Certificate Policy for External Certification Authorities

June 4, 2003

Version 2.0

Prepared By:

DoD Public Key Infrastructure Program Management Office

Approved:

John P Stenbit

Assistant Secretary of Defense
(Networks and Information Integration)

This page is intentionally left blank

TABLE OF CONTENTS

1 INTRODUCTION

This Certificate Policy (CP) governs the operation of a Public Key Infrastructure (PKI), consisting of products and services that provide and manage X.509 certificates for public-key cryptography. Certificates identify the individual named in the certificate, and bind that person to a particular public/private key pair. This Certificate Policy addresses the requirements for the External Certification Authorities (ECAs) that will issue certificates to Subscribers who have a need to conduct business primarily with the United States (US) Department of Defense (DoD). However, these certificates are not restricted to the conduct of business with the DoD.

The operation of programs that require services such as authentication, confidentiality, integrity, technical non-repudiation, and access control is supported and complemented by the use of public-key cryptography. As a system solution, the components share the burden of the total system security. The use of public key certificates does not add any security services in a poorly designed or implemented system. Thus, it is critical that a PKI is designed with appropriate security in order for the Relying Party to have confidence in the public key certificates issued by the PKI, i.e., have a confidence in binding between the Subscriber and the Subscriber's public key

Security management services provided by PKI include:

- Key Generation/Storage/Recovery;
- Certificate Generation, Update, Renewal, Re-key, and Distribution;
- Certificate Revocation List (CRL) Generation and Distribution;
- Directory Management of Certificate Related Items;
- Certificate token initialization/programming/management;
- Privilege and Authorization Management; and
- System Management Functions (e.g., security audit, configuration management, archive, etc.).

The security of these services is ensured by defining requirements on PKI activities, including the following:

- Subscriber identification and authorization verification;
- Control of computer and cryptographic systems;
- Operation of computer and cryptographic systems;
- Usage of keys and public-key certificates by Subscribers and Relying Parties; and
- Definition of rules to limit liability and to provide a high degree of certainty that the stipulations of this policy are being met.

The reliability of the public-key cryptography portion of the security solution is a direct result of the secure and trustworthy operation of an established PKI, including equipment, facilities, personnel, and procedures.

Electronic commerce is one important PKI application. The use of public key cryptography for electronic commerce applications should be determined on the basis of a review of the security services provided by the public key certificates, the value of the electronic commerce applications, and the risk associated with the applications.

1.1 OVERVIEW

The ECA Certificate Policy CP is the unified policy under which an approved ECA is established and operates. It does not define a particular implementation of PKI, nor the plans for future implementations or future Certificate Policies. This document will be reviewed and updated as described in Section 8, based on operational experience, changing threats, and further analysis.

This document defines the creation and management of X.509 Version 3 public-key certificates for use in applications requiring communication between networked computer-based systems. Such applications include, but are not limited to, electronic mail; transmission of unclassified information; signature of electronic forms; contract formation signatures; signature on mobile code in order verify the integrity and source of mobile code; and authentication of infrastructure components such as web servers, firewalls, and directories. The intended network backbone for these network security products is the Internet.

References and bibliography of related publications are included at the end of this document. Related publications contain information that forms the basis for PKI. A list of acronyms follows the references.

1.2 IDENTIFICATION

There are two levels of assurance in this policy, defined in subsequent sections. Each level of assurance has an object identifier (OID), to be asserted in certificates issued by Certification Authorities (CAs) who comply with the policy stipulations herein. The OIDs are registered under Computer Security Objects Registry (CSOR) maintained by the National Institute of Standards and Technology (NIST).

{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) csor(3) pki(2) cert-policy(1) eca-policies(12)}

id-eca-medium	ID::= {id-eca-policies 1}
id-eca-medium-hardware	ID::= {id-eca-policies 2}

1.3 COMMUNITY AND APPLICABILITY

The following sections introduce the PKI and community roles involved in issuing and maintaining public key certificates. These roles are described in detail in Section 5.2.

1.3.1 PKI Authorities

1.3.1.1 ECA Policy Management Authority

The ECA Policy Management Authority (EPMA) is established to:

- Oversee the creation and update of this CP and plans for implementing any accepted changes;
- Provide timely and responsive coordination to approved ECAs and Government Agencies through a consensus-building process;
- Review the Certification Practice Statements (CPS) of CAs that offer to provide services meeting the stipulations of this CP; and
- Review the results of CA compliance audits to determine if the CA are adequately meeting the stipulations of this CP and associated approved CPS documents, and make recommendations to the CAs regarding corrective actions, or other measures that might be appropriate, such as revocation of CA certificates or changes to this CP.

1.3.1.2 Certification Authority

A Certification Authority (CA) is an entity authorized by the EPMA to create, sign, and issue public key certificates. A CA is responsible for all aspects of the issuance and management of a certificate, including control over the registration process, the identification and authentication process, the certificate manufacturing process, publication of certificates, revocation of certificates, and re-key; and for ensuring that all aspects of the CA services and CA operations and infrastructure related to certificates issued under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy. CA is an inclusive term, and includes all types of CAs. Any CA requirement expressed in this Policy applies to all CA types unless expressly stated otherwise.

CAs that issue certificates under this policy to Subscribers must be subordinate to the ECA Root CA. The nature of the subordination shall be described in one or more CPSs that have been generated for that hierarchy, and implemented through procedure and certificate extensions. The CA to which a second CA is subordinate is called the second CA's "superior CA."

1.3.1.3 Registration Authority

A Registration Authority (RA) is an entity that enters into an agreement with a CA to collect and verify Subscribers' identity and information that is to be entered into public key certificates. The RA must perform its functions in accordance with a CPS approved by the CA and the EPMA.

1.3.1.4 Certificate Management Authority

Both CAs and RAs are considered "Certificate Management Authorities" (CMAs). This policy will use the term CMA when a function may be assigned to either a CA or a RA, or when a requirement applies to both CAs and RAs. The division of Subscriber registration responsibilities between the CA and RA may vary among implementations of this certificate policy. This division of responsibilities shall be described in the CA's CPS.

Server based Certificate Status Authorities (CSAs) such as Online Certificate State Protocol (OCSP) Responders and Simple Certificate Validation Protocol (SCVP) status providers operated by the ECA vendor are also considered CMAs.

ECA vendors shall be responsible for ensuring that all CMAs (i.e., the CA, CSAs, and RAs recognized by the CA) are in compliance with this CP.

