DRAFT 17 Oct 2001

X.509 Certificate Policy

For The

<institution name>

<date>

OBJECT IDENTIFIER ________________________

Version 0.011

Identification and Validation of this Policy

This Certificate Policy has been assigned the global Object Identifier (OID) shown on the cover page. A CA MAY NOT SIGN ANY PUBLIC KEY CERTIFICATE OR OTHER DOCUMENT THAT ASSERTS BY REFERENCE TO THIS OID ITS CONFORMANCE TO THIS CERTIFICATE POLICY UNLESS ALL ASPECTS OF ITS MANAGEMENT AND OPERATION CONFORM COMPLETELY WITH THE REQUIREMENTS CONTAINED HEREIN.

Minor modifications will be indicated by a suffix to this OID. Any significant changes to this policy, as determined by the Policy Management Authority (see Section 1.4.1), will result in a document with a different OID assignment.

This Policy contains definitions for certificate Levels of Assurance (LOA) that have been assigned global Object Identifiers for use in certificate policy and policy mapping extension fields (see Section 1.2). [TBR: These might be defined in the CPS instead of here.] These are:

"Test" level of assurance	___________________
"Rudimentary" level of assurance	___________________
"Basic" level of assurance	___________________
"Medium" level of assurance	___________________
"High" level of assurance	___________________

Minor changes to this policy SHALL NOT change the meaning of these LOA OIDs. If changes in this policy result in new definitions of the LOA, then new OIDs will be assigned.

A copy of this document SHALL be digitally signed using SHA-1 with RSA encryption and the private key associated with the authority certificate of the CA operating under this policy. The signed document SHALL be available on-line at the location specified by certificates issued under this policy (see Section 7.1.8).

Table of Contents

RECORD OF CHANGES

CHANGE NUMBER	DATE OF CHANGE	DATE RECEIVED	DATE ENTERED	SIGNATURE OF PERSON ENTERING CHANGE

1. INTRODUCTION

This Certificate Policy (CP) statement defines the terms and conditions under which a Certificate Authority (CA) that issues Public Key Certificates (PKC) that reference the policy object identifier (OID) for this CP MUST operate. Operation includes management of the PKCs it issues and management of its own infrastructure. The term "issues" in this context refers to the process of digitally signing with the private key associated with its authority certificate a structured digital object conforming to the ISO X.509, version 3 or compatible PKC format.

One or more companion Certification Practice Statement(s) (CPS) MUST be defined for each CA operating under this CP. Such a statement MUST articulate how the CA implements the provisions of this policy.

The CA MAY be stand-alone or it MAY be part of a Public Key Infrastructure (PKI) hierarchy. In the latter case, any CA for which this CA signs an authority certificate MUST adopt this CP or one that is consistent with all of the requirements of this CP as determined by the Policy Management Authority for this CA.

This CP is structured in accordance with RFC 2527 [1]. Within this document the words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", "OPTIONAL" are to be interpreted as in RFC 2119 [2].

1.1 OVERVIEW

This CP defines a set of requirements that helps to determine the viability and applicability of a PKC issued by a conforming CA to its community of users, subject entities, and/or class of applications.

This CP MAY be used by a PKC Relying Party to help in deciding whether a certificate and the information therein and the binding of that information to the Subject are sufficiently trustworthy for a particular application.

Any PKC issued by a CA MUST contain a valid reference to the applicable CP. This CP may be referenced only if the CA is in compliance with all aspects of this CP.

Each CA MUST make available its own CPS(s) in order to provide information to potential clients of the CA and Relying Parties about the underlying technical, procedural and legal foundations which are not otherwise specified in this policy.

A CA MAY delegate any of its responsibilities under this CP to another Person, provided the CA remains responsible for conformance with all provisions of this CP and associated CPS(s).

By relying on information contained in a PKC issued by this CA, the Relying Party is agreeing with the provisions and stipulations of this CP and the associated CPS under which the PKC was issued.

1.1.1 Certificate Policy (CP)

Any CA that intends to refer to this CP in a PKC that it issues MUST digitally sign a copy of this document, using SHA-1 with RSA encryption and its primary PKC signing key, and make the signed copy available on-line as specified in Section 1.2.

1.1.2 Relationship Between the CP and the CPS

This CP states what assurance can be placed in a certificate issued by the CA. The associated CPS states how the CA establishes that assurance.

1.1.3 Interoperation with CAs External to this Policy Domain

The CA MAY issue a cross-certification PKC to an unrelated CA but only after PMA review of the other CA's CP and a mutually agreed upon mapping of the Levels of Assurance as defined by this CP and the other CA's CP. Such agreement MUST take into account all of the relevant requirements and conditions of use as specified in the two CPs. The mapping of Levels of Assurance between this CP and the other CA CP SHALL be specified in the PolicyMappings fields of the cross-certification PKC.

The BasicConstraints fields in any cross-certification PKC SHOULD be set to constrain resulting trust paths to no more levels than can be warranted by the PMA. The BasicConstraints fields in any cross-certification PKC also SHOULD be set to constrain naming in any PKCs issued by the certified CA to that which the PMA deems acceptable.

The CA MAY accept a cross-certification PKC from an unrelated Certificate Authority provided that the Subject name and public key in that PKC are identical to those in the CA's authority PKC.

1.1.3.1 Relationship Between a Bridge CP and this CP

The CA SHALL NOT issue a cross-certification PKC to a Bridge CA unless the conditions in section 1.1.3 are met. In addition, operation of the Bridge CA with respect to additional cross-certifications MUST be consistent with all of the relevant requirements and conditions specified in this CP for the Levels of Assurance included in the cross-certification PKC PolicyMappings fields. The PMA is responsible for reviewing the operation of any such Bridge CA and ensuring that such mapping is appropriate.

1.2 IDENTIFICATION

Each PKC issued by the CA MUST reference an Object Identifier (OID) that identifies this CP document. The PKC MUST also include an OID indicating the Level of Assurance (LOA) that applies to that PKC. How this is to be achieved is described in the remainder of this section with further detail elsewhere in this CP.

The base of the Object Identifier (OID) MUST be registered under the ANSI (or equivalent) arc. Sub-arcs SHALL be defined for both this CP itself and for the different LOAs defined by this CP. OIDs also SHOULD be assigned to all associated CPSs referencing this CP.

When referencing this CP as governing a PKC, the OID given on the cover page SHALL be used in addition to any textual description. If this CP is changed in any substantive way, a new CP OID SHALL be assigned for the new version.

There are five LOAs covered by this CP as defined in subsequent sections. It is the intent of this CP for these LOAs to map directly to the Federal PKI (FPKI) Policy Authority LOAs.

The LOA asserted in any PKC issued by the CA SHALL be indicated by the OID in the CertPolicyID field in the PKC. The LOA OIDs for this CP are defined on the first page. The LOA OIDs SHOULD be defined under a general LOA sub-arc as follows:

Test ::= { LOA 1 }

Rudimentary ::= { LOA 2 }

Basic ::= { LOA 3 }

Medium ::= { LOA 4 }

High ::= { LOA 5 }

The CPSuri extension field in a PKC asserting one of these LOAs MUST point to an on-line copy of the CPS that implements that LOA, digitally signed as specified in Section 1.1.1. That CPS in turn MUST identify explicitly by an appropriate OID the CP to which it is conforming and specify how a Relying Party may obtain a copy of that CP. It SHOULD also include a URI pointing to an on-line, digitally signed copy of that CP.

Subsequent revisions of this CP SHALL have a new OID assignment under the same OID arc. Minor revisions MAY be indicated by a suffix appended to the OID given on the cover page to this CP. The Level of Assurance (LOA) identifiers represent abstractions and SHALL remain the same unless or until new LOAs are required.

1.3 COMMUNITY AND APPLICABILITY

The CA MUST include in any CPS a definition of the Communities to which the CA will issue a PKC. The CA SHOULD NOT issue a PKC to any Person or other entity that is not included in one of the Communities. A Relying Party SHOULD NOT assume that the holder of a PKC issued by this CA has any particular relationship to any of the communities defined in the CPS unless explicitly stated in the CPS that such an assumption is warranted.

The CA MUST include in any CPS a definition of the applicability or any restrictions on the use of any resulting PKC. Such applicability MUST be indicated in the appropriate PKC fields, e.g. KeyUsage. A Relying Party MUST respect any applicability limitations indicated in the PKC.

1.3.1 PKI Authorities

A CA MAY issue a PKC with certificate issuance rights (“authority PKC”) to another CA and in that case the so Authorized CA assumes the role of a CA under this CP. The authority PKC SHOULD contain policy mapping extension defining how the LOAs of the authorizing CA correspond to the LOAs of the authorized CA, to the extent that they do. Naming and path length constraints also MAY be indicated as described in Section 1.1.3. For all purposes under this CP, the Authorized CA SHALL conform to, and operate under, this CP.

The PMA for this CA SHALL have oversight responsibility for the operation of the Authorized CA to ensure its conformance with this CP. This CA MAY delegate any of its responsibilities to a PMA associated with the Authorized CA, provided that this CA remains responsible for conformance with all provisions of this CP.

A CA operating at Basic or lower LOA SHOULD NOT issue authority PKCs.

1.3.2 Registration Authorities

The function of a Registration Authority (RA) is to verify the credentials that establish the binding between a Person or other entity that is the Subject of a PKC and the Subject's Public/Private Key Pair that is associated with that PKC and approve the issuance of a PKC for that Subject. The CA MAY perform the function of a Registration Authority or the CA MAY delegate some or all of the RA functions to one or more other organizations or functional units. The CA remains responsible for conformance with all provisions of this CP and associated CPS(s). Any RA so delegated MUST have a signed agreement with the CA affirming the authority and obligations of both parties.

1.3.3 End Entities

The end entities that may be the Subject of a PKC issued under this policy can be (1) a natural person representing himself or herself, (2) an organization that is defined as part of the Community and is represented by a natural person authorized to act for that organization, or (3) a digital processing entity (e.g., a computer, a router or a defined application program or system), that is capable of performing cryptographic operations and that is owned or operated by an organization that is as part of the Community and that is represented by a natural person authorized to act for that organization ("PKC Sponsor"). In the latter case, the method of verification of the authorization of the person acting on behalf of the digital processing entity SHALL be set forth in the CPS.

1.3.4 Applicability

PKCs issued by a CA MAY be used for any application, provided that the uses are within the limitations imposed by the CPS or as indicated in the PKC itself.

However, only Relying Parties that accept in its entirety this CP and that accept in their entirety any limitations (financial or otherwise) contained in the PKC itself MAY make use of a PKC issued by this CA.

If a Subscriber wishes to have any limitations (financial or otherwise) on transactions authenticated by the PKCs that are not contained in the PKC itself, that Subscriber MUST have a signed agreement with each Relying Party agreeing to such limitations. Any Relying Party that wants to make use of a PKC issued by this CA to authenticate transactions of significant financial value or otherwise of import to the Relying Party SHOULD have a signed agreement with the Subscriber stating any specific limitations.

The table below summarizes the recommended applicability of PKCs at each of the five levels of assurance covered by this CP.

Assurance Level	Applicability
Test	This level is used for interoperability testing. It is solely used for this purpose and conveys no assurance information.
Rudimentary	This level provides the lowest degree of assurance concerning identity of the Subject. One of the primary functions of this level is to provide data integrity to the information being signed. This level is relevant to environments in which the risk of malicious activity is considered to be low. It may not be suitable for transactions requiring reliable authentication. It is generally insufficient for transactions requiring strong confidentiality, but may be used for this where certificates having higher levels of assurance are unavailable.
Basic	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to result in significant negative consequences. It is assumed at this security level that users are not likely to be malicious.

Medium	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud.
High	This level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

1.4 CONTACT DETAILS

Questions about interpretation of this CP and associated CPSs, or concerns about possible abuse of this CP SHALL be directed in writing to the PMA identified under section 1.4.1.

1.4.1 Specification administration organization

The Policy Management Authority (PMA) for this CP MUST be identified by postal address, office location and other contact information in the applicable CPS.

1.4.2 Contact person

Intentionally left blank.

1.4.3 Person determining Certification Practice Statement suitability for the policy

The PMA is responsible for reviewing and approving with an authorized signature any proposed CPS that is to be associated with this CP.

2. GENERAL PROVISIONS

This section defines the responsibilities of each party involved in the issuance and use of PKCs issued by the CA. These responsibilities bear on any potential liability that might be associated with a CA operating under this CP as a result of use of an issued PKC. Relying Parties MUST understand the provisions of this section.

2.1 OBLIGATIONS

Each party to the issuance and use of a PKC has an obligation to perform certain duties as detailed in this section. By accepting an issued PKC, a Subscriber accepts the obligations described hereunder. By making use of a PKC issued by this CA, a Relying Party is accepting its obligations hereunder.

