPS)
- Contractual obligations
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- Revocation requests
- Subscriber identity Authentication data as per Section 3.1.9
- Documentation of receipt and acceptance of certificates
- Documentation of receipt of tokens
- All certificates issued or published
- CA Re-key
- All CARLs and CRLs issued and/or published
- All Audit Logs
- Other data or applications to verify archive contents
- Documentation required by compliance auditors
- Final opinion letter resulting from a compliance audit

A second copy of all material retained or backed up must be stored in a location other than the CA site and must be protected either by physical security alone, or a combination of physical and cryptographic protection. Any such secondary site must provide adequate protection from environmental threats such as temperature, humidity and magnetism.

A CA should verify the integrity of the back-ups once every six months.

Material stored off-site must be periodically verified for data integrity.

4.6.2 Retention Period For Archive

Archive of the key and certificate information must be retained for at least 30 years. Archives of the audit trail log files must be retained for at least six (6) months.

Any signed document may also have public records retention requirements that must also be met.

4.6.3 Protection Of Archive

The archive media must be protected either by physical security alone, or a combination of physical security and cryptographic protection. This protection must meet or exceed State of _____ and Agency electronic records retention requirements for such material.

4.6.4 Archive Backup Procedures

Adequate backup procedures must be in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies will be readily available within a short period of time.

4.6.5 Archive Collection System (Internal Or External)

No stipulation.

4.6.6 Procedures To Obtain And Verify Archive Information

During the compliance audit required by this Policy, the auditor shall verify the integrity of the archives.

4.7 Key Changeover

A Subscriber may only apply to renew his or her key pair within three months prior to the expiration of one of the keys, provided the previous certificate has not been revoked. A Subscriber, the CA, or the RA may initiate this key changeover process. Automated key changeover is permitted. A CA must ensure that the details of this process are indicated in its CPS.

Subscribers without valid keys must be re-authenticated by the CA or RA in the same manner as the initial registration.

Where a Subscriber's certificate has been revoked as a result of non-compliance, the CA must verify that any reasons for non-compliance have been addressed to its satisfaction prior to certificate re-issuance. Keys may not be renewed using an expired Digital Signature key.

4.8 Compromise and Disaster Recovery

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

A CA must establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data. Where a repository is not under the control of the CA, a CA must ensure any agreement with the repository provides that business continuity procedures be established and documented by the repository.

[**Commentary** – the PMA may wish to require specific actions, an example is in an endnote[ii]]

4.8.2 Entity public certificate is revoked (Key Compromise Plan)

In the event of the need for revocation of a Confidentiality/Encryption certificate, the CA must include the Certificate serial number on an appropriate CRL.

The CA must have in place an appropriate key compromise plan that addresses the procedures that will be followed in the event of a compromise of the private signing key used by the CA to issue Certificates, or used by any higher level CA. Such plan shall include procedures for revoking all affected Certificates and promptly notifying all Subscribers and all Relying Parties.

In the event of the need for revocation of a CA's Digital Signature certificate, the CA must immediately notify:

- the PMA;
- all CAs to whom it has issued cross-certificates;
- all of its RAs;
- all Subscribers;
- all individuals or organizations that are responsible for a certificate used by a device or application.

The CA must also:

- publish the certificate serial number on an appropriate CRL;
- revoke all cross-certificates signed with the revoked Digital Signature certificate. After addressing the factors that led to revocation, the CA may:
  - generate a new CA signing key pair;
  - re-issue certificates to all Entities and ensure all CRLs and ARLs are signed using the new key.

In the event of the need for revocation of any other Entity's Digital Signature certificate see 4.4.

4.8.2.1 Entity or CA public certificate is downgraded

This section is not applicable to Confidentiality/Encryption Certificates.

In the event of the need for the downgrade of a CA's Digital Signature certificate, the CA must immediately notify:

- the PMA;

- all CAs to whom it has issued cross-certificates;
- all of its RAs;
- all Subscribers;
- all individuals or organizations that are responsible for a certificate used by a device or application.