1.3.2 Trusted Agents

ECAs may choose to use the services of Trusted Agents to assist CMAs in performing identity verification tasks. Trusted Agents do not have privileged access to CMA functions, but are considered agents of the CMA.

1.3.3 Related Authorities

CAs operating under this policy will require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The CA shall identify, in its CPS, the parties responsible for providing such services, and the mechanisms used to support these services. More detail is given in Section 5.2.

1.3.4 End Entities

1.3.4.1 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate, and who asserts that it uses its key and certificate in accordance with this policy. ECA Subscribers are limited to the following categories of entities:

- Employees of businesses acting in the capacity of an employee and conducting business with a US government agency at local, state or Federal level;
- Employees of state and local governments conducting business with a US government agency at local, state or Federal level;
- Employees of foreign governments or organizations conducting business with a US Government agency at local, state or Federal level;

- Individuals communicating securely with a US government agency at local, state or Federal level; and
- Workstations, guards and firewalls, routers, trusted servers (e.g., database, FTP, and WWW), and other infrastructure components communicating securely with or for a US government agency at local, state or Federal level. These components must be under the cognizance of humans, who accept the certificate and are responsible for the correct protection and use of the associated private key.

CAs are technically Subscribers to the PKI; however, the term Subscriber as used in this document refers only to those who request certificates for uses other than signing and issuing certificates.

1.3.4.2 Relying Parties

A Relying Party is the entity who, by using another's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate, relies on the validity of the binding the Subscriber's name to a public key. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use and does so at their own risk.

1.3.5 Applicability

The PKI is intended to support the following security services: *confidentiality*, *integrity*, *authentication* and *technical non-repudiation.* The PKI supports these security services by providing Identification and Authentication (I&A), integrity, and technical non-repudiation through digital signatures, and confidentiality through key exchange. These basic security services support the long-term integrity of application data, but may not by themselves provide a sufficient integrity solution for all application circumstances. For example, when a requirement exists to verify the authenticity of a signature beyond the certificate validity period, such as contracting, other services such as trusted archival services or trusted timestamp may be necessary. These solutions are application based, and must be addressed by Subscribers and Relying Parties. The PKI provides support of security services to a wide range of applications that protect various types of information, up to and including sensitive unclassified information.

A single solution providing support to every application would appear to be desirable but because of different legal, security and national policy requirements for protection of the different categories of information, the most cost-effective solution is one that supports multiple assurance levels. Applicability statements in this policy are provided as guidance; applications and relying parties may require different levels of assurances.

1.3.5.1 Level of Assurance

The level of assurance associated with a public key certificate is an assertion by a CA of the degree of confidence that a Relying Party may reasonably place in the binding of a Subscriber's public key to the identity and privileges asserted in the certificate. Assurance level depends on the proper registration of Subscribers and the proper generation and management of the certificate and associated private keys, in accordance with the stipulations of this policy. Personnel, physical, procedural, and technical security controls contribute to the assurance level of the certificates issued by a certificate management system.

1.3.5.2 Factors in Determining Usage

The amount of reliance a relying party chooses to place on the certificate will be determined by various risk factors. Specifically, the value of the information, the threat environment, and the existing protection of the information environment are used to determine the appropriate level of assurance of certificates required to protect and authenticate the information.

1.3.5.3 Threat

Threat is any circumstance or event with the potential to cause harm. In terms of information systems, harm includes destruction, disclosure, or modification of data, processes, or processing components. Threats to systems include environmental disasters, physical damage, system penetration, violation of authorization, human error, and communications monitoring or tampering.

1.3.5.4 General Usage

This section contains definitions for two levels of assurance, and guidance for their application. The guidance is based on the previous discussion of information value and environmental protection. Emphasis is placed on two types of activity: integrity and access control to information considered sensitive, and information related to electronic financial transactions and other e-commerce. The final selection of the security mechanisms and level of strength and assurance requires a risk management process that addresses the specific mission and environment. This risk analysis should be carried out by each relying party.

Medium Assurance: This level is intended for applications handling sensitive medium value information, which may include:

- Non-repudiation for small and medium value financial transactions other than transactions involving issuance or acceptance of contracts and contract modifications;
- Authorization of payment for small and medium value financial transactions;
- Authorization of payment for small and medium value travel claims;
- Authorization of payment for small and medium value payroll; and
- Acceptance of payment for small and medium value financial transactions.

Medium Hardware Assurance: This level is intended for all applications operating in environments appropriate for medium assurance but which require a higher degree of assurance and technical non-repudiation.

- All applications appropriate for medium assurance certificates;
- Mobile code signing; and
- Applications performing contracting and contract modifications.

1.4 CONTACT DETAILS

1.4.1 Specification Administration Organization

The EPMA is responsible for the definition, revision and promulgation of this policy. The EPMA is the Office of the Assistant Secretary of Defense for Networks and Information Integration, and its designees.

1.4.2 Contact Information

Questions regarding this CP should be directed to

EPMA
9800 SAVAGE RD STE 6737
FT MEADE MD 20755-6737

1.4.3 Person Determining Certification Practice Statement Suitability for the Policy

The EPMA shall determine the suitability of any CPS to this policy.

2 GENERAL PROVISIONS

2.1 OBLIGATIONS

2.1.1 CA Obligations

A CA, who issues certificates that assert a policy defined in this document shall conform to the stipulations of this document, including:

- Providing to the EPMA a CPS, as well as any subsequent changes, for conformance assessment;
- Conforming to the stipulations of this CP and the approved CPS;
- Ensuring that registration information is accepted only from RAs who understand and are obligated to comply with this policy;
- Including only valid and appropriate information in the certificate, and maintaining evidence that due diligence was exercised in validating that information contained in the certificate;
- Ensuring that obligations are imposed on Subscribers in accordance with Section 2.1.4, and that Subscribers are informed of the consequences of not complying with those obligations,
- Revoking the certificates of Subscribers found to have acted in a manner counter to Subscriber obligations;
- Notifying Subscribers and making public for the benefit of Subscribers and Relying Parties any changes to the CA operations that may impact interoperability or security (e.g., extending the life of the self-signed root certificate);
- Operating or providing for the services of an on-line repository that satisfies the obligations under Section 2.1.6, and informing the repository service provider of those obligations if applicable; and
- Posting certificates and CRLs to the repository.