2.1.1 CA Obligations

The CA MUST operate a certification authority service in accordance with all provisions of this CP and any associated CPS(s). Its obligations include:

(1) Accepting certification requests and issuing PKCs according to a published CPS, including:

(a) verifying the necessary credentials of each Person requesting a certificate and verifying the binding of those credentials to the Subject;

(b) validating the connection between a public/private key pair and the requester's identity including a suitable proof of possession method;

(c) ensuring notification of the Subscriber regarding its obligations and responsibilities;

(d) ensuring to the best of its ability that any additional information to be included in the issued PKC is accurate and appropriately associated with the Subject;

(e) issuing a PKC based on the authenticated Subscriber's request and published PKC profiles;

(f) sending notification of PKC issuance to the Subscriber;

(g) making issued PKCs available on-line as required in section 2.6.1;

(h) logging all transactions and recording the unique identifying marks of any associated credentials.

(2) Accepting certificate revocation requests and effecting certificate revocation or suspension, as defined in section 4.4 including:

(a) accepting and authenticating revocation requests according to the procedures contained in this CP and associated CPS(s);

(b) authenticating Subscribers or other parties requesting that a PKC be revoked and confirming that they are authorized to make such a request;

(c) making any resulting certificate revocation information publicly available;

(d) logging all transactions and recording the unique identifying marks of any associated credentials.

(3) The CA MUST NOT issue more than one PKC with the same public key unless the Subject entity is the same in all instances.

A CA that issues a PKC to a Subscriber MUST have explicit authorization from that Subscriber to do so. The CA MUST respect any restrictions or limitations on Subject names, path length, and/or policy mapping as specified in its authority PKC and/or written agreement with its authorizing CA. A CA SHALL NOT issue any PKC with a Level of Assurance higher than that in its authority PKC.

2.1.2 RA Obligations

An RA functional unit MAY be delegated by a CA any or all of the responsibilities under section 2.1.1 subsections (1)(a) through (d) and (h) and (2)(a) and (b) under this CP. An RA so delegated MUST do the following in addition to the responsibilities specifically delegated by the CA:

(1) confirm to the CA in a secure manner the validation of the connection between a public/private key pair and the requester's identity including the successful use of a suitable proof of possession method;

(2) adhere to the CPS(s) and the written agreement made with the CA.

2.1.3 Subscriber Obligations

A Subscriber MUST:

(1) read and agree to the terms and conditions under which the CA issues PKCs;

(2) present legitimate credentials as required by the CPS for the PKC to be issued;

(3) appropriately protect the private key associated with an issued PKC. Specific requirements are stated in the CPS for the PKC to be issued. Some types of PKCs MAY require that the private key be put in escrow;

(4) notify the CA immediately upon either suspected or known compromise of the private key associated with a PKC issued by the CA.

2.1.4 Relying Party Obligations

Relying Parties MUST understand and accept this CP and associated CPS(s) before making use of any PKC issued by the CA. Relying Parties MUST check a PKC’s revocation status when verifying a PKC with a level of assurance of Basic or higher issued by this CA. Relying Parties MUST NOT use any PKC issued by this CA for purposes that are proscribed by the PKC contents or this CP or associated CPS(s). Relying Parties MUST be aware of and abide by all rules, regulations and statutes applicable to all information contained in a PKC. For example, if a PKC Subject is a student registered at the institution issuing the PKC, the Relying Party may have obligations to treat information in the PKC according to the requirements of the Family Educational Rights and Privacy Act (FERPA).

2.1.5 Repository Obligations

The CA SHALL make available on-line as soon as reasonably possible copies of all PKCs issued, unless a PKC is specifically made confidential per section 2.8 of this CP or the associated CPS. Access control mechanisms SHALL be implemented when needed to protect repository information as described in Section 2.6.3. All information in the Repository that is not otherwise digitally signed SHALL be digitally signed by the CA or its delegated functional unit(s).

The CA SHALL make available its primary authority PKC and any additional authority PKCs in which it is named as the Subject in the repository. In addition, the CA SHOULD make available all primary authority PKCs of CAs above it in the PKC hierarchy as well as all other authority PKCs that name any of those CAs as Subjects.

The CA SHALL make available on-line certificate revocation information according to the issuance requirements in 4.4.9.1 and other relevant public information as soon as is reasonably possible.

For CAs operating at the Basic LOA or higher, the Repository for the above SHALL be designed for high availability, including replicated platforms and redundant network connections, and operated in a highly robust and secure manner.

At a minimum, the CA SHOULD post the public information of the Repository to an x.500 or Lightweight Directory Access Protocol (LDAP) server system. Such information MAY also be accessible through other mechanisms. The specific access protocols SHALL be defined in any CPS associated with this CP.

2.2 LIABILITY

2.2.1 CA Liability

The CA Group disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of the accuracy of information provided, and further disclaims any and all liability for negligence and lack of reasonable care with respect to all PKCs issued by it. The CA Group shall not incur liability for representations of information contained in any PKC. Without limiting the generality of the foregoing, the CA Group accepts no liability of any sort if a Relying Party fails to fulfill its obligations as stated herein.

Liability, if any, SHALL be limited to actual monetary damages.

In no event shall the CA Group be liable for any indirect, special, incidental, or consequential damages, or for any loss of profits, loss of data, or other indirect, consequential, or punitive damages, arising from or in connection with the use, delivery, license, performance, or nonperformance of certificates, digital signatures, or any other transactions or services offered or contemplated by this CPS, even if the CA Group has been advised of the possibility of such damages.

In no event will the aggregate liability of the CA Group to all parties (including without limitation a Subscriber, an applicant, a recipient, or a Relying Party) exceed $1,000. This limitation on damages applies to loss and damages of all types, including but not limited to direct, compensatory, indirect, special, consequential, exemplary, or incidental damages incurred by any person, including without limitation a Subscriber, an applicant, a recipient, or a Relying Party, that are caused by reliance on or use of a certificate the CA Group issues, manages, uses, suspends or revokes, or a certificate that expires. This limitation on damages applies as well to liability under contract, tort, and any other form of liability claim. The liability cap on each certificate shall be the same regardless of the number of digital signatures, transactions, or claims related to such certificate. In the event the liability cap is exceeded, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction. In no event shall the CA Group be obligated to pay more than the aggregate liability cap for each certificate, regardless of the method of apportionment among claimants to the amount of the liability cap.

2.2.2 RA Liability

Intentionally left blank.

2.3 FINANCIAL CONSIDERATIONS

The CA Group assumes no financial responsibility with respect to use or management of any issued PKC.

2.3.1 Indemnification by Relying Parties and subscribers

Intentionally left blank.

2.3.2 Fiduciary relationships

Intentionally left blank.

2.3.3 Administrative processes

Administrative processes pertaining to this CP SHALL be described in the CPS.

2.4 INTERPRETATION AND ENFORCEMENT

Interpretation of this CP or any associated CPS(s) is the responsibility of the PMA.

2.4.1 Governing Law

Operation of this CA SHALL conform to the laws governing the jurisdiction in which the CA is legally formed. Notwithstanding anything to the contrary in this CP, if the laws of any state of the United States or the law of the United States governing a Subscriber (including but not limited to any laws related to choice of law) ("Subscriber Governing Laws") forbid the inclusion of specific provisions of this CP, then with respect to that Subscriber only, the specific provision of this CP shall be deemed null and void as if not included at all. However, wherever possible within the letter and spirit of the Subscriber Governing Laws, rather than causing a provision of this CP to be null and void pursuant to the prior sentence, all Subscriber Governing Laws will be interpreted in such a way as to achieve the letter and spirit of this CP. Where a conflict cannot be resolved between this CP and a Subscriber Governing Law, that Subscriber Governing Law shall prevail.

2.4.2 Severability of Provisions, Survival, Merger, and Notice

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect.

2.4.3 Dispute resolution procedures

The PMA SHALL have the exclusive authority to resolve any disputes associated with the use of the PKCs issued by the CA. If a dispute regarding interpretation of provisions in this CP arises between two CAs that issue PKCs referencing this CP's OID and that obtain their authority to issue PKCs from the same Authorizing CA, all such disputes SHALL be resolved by the PMA identified in the Authorizing CA's CP.

2.4.4 Section Headings

Headings used throughout this CP are for convenience only and SHALL NOT affect the interpretation of this CP.

2.5 Fees

The CA will determine all fees, if any, to be imposed.

2.5.1 Certificate issuance or renewal fees

Fees MAY be imposed for issuance or renewal of PKCs by the CA. Such fees MUST be agreed to by the payer prior to issuance or renewal of the PKC. If fees are imposed but not paid within 60 days of notification to the payer, the issued PKC MAY be revoked.

2.5.2 Certificate access fees

Fees SHALL NOT be charged for on-line access to copies of PKCs issued by this CA and held in its Repository or for on-line access to the authority certificate for this CA.

Fees MAY be charged for other forms of access to issued PKCs.

2.5.3 Revocation or status information access fees

Fees SHALL NOT be charged for certificate revocation or for on-line access to certificate revocation or status information. Fees MAY be charged for other forms of access to certificate revocation or status information.

2.5.4 Fees for other services such as policy information

Fees SHALL NOT be charged for any on-line form of access to this CP or any associated CPS.

2.5.5 Refund policy

Fees are not refundable. Fees charged but not paid are still due regardless of the status of the PKC or service request.

2.6 PUBLICATION AND REPOSITORY

All information about CA operation and PKCs issued SHALL be available on-line, except as indicated in this section 2.6. Each PKC issued SHALL include information sufficient to locate this on-line Repository.

2.6.1 Publication of CA Information

A CA SHALL make available on-line and MAY make available in other forms:

- this CP and any CPS(s) under which it operates,
- its authority PKC(s) and other PKCs as described in Section 2.1.5.
- all issued PKCs except those PKCs of Subscribers that explicitly request that their PKC not be made publicly available,
- signed certificate revocation and other certificate status information.

The CPS referenced by the CPSuri in the PKC SHALL define how a Relying Party can locate and retrieve the rest of the above information.

2.6.2 Frequency of Publication

PKCs SHALL be made available as part of the issuing process except as provided in Section 2.6.1. This process MUST be described in associated CPS(s).

The frequency of certificate revocation publication is specified in 4.4.9.

Changes to this CP or its associated CPS(s) SHALL be published as soon as they are approved. Previous versions SHALL remain available on-line for at least 180 days beyond the latest expiration date of any PKC that references that CP or CPS. Archived copies of all CPs under which the CA has ever issued a PKC SHOULD be kept indefinitely, or as may be required by law (see Section 8.2.4).

2.6.3 Access controls

There SHALL NOT be limitations on access to this CP, CPS(s) or certificate revocation information. There MAY be limitations on access to PKCs, for example to prevent bulk acquisition of data such as e-mail addresses.

2.6.4 Repositories

Repositories MUST be operated in a reliable and secure manner as detailed in CPS(s). The primary Repository SHALL be replicated to at least one on-line secondary Repository in order to increase its availability. Repository contents MUST be replicated off-line for disaster recovery and independent validation purposes. See section 2.1.5.

2.7 COMPLIANCE AUDIT

For a CA operating at the Basic LOA or higher, the operation of the CA SHALL be audited periodically for conformance with this CP and all associated CPS(s) by independent and knowledgeable third parties. CAs operating at the Test or Rudimentary LOA SHOULD conduct internal audits regularly as defined in Section 2.7.1. CAs that have delegated any part of their responsibility to a different functional unit are responsible for ensuring a proper audit of the operation of those functional units. In addition, if the CA derives its authority PKC from an Authorizing CA, that Authorizing CA MAY review any compliance audit for conformance with the Authorizing CA's CP at any time upon reasonable prior notification.

2.7.1 Frequency of Compliance Audit

The CA and Authorized CAs SHALL be subject to a periodic compliance audit that is no less frequent than once per calendar year for CAs operating at High or Medium levels of assurance, and no less than once every two calendar years for those operating at the Basic level of assurance. CAs operating at the Rudimentary level of assurance SHOULD be subject to an internal audit at least annually. There is no audit frequency requirement for CAs operating at the Rudimentary level of assurance.

An Authorizing CA has the right to require periodic and aperiodic compliance audits or inspections of Authorized CA operations to validate that the subordinate entities are operating in accordance with the security practices and procedures described in their respective CPS.

2.7.2 Identity/Qualifications of Compliance Auditor

The auditor SHALL have specific knowledge of the operation of a CA and experience performing audits of CA operation. If no such auditor can be found after a reasonable effort has been made, then an auditor with knowledge and experience performing audits of business data processing centers MAY perform the CA audit. The audit report MUST note and explain this exception to the requirements of this CP.

2.7.3 Compliance Auditor's Relationship to Audited Party

The external auditor SHALL be legally independent of the audited CA. The audit fees, if any, SHALL be paid by the CA.