Prior to re-establishing cross-certification a CA must also:
- request revocation of cross-certificates issued to the CA;
- revoke all certificates signed with the higher assurance key;
- provide appropriate notice (see 4.8.2);
- generate a new CA signing key pair;
- re-issue certificates to all Entities and ensure all CRLs and ARLs are signed using the new key.

In the event of the need for downgrade of any other Entity's Digital Signature certificate the CA or RA must notify the Subscriber in a manner set out in its CPS and the subscriber agreement.

4.8.3 Entity key is compromised

In the event of the compromise, or suspected compromise, of a decryption private key, the CA must notify the PMA immediately.

A CA must ensure that its CPS and appropriate agreements contain provisions outlining the means it will use to provide notice of compromise or suspected compromise.

In the event of the compromise of a CA's Digital Signature key, prior to re-certification within the ___ PKI, a CA must:
- request revocation of cross-certificates issued to the CA;
- revoke all certificates issued using that key;
- provide appropriate notice (see 4.8.2).

After addressing the factors that led to key compromise, the CA may:
- generate a new signing key pair;
- re-issue certificates to all Entities and ensure all CRLs and ARLs are signed using the new key.

In the event of the compromise, or suspected compromise, of any other Entity's Digital Signature key, the Entity must notify the Issuing CA immediately. A CA must ensure that its CPS and appropriate agreements contain provisions outlining the means it will use to provide notice of compromise or suspected compromise.

4.8.4 Secure facility after a natural or other type of disaster

A CA must establish a disaster recovery plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster. Where a repository is not under the

control of the CA, a CA must ensure that any agreement with the repository provides that a disaster recovery plan be established and documented by the repository.

[**Commentary** – the PMA may wish to require specific actions, an example is in an endnote for 4.8.1]

4.9 CA Termination

In the event that a CA ceases operation, it must notify the PMA and its Subscribers immediately upon the termination of operations and arrange with the PMA for the continued retention of the CA's keys and information. It must also notify all CA's with whom it is cross-certified.

In the event of a transfer of a CA's operations to another CA operating at a lower level of assurance the certificates issued by the CA whose operations are being transferred must be revoked through a CRL signed by that CA prior to the transfer.

In the event that the CA ceases operation, all Subscribers, sponsoring organizations, RAs, CMAs, RSPs, and Relying Parties will be promptly notified of the termination. In addition, all CAs with which cross-certification agreements are current at the time of cessation will be promptly informed of the termination. All certificates issued by the CA that reference this Policy will be revoked no later than the time of termination. All current and archived CA identity proofing, certificate, validation, revocation/suspension, renewal, policy and practices, billing, and audit data shall be transferred to the PMA (or designate) within 24 hours of CA cessation and in accordance with this Policy. Transferred data shall not include any non-ESI data. No key recovery enabled repository data will be commingled with this data.

The CA archives must be retained in the manner and for the time indicated in 4.6.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Security Controls

5.1.1 & 5.1.2 Site location, construction and physical access

The CA site must:

- be manually or electronically monitored for unauthorized intrusion at all times;
- ensure unescorted access to the CA server is limited to those personnel identified on an access list;
- ensure personnel not on the access list are properly escorted and supervised;
- ensure a site access log is maintained and inspected periodically; and
- ensure all removable media and paper containing sensitive plaintext information are stored in secure containers.

All RA sites or RA workstations used for on-line Entity management with the CA must be located in areas that satisfy the following controls:

Confidentiality/Encryption Certificate	• Activity is monitored by the personnel, who work there, by other personnel or by security staff. • Access by the public is limited to specific times of the day or for specific reasons. • Entry beyond the reception area is indicated by a recognizable perimeter such as a doorway or an arrangement of furniture and dividers in an open office environment.
Digital Signature Medium Assurance Certificate	The above requirements and • all media security protected when unattended, or • access is limited to personnel who work there and to properly escorted visitors.
Digital Signature High Assurance Certificate	• Monitored manually or electronically for unauthorized intrusion at all times; • Ensure unescorted access to the CA server is limited to those personnel identified on an access list; • Ensure personnel not on the access list are properly escorted and supervised; • Ensure a site access log is maintained and inspected periodically; and • Ensure all removable media and paper containing sensitive plaintext information are stored in secure containers.