A CA who is found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 2.7.5.

2.1.2 RA Obligations

An RA who performs registration functions as described in this policy shall comply with the stipulations of this policy and comply with a CPS approved by the EPMA for use with this policy. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities.

The division of PKI duties between the CA and RA may vary among implementations of this certificate policy as provided in the CA's CPS. For example, the RA may collect information for the CA only, or it may build the certificate for the CA to sign. CAs are ultimately responsible for ensuring that the certificates they sign are generated and managed in accordance with this Policy, and shall ensure that certificate generation, management, and revocation functions are performed only by those who understand the associated certificate policy requirements, and who agree to abide by them. Security requirements imposed on the CA are likewise imposed on any RAs to the extent that the RAs are responsible for the information collected.

2.1.3 Trusted Agent Obligations

A Trusted Agent shall perform Subscriber identity verification in accordance with this CP and in accordance with the ECA's CPS approved by the EPMA for use with this policy.

2.1.4 Subscriber Obligations

Subscribers shall:

- Accurately represent themselves in all communications with the PKI;
- Protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements, and local procedures;
- Notify, in a timely manner, the CMA that issued their certificates upon suspicion that their private keys are compromised or lost. Such notification shall be made directly or indirectly through mechanisms consistent with this CP and the CA's CPS; and
- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates.

PKI Sponsors (as described in Section 5.2.1.6) assume the obligations of Subscribers for the certificates associated with their components.

2.1.5 Relying Party Obligations

Parties who rely upon the certificates issued under a policy defined in this document shall:

- Perform a risk analysis to decide whether the level of assurance provided by the certificate is adequate to protect the Relying Party based upon the intended use;
- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- Check each certificate for validity, using procedures described in the X.509 standard [ISO 9594-8], prior to reliance;

- Establish trust in the CA who issued a certificate by verifying the certification path in accordance with the guidelines set by the X.509 Version 3 Amendment;
- Preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data. Note: data format changes associated with application upgrades may invalidate digital signatures and shall be avoided.

2.1.6 Repository Obligations

Repositories that support a CA in posting information as required by this policy shall:

- Maintain availability of the information as required by the certificate information posting and retrieval stipulations of this policy; and
- Provide access control mechanisms sufficient to protect repository information as described in Section 2.6.3.

2.1.7 CSA Obligations

A CSA, who provides revocation status and/or complete validation of certificates that assert a policy defined in this document shall conform to the stipulations of this document, including:

- Providing to the EPMA a CPS, as well as any subsequent changes, for conformance assessment;
- Conforming to the stipulations of this CP and the approved CPS;
- Ensuring that certificate and revocation information is accepted only from valid ECAs; and
- Including only valid and appropriate response, and to maintain evidence that due diligence was exercised in validating the certificate status.

A CSA who is found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 2.7.5.

2.2 LIABILITY

2.2.1 Warranties and Limitations on Warranties

The ECA, acting as the subordinate CA, shall warrant that their procedures are implemented in accordance with this CP and the ECA's CPS, and that any certificates issued that assert the policy OIDs identified in this CP were issued in accordance with the stipulations of this policy.

The ECA shall warrant that any RA or Trusted Agent will operate in accordance with the applicable sections of this CP and the ECA's CPS.

2.2.2 Damages Covered and Disclaimers

Other than the warranties included in Section 2.2.1, ECAs may disclaim any warranties or obligations of any type concerning the accuracy of information provided by a Subscriber to the ECA, provided that the procedures stated in the ECA's CPS were followed and the procedures were in compliance with this CP. Furthermore, ECAs may disclaim any and all liability for negligence and lack of reasonable care on the parts of Subscribers and Relying Parties.

2.2.3 Loss Limitations

The ECA shall identify in its CPS limits of losses due to operations at variance with its procedures defined in its CPS. The limit for losses per transaction due to improper actions by the ECA, or its RAs, or Trusted Agents shall be at least $1,000 (USD). The limit for losses per incident due to improper actions by the ECA, or its RAs or Trusted Agents shall be at least $1 million (USD). The ECA may disclaim any liability for loss due to use of certificates it issues, if the certificate was issued in accordance with this CP and the ECA's CPS.

2.2.4 Other Exclusions

An ECA may state, in its CPS, other exclusions that do not conflict with this certificate policy.

2.2.5 US Federal Government Liability

Subscribers and Relying Parties shall have no claim against the US Federal Government arising from use of the Subscriber's certificate or a CMA's determination to terminate a certificate. In no event will the Government be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued or revoked by a CA approved under this CP.

The ECA shall have no claim for loss against the EPMA, including but not limited to the revocation of the ECA's certificate.

Subscribers and Relying Parties shall have no claim against the US Federal Government arising from erroneous certificate status information provided by the servers and services operated by the ECA and by the US Federal Government.

2.3 FINANCIAL RESPONSIBILITY

2.3.1 Indemnification by Relying Parties and Subscribers

Agents of an ECA (e.g., RA, Trusted Agents, etc.) assume no financial responsibility for improperly used certificates.

2.3.2 Fiduciary Relationships

Issuance of certificates in accordance with its CPS does not make an ECA, or any RA, an agent, fiduciary, trustee, or other representative of Subscribers or Relying Parties.

2.3.3 Administrative Processes

ECAs shall document any applicable provisions regarding financial responsibilities, such as accounting or auditing.

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1 Governing Law

This Policy shall be governed by the laws of the United States of America.

2.4.2 Severability of Provisions, Survival, Merger, and Notice

Should it be determined that one section of this policy is incorrect or invalid, the other sections shall remain in effect until the policy is updated. Requirements for updating this policy are described in Section 8. Responsibilities, requirements, and privileges of this document are merged to the newer edition upon release of that newer edition.

2.4.3 Dispute Resolution Procedures

The EPMA shall be the sole arbiter of disputes over the interpretation or applicability of this CP.

2.5 FEES

Subscription fees to be paid by subscribers may be published or established contractually by ECAs. ECAs shall make current certificates and current revocation information available to

Relying Parties at no charge. ECAs may charge fees to Relying Parties for providing archived certificates and archived revocation information.

2.6 PUBLICATION AND REPOSITORY

2.6.1 Publication of CA Information

Each CA shall provide an on-line repository that is available to Subscribers and Relying Parties and that contains:

- Issued encryption certificates that assert one or more of the policy OIDs listed in this CP;
- The most recently issued CRL;
- The CA's certificate for its certificate signing key;
- The CA's certificate for its CRL signing key;
- The CPS under which the CA operates; and
- A copy of this Policy, including any waivers granted to the CA by the EPMA.