2.7.4 Topics Covered by Compliance Audit

The purpose of a compliance audit SHALL be to verify that an entity subject to the requirements of this CP is complying with the requirements of this CP and any applicable CPSs.

2.7.5 Actions taken as a result of deficiency

The PMA MAY determine that the CA is not complying with its obligations set forth in this CP. When such a determination is made, the PMA MAY direct the CA to cease operation, or MAY direct that other corrective actions be taken which would allow operation to continue. Procedures for this purpose SHALL be published by the PMA.

When the compliance auditor finds a discrepancy between how the conforming CA is designed or is being operated or maintained, and the requirements of this CP, the following actions SHALL be performed:

- The compliance auditor SHALL note the discrepancy;
- The compliance auditor SHALL promptly notify the PMA of the discrepancy. If the discrepancy is judged by the PMA to be severe in nature (that is, it is determined to be a "material discrepancy" relative to the applicable requirements), the PMA SHALL include that finding in its notification to the CA.
- The party responsible for correcting the discrepancy SHALL determine what further notifications or actions are necessary pursuant to the requirements of this CP, and then proceed to make such notifications and take such actions without delay.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the PMA MAY decide to halt temporarily operation of the CA, or take other actions it deems appropriate. Procedures for making and implementing such determinations will be developed by the PMA.

2.7.6 Communication of Result

Intentionally left blank.

2.8 CONFIDENTIALITY

The CA collects and stores information from Subjects of a PKC that may be personally identifying. These data MUST be processed in a way that ensures privacy and other protections according to the laws applicable to the CA, as specified in section 2.4.1.

2.8.1 Types of information to be kept confidential

All information presented to the CA that is not included in a resulting PKC or certificate revocation record issued by the CA is considered confidential and SHALL NOT be released by the CA to third parties without the Subscriber's authorization; unless such a release is required by a legal authority of competent jurisdiction.

2.8.2 Types of information not considered confidential

Information included in published PKCs or certificate revocation records issued by the CA is not considered confidential except as may be required by law.

2.8.3 Disclosure of certificate revocation information

When a PKC is revoked, a reason code SHALL be included in the certificate revocation record for the action. This reason code is not considered confidential and MAY be shared with all other users and Relying Parties. However, other details concerning the revocation SHALL NOT be disclosed unless required by a legal authority of competent jurisdiction or permitted elsewhere in this CP.

2.8.4 Release to law enforcement officials

The CA SHALL NOT disclose confidential PKC or PKC-related information to any third party, except when required by a legal authority of competent jurisdiction under a duly issued warrant or subpoena or as might be required by the laws applicable to the CA, as specified in section 2.4.1.

2.8.5 Release as part of civil discovery

The CA SHALL NOT disclose confidential PKC or PKC-related information to any third party, except when required by a legal authority of competent jurisdiction under a duly issued warrant or subpoena or as might be required by the laws applicable to the CA, as specified in section 2.4.1.

2.8.6 Disclosure upon Subscriber's request

The CA MAY release Subscriber's confidential information upon validation of a request signed by Subscriber.

2.8.7 Other information release circumstances

Intentionally left blank.

2.9 INTELLECTUAL PROPERTY RIGHTS

The CA MUST NOT claim any intellectual property rights with respect to issued PKCs. If any Subject’s private key is escrowed, ownership of and all rights to that key remain with the Subject.

Any party MAY make use of any or all of the language in this CP or associated CPS(s) providing that appropriate attribution is included.

3. IDENTIFICATION AND AUTHENTICATION

The validity of a PKC for use as a digital credential is dependent heavily upon the validity of the credentials offered during initial verification of the Subject. The CA MUST ensure proper binding between the Subject of a PKC and the credentials provided by the Subscriber or the Subject’s agent during the registration process, as detailed in the applicable CPS. Similar assurance MUST be obtained when renewing or revoking an issued PKC.

In addition, if contents of an issued PKC constitute a direct link to records in a supplemental database containing additional attributes of the Subject, the binding between the Subject and any such database entries MUST be verified before the PKC is issued or renewed. Details of this verification MUST be described in the applicable CPS.

3.1 INITIAL REGISTRATION

The CPS(s) associated with this CP SHALL detail how initial registration is performed. Specific requirements MUST be given for each type of PKC issued by the CA, including the types of credentials to be presented by the applicant, how they are verified, and how the resulting PKC is bound to a private key in the Subscriber's possession. A Relying Party must be able to assess whether the level of assurance and security required for each step in the initial registration process results in a PKC of sufficient trustworthiness for its intended use.

3.1.1 Types of names

If a Subject name is present in a PKC issued by the CA, it SHOULD be reasonably relevant to the Subject. It need not be unique, depending on the nature and intended use of the PKC as defined in the CPS. For example, a Subject name MAY be an abstract object assigned to the class of entities, such as "student," of which the Subject is a member. A Subject name MUST NOT be misleading such that a Relying Party reasonably might assume that the Subject is a physical entity other than the actual holder of the PKC.

The CA SHALL be able to generate and sign PKCs that contain an X.500 Distinguished Name (DN); the X.500 DN MAY also contain domain component (DC=) elements. Where DNs are required, Subscribers SHALL have their DN specified by the CA. PKCs MAY additionally assert an alternate name form, subject to requirements set forth below intended to ensure name uniqueness. The table below describes the naming requirements that apply to each level of assurance.

Test	To be established by the PMA (will depend upon testing circumstances)
Rudimentary	Non-Null Subject Name, or Null Subject Name if Alternative Subject Name is populated and marked critical
Basic	Non-Null Subject Name, and optional Alternative Subject Name that is marked non-critical
Medium	X.500 Distinguished Name, and optional Alternative Subject Name that is marked non-critical
High	X.500 Distinguished Name, and optional Alternative Subject Name that is marked non-critical

3.1.2 Need for names to be meaningful

The CPS defines whether a PKC will contain Subject names that are meaningful. Meaningful in this context means that the name can be interpreted to refer to a defined class of entities. A class that, by definition, includes only a single entity becomes an identity credential for the Subject.

When DNs are used, it is preferable that the common name represent the Subject in a way that is easily understandable for humans. For people, this typically will be a legal name. For equipment, this MAY be a model name and serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter). However, the DN for human Subjects MAY also be a pseudonym (for example, a large number) as long as it respects name space uniqueness requirements.

In the case where a CA certifies another Authorized CA within that policy domain, the Authorizing CA MUST impose restrictions on the name space that MAY be used by the Authorized CA that are at least as restrictive as its own name constraints.

3.1.3 Rules for interpreting various name forms

The CA MUST detail in the CPS(s) the rules for interpreting various name forms used in the PKCs it issues.

3.1.4 Uniqueness of names

The Subject name in a PKC MUST refer to a unique, identifiable entity or class of entities. The Subject name, if present and meaningful, MUST have the same meaning and interpretation whenever that distinguished name is included in a PKC issued by the CA.

The CA and Authorized CAs SHALL document in their respective CPSs:

- What name forms will be used,
- How the CA and Authorized CAs will interact to ensure this is accomplished, and
- How the CA and Authorized CAs will allocate names within the Community to guarantee name uniqueness among current and past Subscribers (e.g., if "Joe Smith" leaves a Community, and a new, different "Joe Smith" enters the Community, how these two people will be provided unique Subject names).

3.1.5 Name claim dispute resolution procedure

There SHOULD NOT be reason for two entities to dispute a distinguished name. The CA SHOULD include sufficient qualifiers in any meaningful Subject name to ensure that the class of entities to which it refers is unambiguously and appropriately identified.

3.1.6 Recognition, authentication and role of trademarks

The Subscriber SHALL NOT request, and the CA SHALL NOT knowingly issue, a PKC in which the distinguished name is composed solely of trademarks; however the CA MAY issue a PKC in which the distinguished name is composed solely of trademarks registered to the CA Group.

3.1.7 Method to prove possession of private key

Except for certain PKCs to be used with data encryption, the applicant for a PKC SHOULD generate its own key pair for use with the resulting PKC. In this case, the CA MUST detail in the CPS how it will verify that the applicant has possession and use of the private key associated with the public key to be included in the PKC. The CA MUST NOT issue a PKC for which the above proof of possession fails.

In the case where a key is generated directly on the applicant's physical key store, or in a key generator that without human intervention transfers the key to the applicant's physical key store, then the applicant is deemed to be in possession of the private key at the time of generation or transfer. If the applicant is not in possession of the physical key store when the key is generated, then the physical key store SHALL be delivered to the Subscriber via a method verifiable by a receipt signed by that Subscriber.

For all assurance levels, when keyed physical key stores are delivered to Subscribers, the delivery SHALL be accomplished in a way that ensures that the correct key stores and activation data are provided to the correct Subscribers. The CA MUST maintain a record of validation for receipt of the physical key store by the Subscriber.

Any mechanism that includes a shared secret (e.g., a password or PIN) SHALL be used only for "basic" or lower LOA PKCs. If such a mechanism is employed, it SHALL be designed to provide a reasonable degree of assurance that the applicant and the CA are the only recipients of this shared secret.

See also Section 6.1.1 Key Pair Generation by the CA.

3.1.8 Authentication of organization identity

Requests for PKCs wherein the Subject is the name of an organization SHALL include the legal name of the organization, the organization's principal address, documentation of the existence of the organization, and identification of the Chief Executive Officer of the organization. The CA SHALL verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

3.1.9 Authentication of Individual Identity

The CA MUST ensure strong binding between the PKC applicant and any attributes of identity that are to be asserted by the PKC. The specific documents required and the method of their verification MUST be detailed in the CPS(s) associated with this CP.

The CA and Authorized CAs SHALL record the process that was followed for issuance of each PKC. Process information MAY depend upon the certificate level of assurance and SHALL be addressed in the appropriate CPS. The process documentation and authentication requirements SHALL include the following, depending upon the level of assurance as set forth below:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the Subscriber as required by the applicable certificate policy;
- A unique identifying number from the ID of the verifier and, if in-person identity proofing is done, from the two forms of photo ID provided by the applicant;
- The date and time of the verification;
- A declaration of identity signed by the applicant using a handwritten signature. If in-person identity proofing is done, this SHALL be performed in the presence of the person performing the identity authentication.

For All Levels: Where photo ID document serial numbers or other identifying information is required in the table below, such numbers or information MUST be recorded to an archive at the time the registration is made. This record SHALL be retained for at least 12 months after the expiration of the associated PKC.

The table below summarizes the identification requirements for each level of assurance. A Relying Party MUST take into account the potential risk associated with accepting the PKC as a reliable credential.

Assurance Level	Identification Requirements
Test	To be established by the PMA (will depend upon test circumstances)
Rudimentary	No in-person identification requirement; applicant may apply and receive a PKC by providing personally identifying information that only the RA and the Subject should know.
Basic	Identity may be established by in-person appearance before a Registration Authority for the CA or Trusted Agent; or comparison of user-supplied information (obtained and/or checked electronically, through other trusted means (such as the U.S. mail), or in-person) to a database; or by attestation of a supervisor, or administrative or information security officer, or a person certified by a state or Federal institution as being authorized to confirm identities (such as notaries public) who uses a stamp, seal or other mechanism to authenticate their identity confirmation
Medium	Identity established by in-person appearance before the Registration Authority for the CA, Trusted Agent or an entity certified by a State or Federal institution as being authorized to confirm identities (such as notaries public) who uses a stamp, seal or other mechanism to authenticate their identity confirmation Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which SHALL be a photo I.D. (e.g., Drivers License)
High	Identity established by in-person appearance before the Registration Authority for the CA or Trusted Agent Credentials required are either one Federal Government-issued Picture I.D., or two nonFederal Government I.D.s, one of which SHALL be a photo I.D. (e.g., Drivers License)

3.1.10 Authentication of Component Identities

Some computing and communications components (routers, firewalls, servers, etc.) MAY be named as PKC Subjects. In such cases, the component MUST have a PKC Sponsor. The PKC Sponsor is responsible for providing the following registration information:

- Equipment identification

- Equipment public key(s)
- Equipment attributes and authorizations (if any are to be included in the PKC)
- Contact information to enable the CA to communicate with the PKC Sponsor when required

The registration information SHALL be verified to an assurance level commensurate with the certificate assurance level being requested. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the PKC Sponsor (using certificates of equivalent or greater assurance than that being requested).
- In person registration by the PKC Sponsor, with the identity of the PKC Sponsor confirmed in accordance with the requirements of Section 3.1.9.

3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY

Renewal of an issued PKC SHALL only be performed by the same CA that issued it and MUST be performed while the prior PKC is still valid. Renewal MAY be based on a digitally signed request using the still-valid PKC without in-person identification as required in section 3.1.