The CA will ensure the operation of the RA site provides appropriate security protection of the cryptographic module, all system software and the RA Administrator's private key. The CA must conduct a threat and risk assessment. For example, the cryptographic module and the RA Administrator's private key could be stored in a secure container or safe.

Where a PIN or password is recorded, it must be stored in a security container accessible only to authorized personnel.

Subscribers must not leave their workstations unattended when the cryptography is in an unlocked state (i.e., when the PIN or password has been entered). A workstation that contains private keys on a hard drive must be physically secured or protected with an appropriate access control product.

In addition, for Digital Signature High Assurance Certificates, the required Subscriber's hardware cryptomodule must be protected physically. This may be done through site protection or by being kept with the Subscriber.

5.1.3 Power and air conditioning

A CA must ensure that the power and air conditioning facilities are sufficient to support the operation of the CA system.

5.1.4 Water exposures

A CA must ensure that the CA system is protected from water exposure.

5.1.5 Fire prevention and protection

A CA must ensure that the CA system is protected with a fire suppression system.

5.1.6 Media storage

A CA must ensure that storage media used by the CA system is protected from environmental threats such as temperature, humidity and magnetism.

5.1.7 Waste disposal

All media used for the storage of information such as keys, activation data or CA files is to be sanitized or destroyed before released for disposal.

5.1.8 Off-site back-up

A CA must ensure that facilities used for off-site back-up, if any, have the same level of security as the primary CA site.

5.2 Procedural Controls

5.2.1 Trusted Roles

5.2.1.1 CA trusted roles

A CA must ensure a separation of duties for critical CA functions to prevent one person from maliciously using the CA system without detection. Each user's system access is to be limited to those actions that they are required to perform in fulfilling their responsibilities.

A CA must provide for a minimum of three distinct PKI personnel roles, distinguishing between day-to-day operation of the CA system, the management and audit of those operations and the management of substantial changes to requirements on the system including its policies, procedures or personnel. The division of responsibilities between the three roles is as follows:

PKI Master User

- configuration and maintenance of the CA system hardware and software;
- commencement and cessation of CA services.

PKI Officer

- management of PKI Operators and other PKI Officers;
- configuring CA security policies;
- verification of audit logs;
- verification of CP and CPS compliance.

PKI Administrator

- management of PKI Operators;
- configuring CA security policies;
- verification of audit logs;
- verification of CP and CPS compliance;
- management of Subscriber initialization process;
- creation, renewal or revocation of certificates;
- distribution of tokens (where applicable).

An alternative division of responsibilities that provides the same degree of resistance to insider attack may be acceptable.

Only those personnel responsible for the duties outlined above are allowed access to the software that controls the CA operation.

5.2.1.2 RA trusted roles

A CA must ensure that RA personnel understand their responsibility for the identification and authentication of prospective Subscribers and perform the following functions:

- acceptance of subscription, certificate change, certificate revocation and key recovery requests;
- verification of an applicant's identity and authorizations;
- transmission of applicant information to the CA;
- provision of authorization codes or other initialization data for on-line key exchange and certificate creation where applicable.

A CA may permit all duties for RA functions to be performed by one individual.

5.2.2 Number of persons required per task

Confidentiality/Encryption Certificates	A CA must ensure that no single individual may gain access to Subscriber private keys stored by the CA. At a minimum two individuals, preferably using a split-knowledge technique, such as twin passwords, must perform any key recovery operation. Multi-user control is also required for CA key generation as outlined

	in 6.2.2. A CA must ensure that any verification process it employs provides for oversight of all activities performed by privileged CA role holders.
Digital Signature Medium Assurance and High Assurance Certificates	Multi-user control is also required for CA key generation as outlined in 6.2.2. An individual operating alone may perform all other duties associated with CA roles. A CA must ensure that any verification process it employs provides for oversight of all activities performed by those holding PKI personnel roles.