2.6.2 Frequency of Publication

Certificates are published following Subscriber acceptance as specified in Section 4.3 and proof of possession of private key as specified in Section 3.1.7. The CRL is published as specified in Section 4.4.3.1. All information to be published in the repository shall be published promptly after such information becomes available to the CA. The CA shall specify in its CPS time limits within which it will publish various types of information.

2.6.3 Access Controls

A CA shall protect any repository information not intended for public dissemination or modification.

2.6.4 Repositories

The location of any publication will be one that provides access to Subscribers and Relying Parties in accordance with the security requirements as stated in this CP.

2.7 COMPLIANCE AUDIT

2.7.1 Frequency of Entity Compliance Audit

All CAs shall conduct an annual compliance audit. Additionally, all CAs have the right to require periodic and aperiodic inspections of subordinate CMA operations to validate that the subordinate CMA is operating in accordance with the security practices and procedures described in the subordinate's CPS. The CA will state the reason for any aperiodic inspection.

The EPMA has the right to require aperiodic compliance audits of CMAs asserting this policy. The EPMA shall state the reason for any aperiodic compliance audit.

2.7.2 Identity/Qualifications of Compliance Auditor

The auditor must demonstrate competence in the field of security compliance audits of Information Technology (IT) systems, and must be thoroughly familiar with the CMA's CPS. The compliance auditor must perform CA or IT system compliance audits as a primary responsibility. In addition, the compliance auditor shall have expertise in information security, cryptography and PKI.

2.7.3 Compliance Auditor's Relationship to Audited Party

The compliance auditor and CA shall have a contractual relationship for the performance of the compliance audit, or be sufficiently organizationally separated from the audited CA to provide an unbiased, independent evaluation.

2.7.4 Topics Covered by Compliance Audit

The purpose of a compliance audit shall be to verify that the CA has in place a system to assure the quality of the CA services that it provides, and that it complies with all of the requirements of this CP and its CPS. All aspects of the CA operation related to this CP shall be subject to compliance audit inspections.

2.7.5 Actions Taken as a Result of Deficiency

When the compliance auditor finds a discrepancy between a CMA's operation and the stipulations of its CPS, the following actions must occur:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the parties identified in Section 2.7.6 of the discrepancy; and

- The CMA will propose a remedy, including expected time for completion, to the EPMA.

The EPMA will determine the appropriate remedy, up to and including revocation or non-recognition of the CMAs certificate. Upon correction of the deficiency, the EPMA may reinstate the CMA.

2.7.6 Communication of Results

The compliance auditor shall report the results of a compliance audit to the EPMA. The results will be reported to the audited CA and its superior CA if applicable. The implementation of remedies shall be communicated to the appropriate authority, i.e., the EPMA and the superior CA who issued a certificate to the audited entity. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

2.8 CONFIDENTIALITY

2.8.1 Types of Information to be Protected

A certificate should only contain information that is relevant and necessary to effect secure transactions with the certificate. For the purpose of proper administration of the certificates, a CMA may request non-certificate information to be used in managing the certificates within an organization (e.g., identifying numbers, business or home addresses and telephone numbers). Any such information shall be explicitly identified in a CPS. All information stored locally on the CA equipment and not in the repository shall be handled as sensitive, and access shall be restricted to those with an official need-to-know in order to perform their official duties or in accordance with Section 2.8.2 below.

2.8.2 Information Release Circumstances

A CA will not disclose certificate or certificate-related information to any third party unless authorized by this Policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. Any request for release of information shall be authenticated by the CA.

2.9 INTELLECTUAL PROPERTY RIGHTS

The ECA may maintain ownership of public key certificates. Any such claim shall be made in the ECA CPS. All private keys shall be owned by Subscribers and their organizations. This stipulation, however, shall not prevent ECA from offering key escrow services for private encryption keys.

3 IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

3.1.1 Types of Names

All CAs shall be able to generate and sign certificates that contain an X.500 Distinguished Name (DN).

Certificates issued to CAs and RAs shall use the X.500 DN form.

Certificates may additionally assert an alternate name form. Details related to this requirement are provided in Section 7.1.4.

3.1.2 Need for Names to be Meaningful

Names shall identify the person or object to which they are assigned. The CMA shall ensure that an affiliation exists between the Subscriber and any organization that is identified by any component of any name in its certificate.

When DNs are used, the common name shall represent the Subscriber in a way that is easily understandable for humans. For people, this will typically 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).

The EPMA will establish one or more authorities for the creation of DNs. ECAs will coordinate with such an authority to determine the proper elements for a given Subscriber.

Each ECA asserting this policy shall only sign certificates with subject names from within a name-space approved by the EPMA. ECA's shall not certify other CAs.

3.1.3 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are contained in the applicable certificate profile (see Section 7.1.2), and are established by the EPMA established naming authority.

3.1.4 Uniqueness of Names

Name uniqueness across ECAs must be enforced. Wherever practical, X.500 DNs allocated from the EPMA designated naming authority shall be used, and the CAs and RAs shall enforce name uniqueness within the X.500 name space that they have been authorized to use. When other name forms are used, they too must be allocated such that name uniqueness across the ECA program is ensured. A CA shall document in its CPS what name forms will be used, how the CA will interact with EPMA, and how they will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (i.e., if "Joe Smith" leaves a CA's community of Subscribers, and a new, different "Joe Smith" enters the community of Subscribers, how will these two people be provided unique names).

The assignment of the unique DN for CA is the responsibility of the EPMA designated naming authority. The ECA Root CA CPS shall describe how the ECA names are kept unique.

The assignment of unique DN for Subscribers is the responsibility of the ECA. The ECA may append serial number or other information to make the DN unique. The ECA shall ensure the following for Subscriber names:

- The name contains the Subscriber identity and organization affiliation (if applicable) that is meaningful to humans;
- The naming convention shall be described in the ECA CPS; and
- The ECA shall obtain the EPMA naming authority approval for the naming convention.

This does not prevent devices from sharing a Fully Qualified Domain Name (FQDN) as common name.

3.1.5 Name Claim Dispute Resolution Procedure

The CMA shall investigate and correct if necessary any name collisions brought to its attention. If appropriate, the CMA shall coordinate with and defer to the EPMA naming authority.