Renewal SHOULD require generation of a new key pair. However, if the renewal occurs within three years of the original date of issuance of the first issued PKC to include the public key, and the key is at least 1,024 bits long, then the same public key MAY be included in the renewal PKC.

3.2.1 Certificate Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtains new keys and re-establishes its identity. Re-keying a PKC means that a new PKC is created that has the same characteristics and level as the old one, except that the new PKC has a new, different public key (corresponding to a new, different private key); a different serial number; and MAY be assigned a different validity period.

Subscribers SHALL identify themselves for purpose of re-keying as required in the table below.

Assurance Level	Routine Rekey Identity Requirements for Subscriber Signature and Encryption Certificates
Test	To be determined by the PMA
Rudimentary	Identity may be established through use of current signature key
Basic	Identity MAY be established through use of current signature key, except that identity SHALL be reestablished through initial registration process at least once every 15 years from the time of initial registration
Medium	Identity MAY be established through use of current signature key, except that identity SHALL be established through initial registration process at least once every nine years from the time of initial registration
High	Identity MAY be established through use of current signature key, except that identity SHALL be established through initial registration process at least once every three years from the time of initial registration

3.2.2 Certificate Renewal

Renewing a PKC means creating a new PKC with the same name, key, and other information as the old one, but a new, extended validity period and a new serial number. PKCs MAY be renewed in order to reduce the size of the certificate revocation database. A PKC MAY be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subject name and attributes are unchanged. Thus, a CA MAY choose to create a PKC good for one year, renew it twice (each for a one year period), then re-key at the end of the third year.

3.2.3 Certificate Update

Updating a PKC means creating a new PKC that has the same or a different key, a different serial number, and differs in one or more other fields, from the old PKC. For example, a CA MAY choose to update a PKC of a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The old PKC may or may not be revoked, but MUST NOT be further re-keyed, renewed, or updated.

Further, if a human Subject's name changes (e.g., due to marriage), then proof of the name change MUST be provided to the CA in order for an updated PKC which includes the new name to be issued.

Finally, when a CA updates its private signature key and thus generates a new public key, the CA SHALL notify all Authorized or cross-certified CAs, and SHOULD make a best effort to notify any Subscribers that rely on the CA's PKC, that it has been changed. For self-signed ("root") PKCs, such PKCs SHALL be made available on-line along with separately retrievable verification information to enable a relying party to verify that it has received a valid copy of the new “root” PKC. The CPS SHALL define how this is accomplished.

3.3 OBTAINING A NEW CERTIFICATE AFTER REVOCATION

A public key whose associated PKC has been revoked for private key compromise MUST NOT be re-certified. The public key MAY be re-certified if the PKC was merely suspended. In the latter case, identification of the Subject MAY be accomplished with the same procedure indicated in section 3.1 for initial registration, or by using a digitally signed request using the suspended PKC. Such a request MUST be sent to the CA during the period of validity of the PKC to be restored.

3.4 REVOCATION REQUEST

The CA MUST accept as a revocation request an appropriate message digitally signed with the PKC to be revoked as long as it is still valid and not already revoked or suspended. The same procedures adopted for Subject identity during initial registration MAY also be used. Alternative procedures MAY be supported but MUST be detailed in the relevant CPS.

4. OPERATIONAL REQUIREMENTS

This section specifies requirements imposed upon entities involved in the certification and certificate revocation process.

4.1 APPLICATION FOR A CERTIFICATE

Procedures to apply for a certificate are found in the CPS.

4.1.1 Delivery of public key for certificate issuance

Public keys MUST be delivered to the CA in a way that binds the applicant's verified identification to the public key. For all levels of assurance, this binding MAY be accomplished using cryptography. If cryptography is used, it MUST be at least as strong as that employed in certificate issuance. Additionally, for Medium and Basic Assurance, this binding MAY also be accomplished using non-cryptographic physical and procedural mechanisms. These mechanisms MAY include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a token to a certificate issuer for local key generation at the point of certificate issuance or request. For Rudimentary Assurance, no trusted delivery mechanism is required. For Test Assurance, the mechanism SHALL be defined by the CA. In all cases, the method used for public key delivery MUST be set forth in a CPS.

In those cases where public/private key pairs are generated by the CA or Authorized CA on behalf of the Subscriber, the CA or Authorized CA (respectively) SHALL implement secure mechanisms to ensure that the token on which the public/private key pair is held is securely sent to the proper Subscriber. The CA or Authorized CA (respectively) SHALL also implement procedures to ensure that the token is not activated by an unauthorized entity.

4.2 CERTIFICATE ISSUANCE

Upon receiving a request from an applicant for a PKC, the conforming CA MUST respond in accordance with the requirements set forth in this CP and applicable CPS.

The PKC request MAY contain an already built ("to-be-signed") PKC. This PKC MUST NOT be signed until its contents are verified according to the process set forth in this CP and applicable CPS.

While the Subscriber MAY do most of the data entry, it is still the responsibility of the CA to verify that the information is correct and accurate. This MAY be accomplished through a system approach linking trusted databases containing personnel information, other equivalent authenticated mechanisms, or through personal contact with the Subscriber. If databases are used to confirm Subscriber information, then these databases MUST be protected from unauthorized modification to a level commensurate with the level of assurance of the certificate being sought.

4.2.1 Delivery of Subscriber's private key to Subscriber

Anyone who is not the Subscriber SHALL NOT under any circumstances have knowledge of or control over a private key that is to be used by a Subscriber for digital signatures or authentication. Except as described in Section 6.2.3.1, the key pair to be associated with a Subject named in a PKC issued by the CA SHALL be generated by the Subscriber or as otherwise described in Section 3.1.7. A private key will be generated and remain within the cryptographic boundary of the cryptographic module under control of the Subscriber. Since the Subscriber generates the keys, there is no need for the CA to deliver the private key to the Subscriber. Accountability for the location and state of the private key SHALL be the responsibility of the Subscriber as described in the CPS.

4.3 CERTIFICATE ACCEPTANCE

Once a PKC has been issued, its acceptance by the Subscriber triggers its obligations under the terms and conditions of this CP.

For Medium and High Assurance levels, a Subscriber SHALL be required to legally sign a document defining the requirements and obligations of the Subscriber with respect to protection of the private key and use of the PKC before being issued the PKC. For Basic Assurance level, the Subscriber SHALL be required to acknowledge his or her obligations respecting protection of the private key and use of the PKC before being issued the PKC. For Rudimentary or Test Assurance level, there are no requirements for this acknowledgement.

As soon as possible after a PKC is accepted, it SHALL be published in an appropriate on-line directory and made available to Subscribers and Relying Parties upon request, as described in section 2.1.5.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

A CA is also responsible for maintaining and making available certification revocation information, herein referred to as a CRL. Such information MUST be made available in the form of a complete list of all revoked but unexpired certificates and MAY be made available via a network protocol such as the Online Certificate Status Protocol (OCSP). A CA SHALL NOT issue a revocation for a PKC it has not issued. It need not issue a revocation for a PKC that has already expired. Any revocation entry for a PKC that expires MAY be removed from all CRLs. CAs operating at the Test or Rudimentary LOA SHOULD but are not required to support certificate revocation.

4.4.1 Circumstances for revocation of a certificate

A PKC SHALL be revoked when the binding between the Subject and the Subject's public key contained within a PKC is no longer considered valid within the Level of Assurance indicated. Examples of circumstances that invalidate the binding include:

- Identifying information in the PKC becomes invalid;
- The Subscriber, issuing CA, or Authorizing CA (if any) can be shown to have violated, or is strongly suspected of violating, the requirements of this CP or applicable CPS;
- The private key has been or is suspected of having been compromised, or has been lost, stolen, or destroyed in a fashion where there is potential for compromise or loss of control over the use of the private key.

Additionally, a Subscriber MAY always request the revocation of his or her PKC directly. Whenever any of the above circumstances occur, the associated PKC SHALL be revoked and notification placed on the CRL. Revocation notices SHALL be included on all new publications of the certificate status information until the associated PKCs expire.

4.4.2 Who can request revocation of a certificate

The process for requesting revocation of a Subscriber PKC issued by the CA SHALL be set forth in this CP or applicable CPS.

In addition, revocation normally will proceed if:

- A CA receives sufficient evidence of compromise or loss of the Subscriber's corresponding private key, or
- An authenticated request is made to the CA by the Subscriber, or
- The CPS under which the PKC was issued states that a Relying Party can assume the Subject is a member of a particular Community and the CA receives sufficient evidence that the Subscriber is no longer a member of that Community.

4.4.3 Procedure for revocation request

A request to revoke a PKC SHALL identify the PKC to be revoked, explain the reason for revocation, and enable the request to be authenticated (e.g., digitally or manually signed).

Authentication of PKC revocation requests is important to prevent malicious revocation of PKCs by unauthorized parties. In particular, if the revocation is being requested for reason of key compromise or suspected fraudulent use, then the Subscriber's revocation request MUST so indicate. For signed requests from the PKC Subject, verification of the signature is sufficient.

Upon receipt of a valid revocation request, the CA SHALL revoke the certificate by placing its serial number and other identifying information on a CARL/CRL and then posting the CARL/CRL in the CA Repository, in addition to any other revocation mechanisms used.

When revocation of a PKC issued by the CA or an Authorized CA is required, it SHALL be done within the time limits specified in the table below. The CPS MAY set forth emergency procedures for the CA to use to effect immediate revocation of a PKC when appropriate.

Assurance Level	**Revocation Time Period**
Test	Established by the PMA
Rudimentary	Established by the PMA
Basic	Within 6 hours
Medium	Within 2 hours
High	Within 30 minutes

Revocation SHALL take effect upon the publication of status information (identifying the reason for the revocation, which may include loss, compromise, or termination of employment) within the time limits as specified in the table above (starting from the time the request is authenticated or sufficient evidence of compromise or loss is received). A revocation notice regarding a PKC that is revoked SHALL remain in the CRL until the PKC expires and for one additional CRL issuance cycle beyond that point. A revocation notice MAY be removed from the second CRL issued after the corresponding PKC expires.

4.4.4 Revocation Request Grace Period

There is no revocation grace period for the revocation of PKCs issued under this CP.

4.4.5 Suspension

Suspension SHALL NOT be used by the CA.

4.4.6 Who can request suspension

Not applicable.

4.4.7 Procedure for suspension request

Not applicable.

4.4.8 Limits on suspension period

Not applicable.

4.4.9 Certificate Authority Revocation Lists / Certificate Revocation Lists

CAs operating at the Basic LOA or higher SHALL issue Certification Authority Revocation Lists (CARLs) and Certificate Revocation Lists (CRL). CAs operating at the Test or Rudimentary LOA MAY issue CRLs as defined by their PMA and documented in their CPS(s).

4.4.9.1 CARL/CRL Issuance Frequency

CARLs and CRLs SHALL be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information MAY be issued more frequently than the issuance frequency described below. The CA SHALL ensure that superseded PKC status information is removed from the Repository upon posting of the more recent status information.

PKC status information SHALL be published not later than the next scheduled update. This will facilitate the local caching of PKC status information for off-line or remote (laptop) operation. The CA SHALL coordinate with the Repository to which it posts PKC status information to reduce latency between creation and availability.

The following table provides CARL/CRL issuance requirements.

Assurance Level	CARL/CRL Issuance Frequency for CAs	CARL/CRL Issuance for CAs (Loss or Compromise of Private Key)
Test	As defined by the PMA	As defined by the PMA
Rudimentary	As defined by the PMA and documented in the CPS	As defined by the PMA and documented in the CPS
Basic	At least once each week	Within 24 Hours of Notification
Medium	At Least Once Each Day	Within 24 Hours of Notification
High	At Least Once Each Day	Within 6 Hours of Notification

4.4.10 CARL/CRL Checking requirements

Reliance on revoked PKCs could have serious consequences for the Relying Party. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a PKC whose revocation status may be unknown. A Relying Party SHOULD always check revocation status for PKCs indicating Basic or higher LOA.

4.4.11 On-line Revocation / Status checking availability

In addition to download access to CARL/CRLs, conforming CAs and Relying Party client software MAY optionally support on-line status checking with a documented protocol such as the On-line Certificate Status Protocol (OCSP). Client software using on-line status checking need not obtain or process file based CARL/CRLs. The CPS will specify when and under what circumstances the CA will provide on-line status checking of issued PKCs.

4.4.12 On-line revocation checking requirements

If the CA supports OCSP, it is still the responsibility of the Relying Party to determine when to make use of it, as described in section 4.4.10.

4.4.13 Other forms of revocation advertisements available

Intentionally left blank.

4.4.14 Checking requirements for other forms of revocation advertisements

Intentionally left blank.

4.4.15 Special requirements related to key compromise

Intentionally left blank.