5.2.3 Identification and authentication for each role

All CA personnel must have their identity and authorization verified before they are:

- included in the access list for the CA site;
- included in the access list for physical access to the CA system;
- given a certificate for the performance of their CA role
- given an account on the PKI system.

- Each of these certificates and accounts (with the exception of CA signing certificates) must:
- be directly attributable to an individual;
- not be shared;
- be restricted to actions authorized for that role through the use of CA software, operating system and procedural controls.

CA operations must be secured, using mechanisms such as token-based strong authentication and encryption, when accessed across a shared network.

5.3 Personnel Security Controls

A CA must ensure that all personnel performing duties with respect to the operation of a CA or RA must:

- be appointed in writing;
- be bound by contract or statute to the terms and conditions of the position they are to fill;
- have received comprehensive training with respect to the duties they are to perform;
- be bound by statute or contract not to disclose sensitive CA security-relevant information or Subscriber information; and
- not be assigned duties that may cause a conflict of interest with their CA or RA duties.

5.3.1 Background, qualifications, experience, and clearance requirements

A CA must formulate and follow personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in manner consistent with this Policy.

5.3.2 Background check procedures

CAs shall conduct an appropriate investigation of all personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary), to verify their trustworthiness and competence in accordance with the requirements of this Policy and CA's personnel practices or equivalent. All personnel who fail an initial or periodic investigation shall not serve or continue to serve in a trusted role. The PMA may establish additional requirements conforming to state law and policy.

5.3.3 Training requirements

A CA must ensure that all personnel performing duties with respect to the operation of a CA or RA must receive comprehensive training in:

- the CA/RA security principles and mechanisms;
- all PKI software versions in use on the CA system;
- all PKI duties they are expected to perform; and
- disaster recovery and business continuity procedures.

All CA, RA, CMA, and RSP personnel must receive proper training in order to perform their duties, and update briefings thereafter as necessary to remain current.

5.3.4 Retraining frequency and requirements

The requirements of 5.3.3 must be kept current to accommodate changes in the CA system. Refresher training must be conducted as required, and the CA must review these requirements at least once a year.

5.3.5 Job rotation

No stipulation.

5.3.6 Sanctions for unauthorized actions

In the event of actual or suspected unauthorized action by a person performing duties with respect to the operation of a CA or RA, a CA may suspend his or her access to the CA system.

5.3.7 Contracting personnel

CA must ensure that contractor access to the CA site is in accordance with 5.1.1.

5.3.8 Documentation supplied to personnel

A CA must make available to its CA, RA, CMA, and RSP personnel the certificate policies it supports, its CPS, and any specific statutes, policies or contracts relevant to their position.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

Confidentiality/Encryption Certificates	Each confidentiality/encryption key pair must be generated using a PMA-approved algorithm.
Digital Signature Medium Assurance and High Assurance Certificates	Each prospective certificate holder must generate its own Digital Signature key pair using a PMA-approved algorithm.

6.1.2 Private key delivery to Entity

Confidentiality/Encryption Certificates	If the private decryption key is not generated by the prospective certificate holder it must be either delivered to the Entity in an on-line transaction in accordance with PKIX-3 Certificate Management Protocol, or via an equally secure manner approved by the PMA.
Digital Signature Medium Assurance and High Assurance Certificates	Not applicable.

6.1.3 Public key delivery to certificate issuer

The public verification key must be delivered to the CA either via an on-line transaction in accordance with the PKIX-3 Certificate Management Protocol, or via an equally secure manner approved by the PMA.

6.1.4 CA public key delivery to users

The CA key must deliver the public verification to the prospective certificate holder in an on-line transaction in accordance with PKIX-3 Certificate Management Protocol, or via an equally secure manner approved by the PMA.

6.1.5 Asymmetric key sizes

A CA must ensure that the key pairs for all PKI entities must be either 1024 bit RSA or DSA or 2048 bit RSA.