3.1.6 Recognition, Authentication, and Role of Trademarks

A corporate entity is not guaranteed that its name will contain a trademark if requested. The ECA shall not knowingly issue a certificate including a name that a court of competent jurisdiction has determined infringes the trademark of another. The ECA is not subsequently required to issue that name to the rightful owner if it has already issued one sufficient for identification.

3.1.7 Method to Prove Possession of Private Key

In all cases where the Subscriber generates keys, the Subscriber shall be required to prove, to the CMA, possession of the private key that corresponds to the public key in the certificate request. For signature keys, this proof of possession may be done by signing the request. For encryption keys, the CA or RA may encrypt the Subscriber's certificate in a confirmation request message. The Subscriber can then decrypt and return the certificate to the CA or RA in a confirmation message. The EPMA may determine other mechanisms that are at least as secure as those cited here to be acceptable.

In the case where key is generated directly on the Subscriber's token, or in a key generator that benignly transfers the key to the Subscriber's token, then the Subscriber is in possession of the private key at the time of generation or transfer. If the Subscriber is not in possession of the token when the key is generated, then the token shall be delivered to the Subscriber via an accountable method (see Section 4.2.1).

3.1.8 Authentication of Organization Identity

Requests for certificates in the name of an organization shall include the organization name, address, and documentation of the existence of the organization. The CMA shall verify this information, in addition to the authenticity of the requesting representative, and that representative's authorization to act in the name of the organization.

Use of organization certificates shall be addressed in the ECA's CPS and shall preclude their use where individual non-repudiation is required.

3.1.9 Authentication of Individual Identity

3.1.9.1 In-Person Authentication

The CMA shall ensure that the applicant's identity information and public key are bound adequately. Each CMA shall specify in its CPS procedures for authenticating a Subscriber's identity. Additionally, a CMA shall record the process that was followed for each certificate. At a minimum, process documentation must include:

- The identity of the person performing the identification;
- A signed declaration by that person that he verified the identity of the Subscriber as required by this certificate policy;
- The method used to authenticate the individual's identity, including identification type and unique numeric or alphanumeric identifier if appropriate; and
- The date of the verification.

Additionally, the process documentation must include a declaration of identity. The declaration shall be signed with a handwritten signature by the certificate applicant in the presence of the person performing the identity authentication.

Applicant identity proofing requires the applicants to provide two official identification credentials, at least one of which must be a photo ID such as a drivers license. As an alternative to presentation of identification credentials, other mechanisms of equivalent or greater assurance (such as comparison of biometric data to identities pre-verified to the standards of this policy, and obtained via authenticated interaction with secured databases) may be used.

For Medium Assurance, the applicant's identity must be personally verified prior to the applicant's certificate being enabled. The applicant shall appear personally before either:

- A CMA;
- A Trusted Agent personally approved by the CMA; or
- A person certified by a US State or Federal Government as being authorized to confirm identities (such as Notaries Public), that uses a stamp, seal, or other mechanism to authenticate their identity confirmation.

The applicant shall appear before one of the required identity verifiers no more than 30 days prior to application of the CA's signature to the applicant's certificate.

For Medium Hardware Assurance, the applicant's identity shall be personally verified by a CMA prior to the applicant's certificate being enabled. There are two ways to meet this requirement:

- The applicant shall personally appear before the CMA, or a Trusted Agent personally approved by the CMA, at any time prior to application of the CA's signature to the applicant's certificate; or
- When private keys are delivered to Subscribers via hardware tokens, the Subscribers shall personally appear before the CMA to obtain their tokens or token activation data.

Minors and others not competent to perform face-to-face registration alone shall be accompanied by a person already certified by the PKI, who will present information sufficient for registration at the level of the certificate being requested, for both himself and the person accompanied.

3.1.9.2 Electronic Authentication

Certificates may be issued on the basis of electronically authenticated (using a current, valid PKI signature certificate issued by that CA and associated private key) Subscriber requests, subject to the following restrictions:

- The assurance level of the new certificate shall be the same or lower than the assurance level of the existing certificate used as an authentication credential;
- The DN of the new certificate shall be identical to the DN of the certificate used as the authentication credential;

- Information in the new certificate that could be used for authorization shall be identical to that of the certificate used as the authentication credential;
- The expiration date of the new certificate shall be no later than the next required in-person authentication date associated with the certificate used as the authentication credential;
- The in-person authentication date associated with a new certificate shall be no later than the in-person authentication date associated with the certificate used for authentication; and
- The validity period of the new certificate shall not be greater than the maximum validity period requirements of this CP for that type of certificate.

Electronically authenticated issuance is similar to certificate re-key (section 3.2.1) except that the new certificate is valid concurrently with the existing certificate but with a potentially different expiration date

3.1.10 Authentication of Component Identities

Some computing and communications components (routers, firewalls, etc.) may be named as certificate subjects. In such cases, the component must have a human PKI Sponsor as described in Section 5.2.1.6. The PKI Sponsor is responsible for providing the CMA, or to CMA approved Trusted Agents correct information regarding:

- Equipment identification;
- Equipment public keys;
- Equipment authorizations and attributes (if any are to be included in the certificate); and
- Contact information to enable the CMA to communicate with the PKI sponsor when required.

The CMA or an authorized Trusted Agent shall authenticate the validity of any authorizations to be asserted in the certificate, and shall verify source and integrity of the data collected to an assurance level commensurate with the certificate 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 PKI sponsors (using certificates of equivalent or greater assurance than that being requested); or
- In person registration by the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 3.1.9.

3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY

3.2.1 Certificate Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. This weakens the assurance provided to a Relying Party that the unique binding between a key and its named Subscriber is valid. Therefore, it is important that Subscribers periodically obtain new keys and re-establish their identities. Re-keying a certificate means that a new certificate is created that is identical to the old one, except that the new certificate 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.

Re-key requests for medium assurance certificates can be authenticated on the basis of existing Subscriber certificates twice, after which Subscribers must present themselves for in-person identity proofing, in accordance with Section 3.1. In-person registration is periodically required to limit the damage caused by unreported key compromises. Medium assurance certificate Subscribers may identify themselves in-person, then request re-key authenticating using their existing certificates in year three, and again in year six. In year nine, Subscribers must request new certificates in person. Applications for re-key using existing certificates shall result in new certificates asserting the same level of assurance as that asserted in the old certificate that was used to authenticate the re-key request.