4.5 SECURITY AUDIT PROCEDURE

Audit log files SHALL be generated for all events relating to the security of the CA or Authorized CAs. Where possible, the security audit logs SHALL be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism SHALL be used. All security audit logs, both electronic and non-electronic, SHALL be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section SHALL be maintained in accordance with Section 4.6.2.

4.5.1 Types of Events Recorded

All security auditing capabilities of the CA or Authorized CA operating system and PKI CA applications required by this CP SHALL be enabled. As a result, most of the events identified in the table below SHALL be automatically recorded. Auditing capabilities relevant to Test Assurance level are not described below. At a minimum, each audit record SHALL include the following (either recorded automatically or manually for each auditable event):

- The type of event
- The date and time the event occurred
- A success or failure indicator when executing the CA or Authorized CA's signing process
- A success or failure indicator when performing certificate revocation
- Identity of the entity and/or operator of the CA or Authorized CA that caused the event.
- Message from any source requesting an action by the CA or Authorized CA is an auditable event. The message MUST include message date and time, source, destination and contents.

Auditable Event	Rudimentary	Basic	Medium	High
SECURITY AUDIT				
Any changes to the Audit parameters, e.g., audit frequency, type of event audited		X	X	X
Any attempt to delete or modify the Audit logs		X	X	X
Obtaining a third-party time-stamp		X	X	X

Auditable Event	Rudimentary	Basic	Medium	High
IDENTIFICATION AND AUTHENTICATION				
Successful and unsuccessful attempts to assume a role		X	X	X
The value of *maximum authentication attempts* is changed		X	X	X
Maximum authentication attempts unsuccessful authentication attempts occur during user login		X	X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts		X	X	X
An Administrator changes the type of authenticator, e.g., from password to biometrics		X	X	X
LOCAL DATA ENTRY				
All security-relevant data that is entered in the system		X	X	X
REMOTE DATA ENTRY				
All security-relevant messages that are received by the system		X	X	X
DATA EXPORT AND OUTPUT				
All successful and unsuccessful requests for		X	X	X

Auditable Event	Rudimentary	Basic	Medium	High
confidential and security-relevant information				
KEY GENERATION				
Whenever the CA or Authorized CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X	X	X
PRIVATE KEY LOAD AND STORAGE				
The loading of Component private keys	X	X	X	X
All access to certificate Subject private keys retained by the CA or Authorized CA if the CA supports key escrow services	X	X	X	X
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE				
All changes to the trusted public keys, including additions and deletions	X	X	X	X
SECRET KEY STORAGE				
The manual entry of secret keys used for authentication			X	X
PRIVATE AND SECRET KEY EXPORT				
The export of private and secret keys (keys used for a single session or message are	X	X	X	X

Auditable Event	Rudimentary	Basic	Medium	High
excluded)				
CERTIFICATE REGISTRATION				
All certificate requests	X	X	X	X
CERTIFICATE REVOCATION				
All certificate revocation requests		X	X	X
CERTIFICATE STATUS CHANGE APPROVAL				
The approval or rejection of a certificate status change request		X	X	X
CA OR AUTHORIZED CA CONFIGURATION				
Any security-relevant changes to the configuration of the CA or Authorized CA		X	X	X
ACCOUNT ADMINISTRATION				
Roles and users are added or deleted	X	X	X	X
The access control privileges of a user account or a role are modified	X	X	X	X
CERTIFICATE PROFILE MANAGEMENT				

Auditable Event	Rudimentary	Basic	Medium	High
All changes to the certificate profile	X	X	X	X
REVOCATION PROFILE MANAGEMENT				
All changes to the revocation profile		X	X	X
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT				
All changes to the certificate revocation list profile		X	X	X
MISCELLANEOUS				
Installation of the Operating System		X	X	X
Installation of the CA or Authorized CA		X	X	X
Installing hardware cryptographic modules			X	X
Removing hardware cryptographic modules			X	X
Destruction of cryptographic modules		X	X	X
System Startup		X	X	X
Logon Attempts to CA or Authorized CA Apps		X	X	X
Receipt of Hardware / Software			X	X
Attempts to set passwords		X	X	X
Attempts to modify passwords		X	X	X
Backing up CA or Authorized CA internal database		X	X	X

Auditable Event	Rudimentary	Basic	Medium	High
Restoring CA or Authorized CA internal database		X	X	X
File manipulation (e.g., creation, renaming, moving)			X	X
Posting of any material to a Repository			X	X
Access to CA or Authorized CA internal database			X	X
All certificate compromise notification requests		X	X	X
Loading tokens with certificates			X	X
Shipment of Tokens			X	X
Zeroizing tokens		X	X	X
Rekey of the CA or Authorized CA	X	X	X	X
Configuration changes to the CA server involving:				
Hardware		X	X	X
Software		X	X	X
Operating System		X	X	X
Patches		X	X	X
Security Profiles			X	X
PHYSICAL ACCESS / SITE SECURITY				
Personnel Access to location of CA or Authorized CA			X	X
Access to the CA or Authorized CA server			X	X

Auditable Event	Rudimentary	Basic	Medium	High
Known or suspected violations of physical security		X	X	X
ANOMALIES				
Software Error conditions		X	X	X
Software check integrity failures		X	X	X
Receipt of improper messages			X	X
Misrouted messages			X	X
Network attacks (suspected or confirmed)		X	X	X
Equipment failure	X	X	X	X
Electrical power outages			X	X
Uninterruptible Power Supply (UPS) failure			X	X
Obvious and significant network service or access failures			X	X
Violations of Certificate Policy	X	X	X	X
Violations of Certification Practice Statement	X	X	X	X
Resetting Operating System clock		X	X	X

4.5.2 Frequency of processing data

Audit logs SHALL be reviewed as specified in the table below. All significant events SHALL be explained in an audit log summary. In addition to statistical sampling as required, such reviews SHALL include 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 noted in the logs. Actions taken as a result of these reviews SHALL be documented.

Assurance Level	Review Audit Log
Test	As defined by the PMA
Rudimentary	Only required for cause
Basic	Only required for cause
Medium	At least once every two months Statistically significant set of security audit data generated by CAs since the last review SHALL be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity
High	At least once per month Statistically significant set of security audit data generated by CAs since the last review SHALL be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity

100% of security audit data generated by the CA since the last review SHALL be examined.

4.5.3 Retention period for security audit data

Audit logs SHALL be retained on-site for at least two months as well as being retained in the manner described below. The individual who removes audit logs from the CA or Authorized CA system SHALL be different from any of the individuals who, in combination, manage the CA or an Authorized CA signature key.

4.5.4 Protection of security audit data

CA and Authorized CA system configuration and procedures MUST be implemented together to ensure that:

- only authorized people have read access to the logs;
- only authorized people may archive or delete audit logs; and,

- audit log entries are not modified.

The entity performing audit log archive need not have modify access, but procedures MUST be implemented to protect archived data from deletion or destruction prior to the end of the audit log retention period (note that deletion requires modification access). Audit logs SHALL be moved to a safe, secure storage location separate from the CA equipment.

4.5.5 Security Audit data backup procedures

Audit logs and audit summaries SHALL be backed up at least monthly. A copy of the audit log SHALL be sent off-site at least once a month.

4.5.6 Security Audit collection system (internal vs. external)

The audit record collection process SHALL NOT be done by or under the control of the CA or Authorized CA. Audit record collection processes SHALL be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit record collection system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the PMA SHALL determine whether to suspend CA operation, or Authorized CA operation respectively, until the problem is remedied.

4.5.7 Notification to event-causing subject

Intentionally left blank.

4.5.8 Vulnerability Assessments

Intentionally left blank.

4.6 RECORDS ARCHIVAL

Records archiving is REQUIRED only for any CA operating at the Basic or higher LOA.

4.6.1 Types of events archived

CA or Authorized CA archive records SHALL be sufficiently detailed to verify the proper operation of the CA or Authorized CA, and the validity of any PKC (including those revoked or expired) issued by the CA or Authorized CA.

At a minimum, the following data SHALL be recorded for archive in accordance with each assurance level.

Data To Be Archived	Rudimentary	Basic	Medium	High

Data To Be Archived	Rudimentary	Basic	Medium	High
CA authority certificate	X	X	X	X
Certification Practice Statement	X	X	X	X
Contractual obligations	X	X	X	X
Initial and periodic snapshots of the CA system and equipment configuration		X	X	X
Significant modifications and/or updates to system or configuration		X	X	X
Certificate requests	X	X	X	X
Revocation requests		X	X	X
Subscriber identity Authentication data as per Section 3.1.9		X	X	X
Documentation of receipt and acceptance of PKCs and associated tokens, if applicable		X	X	X
All PKCs issued or published	X	X	X	X
Record of CA or subordinate CA Re-key	X	X	X	X
All CARLs and CRLs issued and/or published		X	X	X
All Audit Logs	X	X	X	X
Other data or applications to verify archive contents		X	X	X
Documentation required by compliance auditors		X	X	X

4.6.2 Retention period for archive

The minimum retention period for archived CA data is identified below.

Assurance Level	Retention Period
Test	As defined by the PMA
Rudimentary	7 Years & 6 Months
Basic	7 Years & 6 Months
Medium	10 Years & 6 Months
High	20 Years & 6 Months

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media SHALL be defined by the archive site. Applications required to process the archive data SHALL also be maintained for as long as necessary as determined by the CA.

4.6.3 Protection of archive

An unauthorized user SHALL NOT be permitted to write to, modify, or delete the archive. Archived records MAY be moved to another medium when authorized by the PMA. The contents of the archive SHALL NOT be released except as determined by the PMA or as required by law. Records of individual transactions MAY be released upon request of the Subscriber involved in the transaction. Archive media SHALL be stored in a safe, secure storage facility separate from the CA itself.

4.6.4 Archive backup procedures

Intentionally left blank.

4.6.5 Requirements for time-stamping of records

Intentionally left blank.

4.6.6 Archive collection system (internal or external)

Intentionally left blank.

4.6.7 Procedures to obtain and verify archive information

Each applicable CPS used by the CA SHALL include procedures for how to create, verify, package, transmit, and store the CA's archive information

4.7 KEY CHANGEOVER

To minimize risk from compromise of a CA's private signing key, that key SHOULD be changed periodically; and from that time on, only the new key will be used for certificate signing purposes. The older, but still valid, PKC will be available to verify old signatures until all of the PKCs signed using the associated private key also have expired. If the old private key is to be used to sign CRLs that contain certificates signed with that key, then the old key MUST be protected and retained as well.

The CA's signing key SHALL have a validity period of five years, and its corresponding certificate SHALL have a validity period of eight years. All values are in years.

Assurance Level	**CA (signing key / certificate validity period)**
Test	As defined by the PMA
Rudimentary	5 / 8
Basic	5 / 8
Medium	5 / 8
High	5 / 8

4.8 COMPROMISE AND DISASTER RECOVERY

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

If CA equipment is damaged or rendered inoperative, but the CA signature keys are not destroyed, the CA operation SHALL be reestablished as quickly as possible, giving priority to the ability to generate certificate status information.

4.8.2 CA signature keys are revoked

If the CA cannot issue a revocation prior to the time specified in the next update field of its currently valid CARL/CRL, then the PMA SHALL be immediately and securely notified. The PMA SHALL determine whether to revoke the authority certificate issued to any Authorized

CA. The CA SHALL re-establish revocation capabilities as quickly as possible in accordance with procedures set forth in the applicable CPS. The CA SHALL immediately and securely advise the PMA in the event of a disaster where the CA installation is physically damaged and all copies of the CA signature keys are destroyed.

4.8.3 CA signature keys are compromised

If a CA's signature keys are compromised or lost (such that compromise is possible even though not certain):

- The PMA SHALL be immediately and securely notified so that the Authorizing CA or CAs from whom a cross certification certificate has been issued MAY issue revocations for any authority or cross-certificates issued to the CA;
- The CAs that have issued PKCs to the affected CA SHALL immediately publish a CARL revoking the affected CA's PKC as set forth above;
- A new CA key pair SHALL be generated by the CA in accordance with procedures set forth in the applicable CPS;
- New CA authority PKCs SHALL be acquired or generated by the CA and made available in the Repository immediately;
- New cross-certificates SHALL be acquired and issued by the CA also in accordance with the applicable CPS; and
- All Subscribers SHALL be required to recertify following the initial identification procedures defined in section 3.1 and the CPS.

The CA SHALL investigate and report to the PMA what caused the compromise or loss and what measures have been taken to preclude recurrence.

4.8.4 Secure Facility Impaired after a Disaster

In the case of a disaster whereby the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the PMA SHALL be immediately and securely notified, and the PMA SHALL take whatever action it deems appropriate. The CA installation SHALL then be completely rebuilt, by reestablishing the CA equipment, generating new private and public keys, acquiring a new authority certificate, and re-issuing all authority PKCs to Authorized CAs. Relying Parties may decide of their own volition whether to continue to use PKCs signed with the destroyed private key pending reestablishment of CA operation with new PKCs.