6.1.6 Public key parameters generation

A CA that utilizes the DSA must generate parameters in accordance with FIPS 186.

6.1.7 Parameter quality checking

Not applicable.

6.1.8 Hardware/software key generation

Confidentiality/Encryption Certificates	Key pairs for all Entities may be generated in a software or hardware cryptographic module.
Digital Signature Medium Assurance Certificates	CA Digital Signature key pairs must be generated in a hardware cryptographic module. Key pairs for all other Entities may be generated in a software or hardware cryptographic module.
Digital Signature High Assurance Certificates	The generation of Digital Signature keys for all Entities must be generated in a hardware cryptographic module.

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

Confidentiality/Encryption Certificates	Keys may be used for exchange and establishment of keys used for session and data confidentiality/encryption. The certificate KeyUsage field must be used in accordance with PKIX-1 Certificate and CRL Profile. One of the following Key Usage values must be present in all certificates: Key Encipherment, or data Encipherment. No other values may be present.
Digital Signature Medium Assurance and High Assurance Certificates	Keys may be used for authentication, non-repudiation and message integrity. They may also be used for session key establishment. CA signing keys are the only keys permitted to be used for signing certificates and CRLs. The certificate Key Usage field must be used in accordance

	with PKIX-1 Certificate and CRL Profile. One of the following Key Usage values must be present in all certificates: Digital Signature or Non-Repudiation. One of the following additional values must be present in CA certificate-signing certificates: Key Cert Sign, or CRL Sign.

6.2 Private Key Protection

The certificate holder must protect its private keys from disclosure.

6.2.1 Standards for crypto-module

Refer to 6.8.

6.2.2 Private key multi-person control

There must be multiple person control for CA key generation operations. For Confidentiality/Encryption Certificates there must be multiple person control for private key recovery. Two staff, performing duties associated with the roles of PKI Master User or PKI Officer positions, must participate or be present.

6.2.3 Private key escrow

Digital Signature private keys must not be escrowed.

6.2.4 Private key back-up

Confidentiality/Encryption Certificates	The Issuing CA must back-up private keys. The Entity may also make a back-up of the key. Backed-up keys must be stored in encrypted form and protected at a level no lower than stipulated for the primary version of the key.
Digital Signature Medium Assurance and High Assurance Certificates	An Entity may optionally back-up its own Digital Signature private key. If so, the keys must be copied and stored in encrypted form and protected at a level no lower than stipulated for the primary version of the key.

6.2.5 Private key archival

No stipulation.

6.2.6 Private key entry into cryptographic module

Confidentiality/Encryption Certificates	If the private decryption key is not generated in the Entity's cryptographic module, it must be either entered into the module in accordance with PKIX-3 Certificate Management Protocol, or via an equally secure manner approved by the PMA.
Digital Signature Medium Assurance and High Assurance Certificates	Not permissible.

6.2.7 Method of activating private key

The Entity must be authenticated to the cryptographic module before the activation of the private key. This authentication may be in the form of a password. When deactivated, private keys must be kept in encrypted form only.

6.2.8 Method of deactivating private key

When keys are deactivated they must be cleared from memory before the memory is de-allocated. Any disk space where keys were stored must be over-written before the space is released to the operating system. The cryptographic module must automatically deactivate the private key after a pre-set period of inactivity.

6.2.9 Method of destroying private key

Upon termination of use of a private key, all copies of the private key in computer memory and shared disk space must be securely destroyed by over writing. The method of over writing must be approved by the PMA. Private key destruction procedures must be described in the CPS or other publicly available document.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

Refer to 4.6.

6.3.2 Usage periods for the public and private keys

Confidentiality/Encryption Certificates	All keys (1024 bits) must have validity periods of no more than ____ years.
Digital Signature Medium Assurance Certificates	1024 bit keys must have validity periods of no more than ____ years. 2048 bit keys must have validity periods of no more than ____ years.

Digital Signature High Assurance Certificates	All keys (2048 bits) must have validity periods of no more than ____ years.