Medium hardware assurance certificates may be renewed or updated on the basis of electronically authenticated Subscriber requests. Every three years, in-person authentication is required, in accordance with Section 3.1.

Any ECA who includes authorizations in a certificate, including any conveyed or implied by the subject's DN, shall document in its CPS the mechanisms used to notify the ECA of the withdrawal of authorization. Withdrawal of authorization shall result in revocation of the old certificate and, if necessary, the issuance of a new certificate with a different public key and the appropriate authorizations.

The key lifetimes given are maximums. An ECA may always require shorter lifetimes. The following key lifetimes are for Subscribers; ECA key lifetimes are provided in Section 4.7.

Medium Assurance	Signature re-key every three years Confidentiality re-key every three years Identity established through use of current signature key Must prove possession of corresponding private key May authenticate to PKI for re-key with current key twice
Medium Hardware Assurance	Signature re-key every three years Confidentiality re-key every three years Identity established in person Must prove possession of corresponding private key

3.2.2 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and authorizations as the old one, but a new, extended validity period and a new serial number. Certificates may be renewed as a means of CRL size management. A certificate may be renewed if the public key has not reached the end of its validity, the associated private key has not been compromised, and the Subscriber name and attributes are correct. Thus, a CMA may choose to implement a three-year re-key period with an initial issue and two annual renewals. The old certificate need not be revoked, but must not be further re-keyed, renewed, or updated.

3.2.3 Certificate Update

Updating a certificate means creating a new certificate that has the same or a different key, a different serial number, and differs in one or more other fields, from the old certificate. For example, an ECA may choose to update a certificate of a Subscriber who gains an authorization. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

The ECA shall authenticate the validity of any authorizations using the same means as for the initial authorization or means of equal or greater security and assurance.

3.3 OBTAINING A NEW CERTIFICATE AFTER REVOCATION

For all levels of assurance, Subscribers requesting certificates after revocation must meet initial registration requirements.

3.4 REVOCATION REQUEST

Revocation requests must be authenticated; see Section 4.4.1.3. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

4 OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

This Policy identifies the minimum requirements and procedures that are necessary to support trust in the PKI, and to minimize imposition of specific implementation requirements on CMAs, Subscribers, and Relying Parties.

The applicant and the CMA must perform the following steps when an applicant applies for a certificate:

- Establish and record identity of Subscriber (per Section 3.1);
- Record the subscriber's basis for requesting a certificate, including a point of contact for verification, if required;
- Obtain a public/private key pair for each certificate required;
- Establish that the public key forms a functioning key pair with the private key held by the Subscriber (per Section 3.1.7); and
- Provide a point of contact for verification of any roles or authorizations requested.

These steps may be performed in any order that is convenient for the CMA and Subscribers, and that does not defeat security; but all must be completed prior to certificate issuance. All communications among CMAs supporting the certificate application and issuance process shall be authenticated and protected from modification using mechanisms commensurate with the requirements of the data to be protected by the certificates being issued (i.e., communications supporting the issuance of medium assurance certificates shall be protected using medium assurance certificates, or some other mechanism of equal or greater strength). Any electronic transmission of shared secrets shall be protected (e.g., encrypted) using means commensurate with the requirements of the data to be protected by the certificates being issued.

ECAs implementing this CP shall not certify other CAs with the exception of the ECA Root CA. The ECA Root CA shall only certify ECAs. The ECA Root CA may cross-certify with other domains such as the Federal Bridge Certification Authority (FBCA) upon EPMA approval.

Requests by ECAs for CA certificates shall be submitted to the EPMA using the contact provided in Section 1.4, and shall be accompanied by a CPS written to the format of the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [RFC2527].

The EPMA will evaluate the submitted CPS for acceptability. The EPMA may require an initial compliance audit, performed by parties of the EPMA's choosing, to ensure that the CMA is prepared to implement all aspects of the submitted CPS, prior to the EPMA authorizing the CMA to issue and manage certificates asserting the ECA CP OIDs.

CAs shall only issue certificates asserting ECA CP OIDs upon receipt of written authorization from the EPMA, and then may only do so within the constraints imposed by the EPMA or its designated representatives.

4.1.1 Delivery of Subscriber's Public Key to Certificate Issuer

Public keys shall be delivered to the certificate issuer in a way that binds the applicant's verified identification to the public key being certified. This binding shall be accomplished using means that are as secure as the security offered by the keys being certified. The binding shall be accomplished using cryptographic, physical, procedural, and other appropriate methods. The methods used for public key delivery shall be stipulated in the CPS.

In those cases where public/private key pairs are generated by the CMA on behalf of the Subscriber, the CMA 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, and that the token is not activated prior to receipt by the proper Subscriber.

4.2 CERTIFICATE ISSUANCE

Upon receiving the request, the CMA will:

- Verify the identity of the requestor;
- Verify the authority of the requestor and the integrity of the information in the certificate request;
- Build and sign a certificate, if all certificate requirements have been met (in the case of a RA, have the CA sign the certificate); and
- Make the certificate available to the Subscriber.

The certificate request may contain an already built ("to-be-signed") certificate. This certificate will not be signed until all verifications and modifications, if any, have been completed to the ECA's satisfaction. If a certificate request is denied, then the ECA will not sign the requested certificate, and will work with the RA to resolve the problem.

While the Subscriber may do most of the data entry, it is still the responsibility of the CMA to verify that the information is correct and accurate. This may be accomplished either through a system approach linking databases containing personnel information or through personal contact with the program's attribute authority (as put forth in the CMA's CPS). If databases are used to confirm Subscriber attributes, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance specified for the certificates conveying the Subscriber attributes.

CMAs shall verify all authorization and other attribute information received from an applicant. In most cases, the RA is responsible for verifying applicant data, but if ECAs accept applicant data directly from applicants, then the ECA is responsible for verifying the applicant data.

Information regarding attributes shall be verified via those offices or roles that have authority to assign the information or attribute. Relationships with these offices or roles shall be established prior to commencement of ECA duties, and shall be described in the ECA CPS.