4.9 CA TERMINATION

In the event of termination of the CA operation, PKCs signed by the CA SHALL be revoked and the PMA SHALL continue operation of the Repository and include in the Repository notice of the termination of the CA. Prior to CA termination, the CA SHALL provide archived data to a PMA approved archival facility.

In the event that an Authorized CA terminates operation, the CA SHALL ensure that any authority PKCs issued to that Authorized CA have been revoked.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS FOR THE CA OR AUTHORIZED CA

The CA SHALL impose physical security requirements that provide similar levels of protection as those specified below.

CA equipment SHALL be protected from unauthorized access while the cryptographic module is installed. The CA SHALL implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed. These security mechanisms SHALL be commensurate with the level of threat in the CA equipment environment.

5.1.1 Site location and construction

The location and construction of the facility housing the CA equipment SHALL be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, SHALL provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical access

The CA equipment SHALL always be protected from unauthorized access. These security mechanisms SHALL be commensurate with the level of threat in the equipment environment. At a minimum, the CA MUST be operated and controlled in accordance with the requirements below pertaining to the highest assurance level PKC to be issued.

The physical security requirements pertaining to CAs that issue Rudimentary or Basic assurance PKCs are:

- Ensure no unauthorized access to the hardware is permitted;
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers.

In addition to those requirements, the following requirements SHALL apply to CAs that issue Medium or High assurance PKCs:

- The facility SHALL be manually or electronically monitored for unauthorized intrusion at all times;

- The facility SHALL maintain an access and egress log and ensure that it is inspected concurrently with the security audits required in section 4.5 at the frequency specified in 4.5.2.

Physical security requirements pertaining to CAs at the Test Assurance level SHALL be commensurate with the risks associated with their use.

Removable cryptographic modules SHALL be inactivated prior to storage. When not in use, removable cryptographic modules and activation information used to access or enable cryptographic modules for the CA or equipment SHALL be placed in secure containers. Activation data SHALL be recorded and stored in a manner commensurate with the security afforded the cryptographic module. Activation data SHALL NOT be stored with the cryptographic module.

A security check of the facility housing the CA equipment for a CA operating at the Basic Assurance level or higher SHALL occur if the facility is to be left unattended. At a minimum, the check SHALL verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when "open", and secured when "closed"; and that all equipment other than the Repository is shut down);

- Any security containers are properly secured;

- Physical security systems (e.g., door locks, vent covers) are functioning properly; and

- The area is secured against unauthorized access.

A person or group of persons SHALL be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance SHALL be maintained. If the facility is not continuously attended, the last person to depart SHALL initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.3 Electrical Power

The CA SHALL operate with an uninterruptible power source sufficient to allow its orderly shutdown in the event primary electrical power is lost.

5.1.4 Water Exposures

Intentionally left blank.

5.1.5 Fire Prevention and Protection

Intentionally left blank.

5.1.6 Media Storage

CA media SHALL be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive, or backup information SHALL be duplicated, encrypted, and stored in a location separate from the CA.

5.1.7 Waste Disposal

Intentionally left blank.

5.1.8 Off-Site Backup

For the CA operating at the Basic Assurance level or higher, system backups, sufficient to recover from system failure, SHALL be made on a periodic schedule as described in the applicable CPS. Backups are to be performed, encrypted, and stored off-site not less than once per week at a location separate from the CA equipment. Only the latest backup need be retained. The backup SHALL be stored at a site with physical and procedural controls commensurate to that of the operational CA.

5.2 PROCEDURAL CONTROLS FOR THE CA

5.2.1 Trusted Roles

The requirements of this Section of the CP are described in terms of four roles:

Administrator -- authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; generate component keys; and perform any manual operations required for the issuance of PKCs.

Officer -- authorized to request or approve PKCs or PKC revocations, e.g. is the RA.

Auditor -- authorized to view and maintain audit logs.

Operator -- authorized to perform system backup and recovery.

These roles may be fulfilled by one or more individuals, as described in the following sections.

5.2.1.1 Administrator

The administrator role is responsible for:

- installation, configuration, and maintenance of the CA;
- establishing and maintaining CA system accounts;
- configuring certificate profiles or templates and audit parameters, and;
- generating and backing up CA keys.

If manual intervention is required in order to issue a PKC, the Administrator performs that function.

5.2.1.2 Officer

The officer role is responsible for approving the issuance of PKCs, that is:

- registering new Subscribers and requesting the issuance of PKCs;
- verifying the identity of Subscribers and accuracy of information included in PKCs;
- approving the issuance of PKCs;
- requesting or approving the revocation of PKCs.

Typically the Officer has no direct access to the CA physical hardware.

5.2.1.3 Auditor

The auditor role is responsible for:

- reviewing, maintaining, and archiving audit logs;
- performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with the applicable CPS.

Typically the Auditor has no direct access to the CA physical hardware.

5.2.1.4 Operator

The operator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.1.5 Separation of Roles

Role separation may be enforced either by the CA equipment, or procedurally, or by both means.

The separation of roles for the CA SHALL be as follows:

Assurance Level	**Role Separation Rules**
Test	Intentionally left blank.
Rudimentary	A CA operating at the Rudimentary LOA SHOULD implement the role separation defined under Basic below.
Basic	Individual CA personnel SHALL be specifically designated to the four roles defined in Section 5.2.1 above. Individuals MAY assume more than one role, however, a given individual SHALL NOT assume both the Officer and Administrator roles. One individual MAY be both the Officer and the Auditor. One individual MAY be both the Administrator and Operator.
Medium	Individual CA personnel SHALL be specifically designated to the four roles defined in Section 5.2.1 above. Individuals MAY assume more than one role, however, individuals who assume an Officer role MAY NOT assume an Administrator or Auditor role. The CA system SHALL authenticate its users with PKCs that it issues or causes to be issued and SHALL ensure that no user, however they might be identified in their PKC, can assume both an Officer and either an Administrator or Auditor role.
High	Individual CA personnel SHALL be specifically designated to the four roles defined in Section 5.2.1 above. Individuals MAY assume only one of the Officer, Administrator, and Auditor roles, but any individual MAY assume the Operator role. The CA system SHALL authenticate its users with PKCs that it issues or causes to be issued and SHALL ensure that no user, however they might be identified in their PKC, can: · Assume both the Administrator and Officer roles. · Assume both the Administrator and Auditor roles. · Assume both the Auditor and Officer roles.

5.2.2 Number of Persons Required Per Task

The incumbent of a CA role SHALL NOT perform its own auditor function. If the Officer is also the Auditor, then periodic audits SHALL be performed by a third party.

For tasks that represent significant security risks, such as activating the root signing key of a CA hierarchy, at least 2 individuals from an authorized group of no more than 4 individuals SHALL be required.

5.2.3 Identification and Authentication for Each Role

At all assurance levels other than Test of Rudimentary, an individual MUST identify and authenticate him/herself before being permitted to perform any actions set forth above for any role. The identity of individuals that are assigned to each role MUST be kept in read-only storage when accessible to the CA platform and MUST only be modifiable by an off-line device. For example, the list could be stored on CDROM that is created on an off-line system. Copies of the list SHALL be kept in backup storage as described in Section 5.1.8.

5.3 PERSONNEL CONTROLS

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

All persons filling trusted roles SHALL be selected on the basis of loyalty, trustworthiness, and integrity. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA SHALL be set forth in the applicable CPS.

5.3.2 Background Check Procedures

Intentionally left blank.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the CA SHOULD receive comprehensive training. Such training MUST be provided for personnel associated with a CA operating at the Basic, Medium, or High LOA. For a CA operating at the Medium or High LOA, there SHOULD be periodic verification that personnel skill levels reflect successful completion of this training. Training SHALL be conducted in the following areas:

Area	**Operating Level of Assurance of the CA**				
	Test	Rud.	Basic	Med.	High
CA security principles and			√	√	√

mechanisms					
All PKI software versions in use on the CA system		√	√	√	√
All PKI duties they are expected to perform		√	√	√	√
Disaster recovery and business continuity procedures.			√	√	√

5.3.4 Retraining Frequency and Requirements

Intentionally left blank.

5.3.5 Job Rotation Frequency and Sequence

Intentionally left blank.

5.3.6 Sanctions for Unauthorized Actions

The PMA SHALL take appropriate administrative and disciplinary actions against personnel who have performed actions involving the CA or its Repository not authorized in this CP or the applicable CPS.

5.3.7 Contracting Personnel Requirements

Contractor personnel employed to perform functions pertaining to the CA SHALL meet the same set of requirements described in this section 5.3.

In addition, such personnel SHALL be bonded to a level appropriate to the risks that their misfeasance or malfeasance might incur.

5.3.8 Documentation Supplied to Personnel

At a minimum, the CA SHALL make available to its personnel the certificate policies it supports (including this CP), relevant parts of the applicable CPS, and any relevant institutional policies. Documentation SHALL be maintained identifying all personnel who received training and the level of training completed.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation by the CA

Cryptographic keys for the authority certificates used by the CA SHALL be generated in FIPS 140 validated cryptographic modules with the possible exception of the PKC used to issue "Test" certificates. The modules SHALL meet or exceed Security Level 1 (for Rudimentary), Security Level 2 (for Basic or Medium), or Security Level 3 (for High). Requirements for Test Assurance SHALL be defined by the CA.

Cryptographic keys for end-entity certificates SHALL be generated by the end-entity, not by the CA, except possibly in the case of keys to be used for data encryption where escrow of the private key is required (see Section 6.2.3.1). Except as defined in section 6.2.3.1, the end-entity SHALL NOT reveal their private key(s) to the CA or any other entity.

6.1.2 Private Key Delivery to Subscriber

In most cases CA Subscribers will generate their own key pairs and thus will not require delivery of their private key. Whenever keys are generated by an entity other than the Subscriber (see Section 6.2.3.1), delivery of the private key to the Subscriber shall be effected in such a manner that no entity other than the key generating agent, the escrow agent (if any) and the Subscriber have access to an unencrypted version of the private key at any time. Only the escrow agent (if any) and the Subscriber may retain copies of the private key. For Basic or higher LOA PKCs, the Subscriber must sign a receipt for the private key and prove possession of it. This MAY be accomplished by using the private key to digitally sign a receipt for its delivery. If used, the procedure to implement the requirements of this section MUST be documented in the CPS.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys SHALL be delivered to the certificate issuer in an authenticated manner set forth in the applicable CPS. This is usually accomplished by means of an electronic certificate request message from the CA, but it also MAY be done through other secure mechanisms. Alternative mechanisms MAY include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier. If off-line means are used, they SHALL include identity checking as set forth in this CP and SHALL also ensure that proof of possession of the corresponding private key is accomplished.

6.1.4 CA Public Key Availability

The CA SHALL post a copy of its authority certificate, and a copy of any CA authority PKC that it signs, to its public Repository. In addition, the CA SHOULD post to its Repository a copy of any cross-certificate that it signs and any cross-certificate issued to it by another CA.

6.1.5 Key Sizes

Key sizes MUST be commensurate with the risk that they might be compromised during the validity period of the certificate or any document signed with the private key. Based on current and projected technology, 1024 bit keys should be reasonably safe through the year 2015. Based on current and projected technology, signing keys used by a CA MUST be at least 1024 bits in length. However, PKCs signed with 1024-bit keys SHOULD NOT be given a validity period beyond the year 2015. The signing key used by the principal CA in a hierarchy MUST be at least 2048 bits in length.

All FIPS-approved signature algorithms SHALL be considered acceptable. All PKCs issued by the CA SHOULD use at least 1024 bit RSA or DSA (or better) with Secure Hash Algorithm version 1 (SHA-1) (or better) in accordance with FIPS 186 [the most current revision].

If the PMA determines that the security of a particular algorithm might be compromised, it MAY require the CA to revoke the affected PKCs.

Use of SSL, TLS, or another protocol providing similar security SHALL require at a minimum triple-DES or equivalent NIST approved algorithm for the symmetric key, and 1024 bit (or better) RSA, DSA, or equivalent NIST approved algorithm for the asymmetric keys.

6.1.6 Public Key Parameters Generation

Public key parameters prescribed in the Digital Signature Standard (DSS) SHALL be generated in accordance with FIPS 186-2.

6.1.7 Parameter Quality Checking

When generating key pairs, parameter quality checking (including testing for prime numbers) SHALL be performed in accordance with FIPS 186-2, Appendix 2, or a more stringent test if specified by the CPS.

6.1.8 Hardware/Software Subscriber Key Pair Generation

For Subscribers, software or hardware SHALL be used to generate pseudo-random numbers, key pairs and symmetric keys, as set forth in the table below. Any pseudo-random numbers used for key generation material SHALL be generated by a FIPS approved method.