[**Commentary** – each state will need to define an appropriate validity period]

Restrictions On CA's Private Key Use

The CA's signing key used for issuing certificates that conform to this Policy shall be used only for signing certificates and, optionally, CRLs.

A private key used by an RA or RSP for purposes associated with its RA or RSP function shall not be used for any other purpose without the express permission of the CA.

A private key held by a CMA and used for purposes of manufacturing certificates for the CA is considered the CA's signing key, is held by the CMA as a fiduciary for the CA, and shall not be used for any reason without the express permission of the CA. Any other private key used by a CMA for purposes associated with its CMA function shall not be used for any other purpose without the express permission of the CA.

6.4 Activation Data

6.4.1 Activation data generation and installation

Any activation data must be unique and unpredictable. The activation data, in conjunction with any other access control, must have an appropriate level of strength for the keys or data to be protected. Where passwords are used, an Entity must have the capability to change its password at any time.

6.4.2 Activation data protection

Data used for Entity initialization must be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms.

The private keys of Entities must be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms. The level of protection must be adequate to deter a motivated attacker with substantial resources. If a reusable password scheme is used, the mechanism should include a facility to temporarily lock the account after a predetermined number of login attempts.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

Each CA server must include the following functionality:

Confidentiality/Encryption Certificates Digital Signature Medium Assurance Certificates	• access control to CA services and PKI roles; • enforced separation of duties for PKI roles; • identification and authentication of PKI roles and associated identities; • object re-use or separation for CA random access memory; • use of cryptography for session communication and database security; • archival of CA and End-Entity history and audit data; • audit of security related events; • self-test of security related CA services; • trusted path for identification of PKI roles and associated identities; • recovery mechanisms for keys and the CA system.
Digital Signature High Assurance Certificates	All of the above functionality and: • enforcement of domain integrity boundaries for security critical processes.

This functionality may be provided by the operating system, or through a combination of operating system, PKI CA software, and physical safeguards.

6.5.2 Computer security rating

Computer Security Rating (CC Evaluation level) TBD. NSA or another accredited third party laboratory must evaluate the security critical elements of the CA. Such an evaluation must include system-level analysis.

6.6 Life Cycle Security Controls

6.6.1 System development controls

Confidentiality/Encryption Certificates	The CA must use software that has been designed and developed by a formal methodology and supported by configuration management tools. The CA software must have third party verification of process compliance.

Digital Signature Medium Assurance and High Assurance Certificates	The CA must use CA software that has been designed and developed under development methodology such as MIL-STD-498, the System Security Engineering Capability Maturity Model (SSE CMM), or Information Systems Security Engineering Handbook. The design and development process must be supported by third party verification of process compliance and on-going Threat Risk Assessments to influence security, safeguard design and minimize residual risk.

6.6.2 Security management controls

Confidentiality/Encryption Certificates	The configuration of the CA system as well as any modifications and upgrades must be documented and controlled. There must be a method of detecting unauthorized modification to the CA software or configuration. The CA must ensure that it has a configuration management process in place to support the evolution of the CA system. Notice to PMA about significant changes.
Digital Signature Medium Assurance Certificates	A formal configuration management methodology must be used for installation and ongoing maintenance of the CA system. The CA software, when first loaded, must provide a method for the CA to verify that the software on the system: • originated from the software developer; • has not been modified prior to installation; and • is the version intended for use. The CA must provide a mechanism to periodically verify the integrity of the software. The CA must also have mechanisms and policies in place to control and monitor the configuration of the CA system. Upon installation, and at least once a week, the

	integrity of the CA system must be validated.
Digital Signature High Assurance Certificates	Same as above except, upon installation, and at least once every 24 hours, the integrity of the CA system must be validated.

6.7 Network Security Controls

The CA server must be protected from attack through any open or general-purpose network with which it is connected. Such protection must be provided through the installation of a device configured to allow only the protocols and commands required for the operation of the CA. A CA must ensure that its CPS defines those protocols and commands required for the operation of the CA.