4.2.1 Delivery of Subscriber's Private Key to Subscriber

In most cases, a private key will be generated and remain within the cryptographic boundary of a cryptographic module. If the owner of the module generates the key locally, then there is no need to deliver the Subscriber's private key. If the key is generated on a hardware cryptographic module elsewhere, then the hardware cryptographic module must be delivered to the Subscriber. Accountability for the location and state of the hardware cryptographic module must be maintained until the Subscriber is in possession of it. The Subscriber shall acknowledge receipt of the hardware cryptographic module.

When keyed hardware tokens are delivered to Subscribers, the delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers. The CMA must maintain a record of validation for receipt of the token by the Subscriber. When any mechanism that includes a shared secret (e.g., a password or pin) is used, the mechanism shall ensure that the applicant and the CMA are the only recipients of this shared secret.

Private keys associated with medium assurance certificates may be generated and stored in software cryptographic modules. When the Subscriber generates these keys locally, there is no need to deliver them. If the private keys are generated elsewhere, they must be transmitted or delivered to the Subscriber in encrypted form and the encryption method ensures that only the Subscriber may possess the plaintext private signature keys. The encryption must be of strength commensurate with that of the key being protected. The Subscriber shall acknowledge receipt of the private signature key. The originally generated private signature key shall be destroyed. Mechanisms shall ensure that additional copies of software keys are not maintained except as allowed in this Certificate Policy.

Only those authorized by the ECA's key recovery practice statement may access private keys associated with encryption certificates.

Public-key certificates shall be issued to persons whenever possible. For cases where there are several persons acting in one capacity, a certificate may be issued that corresponds to a private key that is shared by multiple Subscribers. (Note that certificates corresponding to private keys held by multiple Subscribers shall not be used for contracting or e-commerce applications). In these cases:

- An individual shall be designated in writing to be responsible as the PKI Sponsor for ensuring control of the private key, including maintaining a list of Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time;
- The list of those holding the shared private key must be provided to, and retained by, the ECA and RA; and

- The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of this Policy (e.g., key generation, private key protection, Subscriber obligations, etc.).

4.2.2 CA Public Key Delivery to Users

The PKI and the Relying Parties must work together to ensure the authenticated and integral delivery of Trusted Certificates. Acceptable methods for Trusted Certificate delivery include but are not limited to:

- ECAs or RAs loading Trusted Certificates onto tokens delivered to Relying Parties via secure mechanisms;
- Secure distribution of Trusted Certificates through secure out-of-band mechanisms;
- Comparison of certificate hashes or fingerprints against Trusted Certificate hashes or fingerprints made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and
- Loading trusted certificates from web sites secured with a currently valid ECA certificate of equal or greater assurance level than the certificate being downloaded. The ECA certificate must have a different trust anchor than the one being loaded. The Subscriber must have received that trust anchor using trusted certificate delivery described herein.

4.3 CERTIFICATE ACCEPTANCE

Before an ECA allows a Subscriber to make effective use of its private key, a CMA shall:

- Explain to the Subscriber its responsibilities as defined in Section 2.1.3;
- Inform the Subscriber of the creation of a certificate and the contents of the certificate;
- Require the Subscriber to indicate acceptance of its obligations and its certificate, with a handwritten or digital signature[1];
- Notify the Subscriber if their decryption private key is escrowed; and
- Document the Subscriber's acceptance of its responsibilities and its certificate.

The ordering of this process, and the mechanisms used, will depend on factors such as where the key is generated and how certificates are posted. In the case of non-human components (router, firewalls, etc.), the PKI Sponsor (as defined in Section 5.2.1.6) shall perform the functions of the Subscriber.

[1] This signature could be obtaining in conjunction with Subscriber Identity Declaration signature described in Section 3.1.9.1. For example, the subscriber could sign one form that contains clauses for declaration of identity and for acceptance of subscriber obligations.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Revocation

4.4.1.1 Circumstances for Revocation

A certificate shall be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- Identifying information or affiliation components of any names in the certificate become invalid;
- Privilege attributes asserted in the Subscriber's certificate are reduced;
- The Subscriber can be shown to have violated the stipulations of its Subscriber agreement;
- The private key is suspected of compromise; and
- The Subscriber or other authorized party (as defined in the CMA's CPS) asks for his/her certificate to be revoked.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. In addition, if it is determined subsequent to issuance of new certificates that a private key used to sign requests for one or more additional certificates may have been compromised at the time the requests for additional certificates were made, all certificates authorized by directly or indirectly chaining back to that compromised key shall be revoked. Revoked certificates shall be included on all new publications of the CRL until the certificates expire.

4.4.1.2 Who can Request a Revocation

Within the PKI, a CMA may summarily revoke certificates within its domain. A written notice and brief explanation for the revocation shall be subsequently provided to the Subscriber. The RA can request the revocation of a Subscriber's certificate on behalf of any authorized party as specified in its CPS.

4.4.1.3 Procedure for Revocation Request

Any format that is used to request a revocation shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). A CMA action is required for revocation (a Subscriber may not, via an automated process, revoke its own certificate or change a prior revocation reason without CMA intervention). Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties.

In particular, if the revocation is being requested for reason of key compromise or suspected fraudulent use, then the Subscriber's and the RA's revocation request must so indicate. If a RA performs this on behalf of a Subscriber, a formal, signed message format known to the ECA shall be employed. All requests shall be authenticated; for signed requests from the certificate subject, or from a RA, verification of the signature is sufficient.

Upon receipt of a revocation request from the Subscriber or another authorized party, the CMA shall authenticate the revocation request. The CMA may, at its discretion, take reasonable measures to verify the need for revocation. If the revocation request appears to be valid, the CMA shall revoke the certificate by placing its serial number and other identifying information on a CRL, in addition to any other revocation mechanisms used.

For PKI implementations using hardware tokens, Subscribers leaving organizations that sponsored their participation in the PKI shall surrender to their CMA (through any accountable mechanism) all cryptographic hardware tokens that were issued under the sponsoring organization prior to leaving the organization. The token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction. If a Subscriber leaves an organization and the hardware tokens cannot be obtained from the Subscriber, then all Subscriber certificates associated with the un-retrieved tokens shall be revoked.

4.4.1.4 Revocation Grace Period

There is no grace period for revocation under this policy; ECAs will revoke certificates as quickly as practical upon receipt of a proper revocation request, and shall always revoke certificates within the time constraints described in Section 4.4.3.1.

4.4.2 Suspension

Certificates that are issued under this Policy shall not be suspended.