Assurance Level	Key Generation Mechanism
Test	As defined by the PMA
Rudimentary	Software or Hardware
Basic	Software or Hardware
Medium	Software or Hardware but Hardware is RECOMMENDED
High	Hardware only

6.1.9 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The use of a specific key pair is determined by the key usage extension in the associated X.509 certificate.

No bits are set to one (1) in the Key Usage field except as follows. Public keys that are bound into PKCs MAY be certified for use in verifying digital signatures or encrypting, but not both, except as specified below. In particular, PKCs to be used for digital signatures (including authentication) SHALL have the *digitalsignature* bit set. Such PKCs asserting a Basic or higher LOA MAY also set the *nonrepudiation* bit except as prohibited below. PKCs to be used for data encryption SHALL have the *dataencryption* bit set. CA authority PKCs SHALL have two key usage bits set: c*RLSign* and *CertSign.* This restriction is not intended to prohibit use of protocols (like the Secure Sockets Layer (SSL)) that provide authenticated connections using key management certificates.

Test, Rudimentary, Basic and Medium Assurance Level PKCs MAY include a single key for use with encryption and signature in support of legacy Secure Multipurpose Internet Mail Extensions (S/MIME) applications. Such "dual-use" PKCs SHALL be generated and managed in accordance with their respective signature PKC requirements, except where otherwise noted in this CP. Such "dual-use" PKCs SHALL NOT assert the *nonrepudiation* key usage bit, and SHALL NOT be used for authenticating data that will be verified on the basis of the dual-use PKC at a future time.

PKCs for which the private key is escrowed (see Section 6.2.3.1) SHALL NOT have the *nonrepudiation* bit set.

CAs at all levels of assurance SHOULD ensure that Subscribers who require both encryption capability and digital signature capability possess two different key pairs, one for data encryption and one for digital signature and authentication.

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for Cryptographic Module

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [latest version of FIPS 140 series]. The CA MAY determine that other comparable validation, certification, or verification standards are sufficient. These standards will be published in the CPS. Cryptographic modules SHALL be validated to the FIPS 140-1 level identified in this section, or validated, certified, or verified to more stringent requirements as published in the CPS.

The table below summarizes the requirements for cryptographic modules.

Assurance Level	**FIPS 140-1**	**Certification Authority Crypto Module**	**Subscriber**	**Registration Authority Crypto Module**
Test	N/A	Defined by the PMA	N/A	Defined by the PMA
Rudimentary	N/A	Level 1 (Hardware or Software)	N/A	Level 1 (Hardware or Software)
Basic	Required	Level 2 (Hardware or Software)	Level 1	Level 1 (Hardware or Software)
Medium	Required	Level 2 (Hardware)	Level 1	Level 2 (Hardware)
High	Required	Level 3 (Hardware)	Level 2	Level 2 (Hardware)

6.2.2 CA Private Key Multi-Person Control

If the CA makes use of a self-signed authority certificate, the private key for that PKC SHALL be kept off-line except when needed immediately to sign a secondary authority certificate or a cross-certificate. Activation of that private key SHALL require actions by at least 2 out of no more than 4 trusted individuals.

6.2.3 Key Escrow of CA Private Signature Key

The CA's signature keys used to support non-repudiation services SHALL NOT under any circumstances be escrowed by a third party. See also Section 6.2.4.1 below.

6.2.3.1 Escrow of End-Entity Decryption Keys

When PKCs are signed for end-entities that include the *dataencryption* bit set, the CA MAY require that the corresponding private key be escrowed. Such escrow MUST be provided by a third party and MAY include key pair generation. The result MUST be achieved in such a way that the CA never has the private key in a usable form. The CA MUST verify that the escrow agent has a valid copy of the private key before the signed certificate is returned to the end-entity.

The CA SHALL establish requirements for the key escrow agent and SHALL publish those requirements in the CPS.

6.2.4 Private Key Backup

The CA SHALL maintain a backup copy of their private keys in order to re-establish functionality in case of destruction of the key.

6.2.4.1 Backup of CA Private Signature Key

The CA private signature keys SHALL be backed-up under the same multi-person control as the original signature key. Such backup SHALL only create a single copy of the signature key at the CA location; a second copy MAY be kept at a secure secondary backup location. Procedures to effect this SHALL be included in the CPS.

6.2.4.2 Backup of End-Entity Private Signature Key

Subscriber private signature keys SHALL NOT be backed-up, escrowed, or copied, except as provided under section 6.2.3.1.

6.2.5 Private Key Archival

CA private signature keys SHALL NOT be archived.

6.2.6 Private Key Entry into Cryptographic Module

CA private keys SHALL be generated by and remain in a cryptographic module. The CA private keys MAY be backed up only in accordance with Section 6.2.4.1.

6.2.7 Method of Activating Private Keys

Activation of the CA signing key SHALL require more than one authorized individual, as described in section 6.2.2.

Activation of an end-entity private key MUST require authentication of the Subject to the cryptographic module, either hardware or software. Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data SHALL be protected from disclosure (i.e., the data SHOULD NOT be displayed while it is entered).

6.2.8 Methods of Deactivating Private Keys

If cryptographic modules are used to store private keys, then the cryptographic modules that have been activated SHOULD NOT be left unattended or otherwise available to unauthorized access. After use, the cryptographic module SHALL be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. Hardware cryptographic modules SHOULD be removed and stored in a secure manner when not in use.

6.2.9 Method of Destroying Subscriber Private Signature Keys

Subscriber private signature keys SHALL be destroyed when they are no longer needed, or when all PKCs to which they correspond have expired or are revoked and no reinstatement is anticipated. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this most likely will be accomplished by executing a "zeroize" command.

6.3 OTHER ASPECTS OF KEY-PAIR MANAGEMENT

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival. A PKC MUST remain archived for at least its validity period or for as long as any document signed with the corresponding private key MUST be able to be revalidated, whichever is longer.

The archival system SHOULD provide integrity controls in addition to digital signature by the archivist since the archive requires tamper protection, which is not provided by digital signatures.

Archived documents MUST be digitally signed by an archive authority and MUST be resigned periodically before the cryptanalysis period for the last signing key is exceeded.

The procedures for appropriate archive and retrieval of certificates and other documents issued by the CA SHALL be set forth in the CPS.

6.3.2 Usage Periods for the Public and Private Keys

The CA private signing keys MAY be used to sign PKCs for up to 8 years. The PKCs the CA issues MAY NOT be valid for longer than 7 years. The actual period will depend upon the nature of the Subject. The total of the signing key age at the time of signing plus the validity period of the signed PKC SHALL NOT exceed the projected period of safety for the key length used.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

The activation data used to unlock CA or Subscriber private keys, in conjunction with any other access control, SHALL have an appropriate level of strength for the keys or data to be protected. For Rudimentary, Basic, and Medium assurance levels, activation data MAY be user selected. For the High assurance level, it SHALL either entail the use of biometric data or satisfy the policy enforced at/by the cryptographic module. Activation data SHALL be generated in conformance with the most current version of the FIPS 112 standard. If the activation data must be transmitted, it SHALL be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation Data Protection

Data used to unlock private keys SHALL be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data SHOULD either be biometric in nature or memorized, and SHOULD NOT be written down. If written down, it SHALL be secured at the level of the data that the associated cryptographic module is used to protect, and SHALL NOT be stored with the cryptographic module. The protection mechanism SHALL include a facility to temporarily lock the account after a predetermined number of login attempts as set forth in the applicable CPS.

6.4.3 Other Aspects of Activation Data

Intentionally left blank.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions MUST be provided. They MAY be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA SHALL provide for the following functionality:

- Require authenticated logins using credentials with at least as high a LOA as the CA itself

- Provide a security audit capability
- Restrict access control to CA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Require a trusted path for identification of PKI roles and associated identities
- Prohibit object re-use or require separation for CA random access memory
- Require use of cryptography for session communication and database security
- Archive CA history and audit data
- Require self-test of security related CA services
- Require a recovery mechanism(s) for keys and the CA system
- Enforce domain integrity boundaries for processes critical to system security

6.5.2 Computer Security Rating

Intentionally left blank.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

The System Development Controls for the CA are as follows:

- The CA operating at the Basic or higher LOA SHALL use software that has been designed and developed under a development methodology such as MIL-STD-498, the System Security Engineering Capability Maturity Model (SSE CMM), FIPS 140 or the Common Criteria.
- Hardware and software procured to operate the CA SHALL be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- The CA operating at the Basic or higher LOA SHALL ensure that all hardware and software used by the CA has been developed in a controlled environment, and that the development process was defined and documented.

- All hardware for a CA operating at the Basic or higher LOA MUST be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the manufacture location to the CA physical location.

- The CA hardware and software SHALL be dedicated to performing the task(s) of the CA. There SHALL NOT be any applications, hardware devices, network connections, or component software, which are not required by the CA operation.

- Proper care SHALL be taken to prevent malicious software from being loaded onto the CA equipment. Only applications required to perform the operation of the CA SHALL be loaded. Such software SHALL be obtained from sources authorized by local policy. CA hardware and software SHALL be scanned for malicious code on first use and periodically afterward.

- Hardware and software updates SHALL be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined and documented manner.

6.6.2 Security Management Controls

The configuration of the CA system as well as any modifications and upgrades SHALL be documented and controlled. There SHALL be a mechanism for detecting unauthorized modification to the CA software or configuration. A formal configuration management methodology SHALL be used for installation and ongoing maintenance of the CA operating at the Basic LOA or higher.. The CA software, when first loaded, SHALL be verified as being that supplied from the vendor as the version intended for use and with no modifications. The integrity of the software used for signing by the CA SHALL be verified by the CA management at least weekly (e.g., in conjunction with CARL publication). For CAs operating at the High LOA, integrity SHALL be verified daily.

6.6.3 Life Cycle Security Ratings

Intentionally left blank.

6.7 NETWORK SECURITY CONTROLS

The CA operational platform and its linked databases/directories SHALL be protected by a network guard, firewall or filtering router to guard against denial of service and intrusion attacks. Unused network ports and services SHALL be turned off. Any network software present MUST be necessary to the functioning of the CA.

The CPS SHALL define the network protocols and mechanisms required for operation of the CA or its linked databases/directories. Any boundary control devices used to protect the network on which PKI equipment is hosted SHALL deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Requirements for cryptographic modules are as stated above in Section 6.2.

7. CERTIFICATE AND CARL/CRL PROFILES

In order to promote interoperability, the CA SHOULD issue PKCs and CARL/CRLs that are compatible with the IETF RFC 2549 (or successor). The profiles for these documents SHALL be published or identified in the CA's applicable CPS(s). These profiles SHALL include the format, syntax, and semantics of each field used.

7.1 CERTIFICATE PROFILE

The CA SHALL issue X.509 version 3 (or higher) PKCs.

7.1.1 Version Numbers

X.509 version 3 PKCs MUST be identified with an integer "2" in the versionNumber field.

7.1.2 Certificate Extensions

Standard extensions, when populated, SHALL be described in an appropriate Certificate Profile. Certificate Profiles SHALL be documented or referenced in the CPS in such a manner that a Relying Party can locate an on-line copy of the profile for any PKC issued by the CA.

Whenever private extensions are used, they SHALL be identified and fully defined in the applicable CPS. Private extensions SHOULD be assigned appropriate OIDs.

CAs that support an OCSP service, either hosted locally or provided by an Authorized Responder, MUST provide for the inclusion of a value for a uniformResourceIndicator (URI) accessLocation and the OID value id-ad-ocsp for the accessMethod in the AccessDescription SEQUENCE of the AuthorityInfoAccess extension.

7.1.3 Algorithm Object Identifiers

PKCs issued under this CP SHALL use the following standard OIDs for signatures:

id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

PKCs under this CP will use the following standard OIDs for identifying the algorithm for which the subject key was generated:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

PKCs containing keys generated for use with DSA or for use with KEA SHALL be signed with id-dsa-with-sha1. Keys generated for use with RSA SHALL be signed using sha-1WithRSAEncryption.

7.1.4 Name forms

Where required as set forth above, the subject and issuer fields of the base PKC SHALL be populated with an X.500 Distinguished Name as documented in the CPS, with the attribute type as further constrained by [RFC2459]. DC components SHOULD be included.

7.1.5 Name constraints

Intentionally left blank.

7.1.6 Certificate policy object identifier

PKCs issued under this CP SHALL assert in the CertPolicyId field the OID appropriate to the Level of Assurance with which it was issued as provided in Section 1.2.