6.8 Cryptographic Module Engineering Controls

Confidentiality/Encryption Certificates	All CA cryptographic operations must be performed in a cryptographic module validated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance. All RA's cryptographic operations must be performed in a cryptographic module validated to at least FIPS 140-1 Level 1 or otherwise verified to an equivalent level of functionality and assurance. End Entities must use cryptographic modules validated to FIPS 140-1 level 1 or otherwise verified to an equivalent level of functionality and assurance.
Digital Signature Medium Assurance Certificates	All CA Digital Signature key generation, CA Digital Signature key storage and certificate signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance. All other CA cryptographic operations must be performed in a cryptographic module validated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality.

	The RA Administrator Digital Signature key generation and signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-1 Level 1 or otherwise verified to an equivalent level of functionality and assurance All other RA cryptographic operations must be performed cryptographic modules rated at FIPS 140-1 Level 1 or otherwise verified to an equivalent level of functionality and assurance. End Entities must use cryptographic modules validated to at least FIPS 140-1 Level 1 or otherwise verified to an equivalent level of functionality and assurance.
Digital Signature High Assurance Certificates	All CA Digital Signature key generation, CA Digital Signature key storage and certificate signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-1 Level 3 or otherwise verified to an equivalent level of functionality and assurance. All other CA cryptographic operations must be performed in a cryptographic module validated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality. The RA Administrator Digital Signature key generation and signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance. All other RA cryptographic operations must be performed cryptographic modules rated at FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance. End Entities must use a hardware cryptographic module validated to at least

	FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

[C**ommentary** – FIPS 140-1 is being superceded by FIPS 140-2, however that will take time, so each state will need to periodically review the status of that transition and whether to upgrade the standards described in this CP to reflect that transition.]

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version number

The CA must issue X.509 Version 3 certificates, in accordance with the PKIX Certificate and CRL Profile.

7.1.2 Certificate extensions

The PKI End-Entity software must support all the base (non-extension) X.509 fields:

Signature:	CA signature to authenticate certificate
Issuer:	name of CA
Validity:	activation and expiry date for certificate
Subject:	Subscriber's distinguished name
Subject Public Key Information:	algorithm ID, key
Version:	version of X.509 certificate, version 3(2)
Serial Number:	unique serial number for certificate

No extension shall modify or undermine the use of these base fields. Additionally,

- *The certificatePolicies field must be set as critical in all* certificates issued in the ___ PKI.
- *Every DN must be in the form of an X.501 printableString.*
- *A CA must include and mark as critical the policyConstraints extension.*
- *Critical extensions shall be interpreted as defined in PKIX.*
- All Entity PKI software must correctly process the extensions identified in 4.2.1 and 4.2.2 of the PKIX certificate profile.
- The CPS must define the use of any extensions supported by the CA, its RAs and End Entities.

7.1.3 Algorithm object Ids CRL distribution points for difference assurance levels

The CA must use and End-Entities must support, for signing and verification, the following algorithms:

- RSA 1024 or 2048 in accordance with PKCS#1 - [OID TBD];
- SHA-1 in accordance with FIPS PUB 180-1 and ANSI X9.30 (Part 2) - [ID sha1WithRSAEncryption, OID 1 2 840 113549 1 1 5, Issuing Authority RSADSI]. Entities may use, for signing and verification, the following algorithms:

- RSA 1024, RSA 2048 in accordance with PKCS#1 - [OID TBD];
- DSA in accordance with DSS (FIPS PUB 186) and ANSI X9.30 (Part 1) - [OID TBD];
- MD5 in accordance with RFC 1321 - [OID TBD];
- SHA-1 in accordance with FIPS PUB 180-1 and ANSI X9.30 (Part 2) - [ID sha1WithRSAEncryption, OID 1 2 840 113549 1 1 5, Issuing Authority RSADSI].

7.1.4 Name forms

Every DN must be in the form of an X.501 printable String.