7.1.7 Usage of Policy Constraints extension

Authority PKCs issued by the CA SHOULD include the *PolicyMappings* extension to indicate how the CA’s LOAs map to the authorized CA’s LOAs. If these extensions are present, the Relying Party MUST make use of the mapping and MUST NOT assume any mapping that is not explicit in the PKC. If these extensions are not present, the Relying Party MAY assume that the LOAs indicated by the authorized CA have the same meaning as those of the authorizing CA.

7.1.8 Policy qualifiers syntax and semantics

The CPSuri policy qualifier SHALL contain a pointer to an on-line, digitally signed copy of the CPS under which the PKC was issued. The CPS SHALL include a URI reference to this CP as specified in Section 1.2.

7.1.9 Processing semantics for the critical certificate policy extension

Intentionally left blank.

7.1.10 Certificate Serial Numbers

Each PKC signed by the CA SHALL include an integer serial number unique among all PKCs issued by that CA. A given serial number SHALL NOT be reused even if an otherwise identical PKC is reissued.

7.2 CARL/CRL PROFILE

7.2.1 Version numbers

The CA SHALL issue X.509 version 2 (or higher) CARLs/CRLs.

7.2.2 CARL and CRL entry extensions

Detailed CARL/CRL profiles addressing the use of each extension SHALL be defined by the CA in corresponding CPS(s).

7.2.3 OCSP Services

If OCSP is supported by the CA, the CPS SHOULD document the OCSP services provided and the message formats supported. The CPS MUST define the timeliness of the certificate status data returned.

8. SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

These procedures apply equally to this CP and any associated CPS(s). The CA SHALL review this CP at least once every year. The CA SHOULD maintain and publish a Certificate Policy Plan that describes any anticipated changes to this CP. Errors, updates, or suggested changes to this CP SHALL be communicated to every Authorized CA and SHALL be available in the Repository to Subscribers. Such communication SHOULD include a description of the change, a change justification, and contact information for the person requesting the change.

All policy changes under consideration by the CA SHALL be published in the Repository. Any affected party may provide their comments to the CA by following the procedure described in the applicable CPS.

8.2 PUBLICATION AND NOTIFICATION POLICIES

8.2.1 Amendments Generally

The CA SHALL be entitled to amend this CP from time to time (prospectively and not retroactively). An amendment to this CP SHALL become effective sixty (60) days after publication in the Repository. Publication in the Repository SHALL be deemed notice to all affected parties.

8.2.2 Urgent Amendments Exception

If, notwithstanding the preceding paragraph, the CA publishes an Urgent amendment to this CP, it SHALL become effective immediately upon publication in the Repository. For purposes of sections 8.2.2 and 8.2.3, an amendment SHALL be deemed "Urgent" if, in the sole discretion of the CA, failure to make the amendment may result in a compromise of the CA or the PKI.

8.2.3 Assent to Amendments

In the case of an amendment that is not deemed "Urgent", a Subscriber's decision not to request revocation of a PKC prior to the effective date of an amendment SHALL constitute agreement to the amendment. In the case of an amendment that is deemed "Urgent", a Subscriber's decision not to request revocation of a PKC within fifteen (15) days following the publication of the amendment SHALL constitute agreement to the amendment. Upon agreement to the amendment, the OID within that PKC pointing to any older version of the CP will be deemed to point to the version as amended.

8.2.4 Maintenance of Prior Versions

Any prior version of this CP SHALL remain publicly available for at least 12 months after the expiration date of the last PKC referencing it. All prior versions that have been referenced in any PKC asserting a LOA of Basic or higher SHALL be archived permanently along with the beginning and ending dates that it was used.

8.3 CPS APPROVAL PROCEDURES

The term certification practice statement (CPS) is defined in the Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework as: "A statement of the practices, which a Certification Authority employs in issuing certificates." It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management. It SHALL detail the implementation of the corresponding certificate policy described in Section 2.1 above. The CPS is contained in a separate document and specifies how the CP will be implemented to ensure compliance with its provisions.

The PMA SHALL approve and cause to be digitally signed any CPS that refers to this CP as its governing policy.

8.4 WAIVERS

Not applicable.

9. BIBLIOGRAPHY

The following documents SHALL be used as guidance in interpretation of this CP to the extent that information in these documents are not inconsistent with this CP:

ABADSG Digital Signature Guidelines, 1996-08-01.
http://www.abanet.org/scitech/ec/isc/dsgfree.html.

FIPS 112 Password Usage, 1985-05-30
http://www.itl.nist.gov/fipspubs/fip112.htm

FIPS 140-1 Security Requirements for Cryptographic Modules, 1994-01-11
http://csrc.nist.gov/publications/fips/fips1401.pdf

FIPS 180-1 Secure Hash Standard, 1995-04-17
http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf

FIPS 186-2 Digital Signature Standard, 2001-01-27
http://csrc.nist.gov/publications/fips/fips186-2/fips186-2.pdf

FOIACT 5 U.S.C. 552, Freedom of Information Act.
http://www4.law.cornell.edu/uscode/5/552.html

Federal Certificate Profile DRAFT, April 2000
http://csrc.nist.gov/pki/documents/FPKI_Certificate_Profile_20000418.xls

ISO9594-8 Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997.
ftp://ftp.bull.com/pub/OSIdirectory/ITU/97x509final.doc

ITMRA 40 U.S.C. 1452, Information Technology Management Reform Act of 1996.
http://www4.law.cornell.edu/uscode/40/1452.html

NAG69C Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.

NSD42 National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990.
http://www.cpsr.org/cpsr/privacy/computer_security/nsd_42.txt
(redacted version)

NS4005 NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.

NS4009 NSTISSI 4009, National Information Systems Security Glossary, January

1999.

PKCS Public Key Cryptography Standards
http://www.rsasecurity.com/rsalabs/pkcs/index.html

PKCS-12 Personal Information Exchange Syntax Standard, April 1997.
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-12/

RFC 2510 Certificate Management Protocol, Adams and Farrell, March 1999.

RFC 2527 Certificate Policy and Certificate Practices Framework, Chokhani and Ford, March 1999.

Security Requirements for Certificate Issuing and Management Components, 3 November 1999, Draft

“Secure Electronic Commerce : Building the Infrastructure for Digital Signatures and Encryption”, Warwick Ford and Michael S. Baum, Prentice Hall, April 1997, ISBN: 0134763424

United States Department of Defense X.509 Certificate Policy, Version 5.0, 13 December 1999

10. GLOSSARY

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by the HEPKIPA or comparable Institution body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.

Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Authority certificate	A PKC that contains the distinguished name of the CA in the SubjectName field and contains the value TRUE in the BasicConstraints cA field and in which the KeyUsage keyCertSign bit is set. The cRLSign bit should be set also.
Authorized CA	A CA for which another CA signs an authority certificate in accordance with this CP.
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
CA	Certification Authority
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
CA Group	Includes all Persons comprising a CA, RA, PMA, and their parent organizations, and includes all employees, officers, directors, and contractors associated with the CA, RA and PMA.
CARL	Certificate Authority Revocation List
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG] As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Practices Statement" (CPS) referenced in the CPSuri field of an X.509 v.3 certificate
Certificate Management	A Certification Authority or a Registration Authority.

Authority (CMA)	
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs. The term "CA" as used in this CP includes Authorizing and Authorized CAs that operate under this CP.
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to subscribers.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).

Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Community	The community or group of Persons or other entities for which the CA will issue a PKC.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
COMSEC	Communications Security
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
CP	Certificate Policy
CPS	Certification Practice Statement
CPSuri	A PKC standard extension that provides a URI pointing to an on-line copy of the CA's CPS.
CRL	Certificate Revocation List
Cross-Certificate	A PKC used to establish a trust relationship between two CAs.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
CSOR	Computer Security Object Registry

Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	The length of the Validity Period.
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Employee	Any person employed by an Institution as defined above.
Encrypted Network	A network that is protected from outside access by NSA approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End Entity	Relying Parties and Subscribers.
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FED-STD	Federal Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
Firewall	Gateway that limits access between networks in accordance with

	local security policy. [NS4009]
FPKI	Federal Public Key Infrastructure
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile
FPKISC	Federal PKI Steering Committee
GPEA	Government Paperwork Elimination Act of 1998
HEBCA	Higher Education Bridge Certification Authority
HEBCA OA	Higher Education Bridge Certification Authority Operational Authority
HEBCA Operational Authority (HEBCA OA)	The Higher Education Bridge Certification Authority Operational Authority is the organization selected by the Higher Education Public Key Infrastructure Policy Authority to be responsible for operating the Higher Education Bridge Certification Authority.
HEPKIPA	Higher Education PKI Policy Authority
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Higher Education Bridge Certification Authority (HEBCA)	The Higher Education Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer to peer interoperability among Institution Principal Certification Authorities.
Higher Education Bridge Certification Authority Membrane	The Higher Education Bridge Certification Authority Membrane consists of a collection of Public Key Infrastructure components including a variety of Certification Authority PKI products, Databases, CA specific Directories, Border Directory, Firewalls, Routers, Randomizers, etc.
Higher Education Public Key Infrastructure Policy Authority (HEPKI PA)	The HEPKIPA is responsible for setting, implementing, and administering policy decisions regarding PKI interoperability among institutions using the HEBCA.

IETF	Internet Engineering Task Force
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]
Inside threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]

Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Memorandum of Agreement (MOA)	Agreement between the HEPKIPA and an Institution allowing interoperability between the Institution Principal CA and the HEBCA.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
MOA	Memorandum of Agreement (as used in the context of this CP, between an Institution and the HEPKIPA allowing interoperation between the HEBCA and Institution Principal CA)
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]

NIST	National Institute of Standards and Technology
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.
NSA	National Security Institution
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
Object Identifier (OID)	A unique specially formatted number that is composed of a most significant part assigned by an internationally recognized standards organization to a specific owner and a least significant part assigned by the owner of the most significant part. For example, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the Higher Education PKI they are used to uniquely identify policies and cryptographic algorithms and possibly other elements contained in a PKC.
OCSP	Online Certificate Status Protocol. See IETF RFC 2560.
OID	Object Identifier
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
Person	An individual or organizational entity, including but not limited to, a corporation, partnership, sole proprietor, trust, etc.

Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PIN	Personal Identification Number
PKC	Public Key Certificate. As used in this CP, refers to an object conforming to X.509v3 or higher.
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKI Sponsor	Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.
PKIX	Public Key Infrastructure X.509
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the HEBCA, the PMA is the HEPKIPA.
Principal CA	The Principal CA is a CA designated by an Institution to interoperate with the HEBCA. An Institution may designate multiple Principal CAs to interoperate with the HEBCA.
Privacy	Restricting access to subscriber or Relying Party information in accordance with Federal law and institution policy.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key MUST be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure	A set of policies, processes, server platforms, software and

(PKI)	workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
RA	Registration Authority
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.
Relying Party	A Person who has received information that includes a PKC and a digital signature verifiable with reference to a public key listed in the PKC, and is in a position to rely on that information.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
RFC	IETF Request For Comments
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

RSA	Rivest-Shamir-Adleman (encryption algorithm)
S/MIME	Secure Multipurpose Internet Mail Extension
Server	A system entity that provides a service in response to requests from clients.
SHA-1	Secure Hash Algorithm, Version 1
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
SSL	Secure Socket Layer
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A Subscriber is a Person that (1) either (a) is the Subject named or identified in a certificate issued to that Person or (b) is the owner or operator of an entity that is the Subject named or identified in a certificate issued to that Person, and (2) holds a private key that corresponds to the public key listed in the certificate.
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
System High	The highest security level supported by an information system. [NS4009]
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.

Trusted Agent	Entity authorized to act as a representative of an Institution in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
TSDM	Trusted Software Development Methodology
UPS	Uninterrupted Power Supply
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [NS4009]
U.S.C.	United States Code
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
URI	A Uniform Resource Identifier (URI) is a compact string of characters for identifying an abstract or physical resource. It is a superset of URLs and URNs and may include other UR types. See RFC2396.
URL	A Uniform Resource Locator (URL) refers to the subset of URI that identify resources via a representation of their primary access mechanism (e.g., their network "location"), rather than identifying the resource by name or by some other attribute(s) of that

	resource. See RFC1738 and RFC1808.
URN	Uniform Resource Name" (URN) refers to the subset of URI that are required to remain globally unique and persistent even when the resource ceases to exist or becomes unavailable. A URN differs from a URL in that it's primary purpose is persistent labeling of a resource with an identifier. See RFC2141.
Validity Period	The period of time during which a PKC is intended to be valid as of the time of issuance. This is specified as a pair of fields labeled “not before” and “not after” containing universal time indicators.
WWW	World Wide Web
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS 140-1]

11. ACKNOWLEDGEMENTS

This Certificate Policy was derived largely from the Federal Bridge Certificate Authority (FBCA) policy. We would like to specially thank Mr. Richard Guida, Chair of the Federal Public Key Infrastructure Steering Committee, for his help and encouragement.