7.1.5 Name constraints

Subject and Issuer DNs must comply with PKIX standards and be present in all certificates.

7.1.6 Certificate policy object identifier

A CA must ensure that the Policy OID is contained within the certificates it issues.

7.1.7 Usage of policy constraints extension

A CA must populate and mark as critical the policy Constraints extension.

7.1.8 Policy qualifiers syntax and semantics

A CA must populate the policy Qualifiers extension with the URL of its CP. If the CA populates the userNotice extension, such text shall be limited to the text described in 2.1.1.

7.1.9 Processing semantics for the critical certificate policy extension

Critical extensions shall be interpreted as defined in PKIX.

7.2 CRL Profile

7.2.1 Version number

The CA must issue X.509 version two (2) CRLs in accordance with the PKIX Certificate and CRL Profile.

7.2.2 CRL and CRL entry extensions

All Entity PKI software must correctly process all CRL extensions identified in the PKIX Certificate and CRL profile. The CPS must define the use of any extensions supported by the CA, its RAs and End Entities.

8. SPECIFICATION ADMINISTRATION

8.1 Specification Change Procedures

8.1.1 Items that can change without notification

None.

8.1.2 Changes with notification

Prior to making any changes to this certificate policy, the PMA will notify all CAs issuing certificates.

8.1.2.1 List of items

All items in this certificate policy are subject to the notification requirement.

8.1.2.2 Notification mechanism

The PMA will notify, in writing, all CAs that issue certificates under this policy of any proposed changes to this certificate policy. The notification must contain a statement of proposed changes, the final date for receipt of comments, and the proposed effective date of change. The PMA may request CAs to notify their Subscribers of the proposed changes. The PMA will also post a notice of the proposal on the PMA World Wide Web site.

8.1.2.3 Comment period

The comment period will be 30 days unless otherwise specified. The comment period will be defined in the notification.

8.1.2.4 Mechanism to handle comments

Written and signed comments on proposed changes must be directed to the PMA. Decisions with respect to the proposed changes are at the sole discretion of the PMA.

8.1.2.5 Period for final change notice

The PMA will determine the period for final change notice.

8.1.2.6 Items whose change requires a new policy

If a policy change is determined by the PMA to warrant the issuance of a new policy, the PMA may assign a new Object Identifier (OID) for the modified policy.

8.2 Publication and Notification Procedures

An electronic copy of this document, digitally signed by an authorized representative of the CA, is to be made available:

- at the PMA World Wide Web site, URL (TBD);
- at the CA World Wide Web site, URL (TBD);
- via an e-mail request to [address to be supplied].

Approved CAs shall post copies of this Policy in their repositories.

8.3 CPS Approval Procedures

A CA's participation in the ___ PKI must be in accordance with procedures specified by the PMA. Where a CPS contains information relevant to the security of a CA, all or part of the CPS need not be made publicly available.

---

[i] Access controls may be instituted at the discretion of the CA with respect to certificates or on-line certificate status (if the latter is provided as a service by the CA). Certificates must be published promptly upon issuance. A CA must ensure, directly or with agreement with a repository, unrestricted access by Relying Parties to CRLs. CRL publication must be in accordance with 4.

The Repository will be available to Relying Parties on a basis that is stipulated by the Policy Authority when approving the CA for this CP and the CA's then current terms of access under the corresponding CPS. CA shall not impose any access controls on this Policy, the CA's certificate for its signing key, and past and current versions of the CA's CPS. CA may impose access controls on Certificates, certificate status information, or CRLs at its discretion, subject to agreement between the CA and Subscriber, in accordance with provisions published in its CPS or otherwise.

ii Disaster Recovery Plan

The CA must have in place an appropriate disaster recovery and business resumption plan. The plan must set up and render operational a facility located in a geographic diverse area that is capable of providing CA Services in accordance with this Policy within forty-eight (48) hours of an unanticipated emergency. Such plan shall include a complete and periodic test of readiness for such facility. Such plan shall be referenced within the CPS or other appropriate documentation and readily available to Relying Parties for inspection.