4.4.3 Certificate Revocation Lists

4.4.3.1 CRL Issuance Frequency

CRLs are periodically issued and posted to a repository, even if there are no changes or updates to be made, to ensure timeliness of information. CRLs may be issued more frequently than required; if there are circumstances under which an ECA will post early updates, these shall be spelled out in its CPS. ECAs shall ensure that superceded CRLs are removed from the repository upon posting of the latest CRL.

The ECA Root CA shall post a CRL every 28 days. The ECA Root CA shall post a CRL within 18 hours of notification that a subordinate ECA must be revoked for any reason.

ECAs other than the ECA Root CA shall issue CRLs daily. If an ECA is issuing a CRL as a result of a subscriber key compromise, that CRL must be posted as quickly as feasible, but shall be posted within 18 hours after notification of the compromise.

The EPMA will notify immediately any externally certified CAs in the event of ECA Root CA or any subordinate CA revocation for any reason.

ECAs shall make public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to Subscribers during certificate request or issuance, and shall be readily available to any potential Relying Party.

4.4.3.2 CRL Checking Requirements

Use of revoked certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party and the system accreditor. If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this policy.

4.4.4 On-line Status Checking

ECAs and Relying Party client software optionally may support on-line status checking. All ECAs shall be required to support CRLs. Client software using on-line revocation checking need not obtain or process CRLs.

On-line CSAs used for verifying certificates asserting a policy OID from this CP shall ensure that:

- Certificates indicated as being valid have a chain of valid certificates (valid as defined by [X.509]) linking back to a EPMA approved "trusted ECA;"
- Each certificate in the certificate chain used to validate the certificate whose status is being requested is checked for revocation, such that the Relying Party need not check more than one CSA to validate a Subscriber certificate;
- Certificate status responses provide authentication and integrity services commensurate with the assurance level of the certificate being verified; and
- It is made clear in the certificate status response which attributes, if any, other than certificate subject name (e.g., citizenship, clearance authorizations, etc.) are being authenticated by the CSA.

On-line CSAs that provide revocation status information only (e.g., OCSP Responder) shall ensure that:

- Accurate and up-to-date from the authorized CA is used to provide the revocation status; and

- Revocation status responses provide authentication and integrity services commensurate with the assurance level of the certificate being checked.

4.4.5 Other Forms of Revocation Advertisements Available

An ECA is required to generate, issue and publish a CRL. In addition to CRL publication, an ECA may use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements:

- The alternative method must be described in the ECA's approved CPS; and
- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.

4.4.6 Special Requirements Related to Key Compromise

A CMA using reason codes must have the ability to transition any reason code to compromise. Operational stipulations are in Section 4.4.3. Refer also to Sections 4.8.1 and 5.3.6.

4.5 SECURITY AUDIT PROCEDURES

This section describes the security requirements of a CMA's certificate issuing system, which includes the equipment used to register Subscribers; generate, sign, and manage certificates; and generate, sign, and manage revocation information.

4.5.1 Types of Events Recorded

Requirements applied to CA, CSA and RA equipment:

Any security auditing capabilities of the underlying CMA equipment operating system shall be enabled during installation.

At a minimum, the following CMA events shall be recorded:

- CMA application access (e.g., logon);
- Messages received from any source requesting CMA actions, (certificate requests, certificate signing, certificate revocation, compromise notification, certificate status request) – CSAs are exempt from this audit requirement;
- Actions taken in response to requests for CMA actions;
- Physical access to, loading, zeroizing, transferring keys to or from, backing-up, acquiring or destroying CMA cryptographic modules;

- Receipt, servicing (e.g., keying or other cryptologic manipulations), and shipping hardware cryptographic modules;
- Posting of any material to a repository;
- Anomalies, error conditions, software integrity check failures, receipt of improper or misrouted messages; and
- Any known or suspected violations of physical security, suspected or known attempts to attack the CMA equipment via network attacks, equipment failures, power outages, network failures, or violations of this certificate policy.

Requirements applied to ECA equipment:

The ECA equipment shall record server installation, access, and modification (to include changes in configuration files, security profiles, administrator privileges).

The following ECA operations shall be recorded:

- ECA equipment access (e.g., room access);
- File manipulation and account management;
- Posting of any material to a repository;
- Access to ECA databases; and
- Any use of the ECA signing key.

Requirements applied to humans and physical operations:

The following events will be audited:

- Appointment of CMA personnel;
- Training of CMA personnel; and
- Physical access to the ECA equipment.

For each auditable event, the CMA security audit record shall include, at a minimum:

- The type of event;
- The time the event occurred;
- For messages from RAs (or other entities) requesting ECA actions, the message source, destination and contents;
- For attempted ECA certificate signature or revocation, a success or failure indication; and
- For operator initiated actions (including equipment and application access), the identity of the equipment operator who initiated the action.

Where possible, the security audit data shall be automatically collected; when this is not possible a log book, paper form, or other physical mechanism shall be used. All security audit logs, both

electronic and non-electronic, shall be retained in accordance with the requirements of Section 4.5.3, and made available during compliance audits.

4.5.2 Frequency of Processing Data

At least 6 aperiodic reviews are required per year, with a minimum of 25 percent of the security audit data generated since the last review to be examined.

The CMA shall implement procedures to ensure that the security audit data is transferred prior to overwriting or overflow of automated security audit log files.

4.5.3 Retention Period for Security Audit Data

The information generated on the CMA equipment shall be kept on the CMA equipment until the information is moved to an appropriate archive facility. Deletion of the security audit data from the CMA equipment shall be performed by an entity other than the CMA. This entity shall be identified in the CMA's CPS. Security audit data shall be retained on-site for at least two months, then off-site as archive records in accordance with Section 4.6.2.

4.5.4 Protection of Security Audit Data

The security audit data shall not be open for reading or modification by any human, or by any automated process other than those that perform security audit processing. CMA system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data. The entity performing security audit data 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 security audit data retention period (note that deletion requires modification access). Security audit data shall be moved to a safe, secure storage location separate from the CMA equipment.

4.5.5 Security Audit Data Backup Procedures

Audit logs shall be backed up at least monthly. A copy of the audit log shall be sent off-site in accordance with the CPS on a monthly basis.

4.5.6 Security Audit Collection System (Internal vs. External)

The security audit process shall run independently and shall not in any way be under the control of the CMA. Security audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated security audit system has failed, the CMA shall cease all operation except for revocation processing until the security audit

capability can be restored. Under these circumstances, the CMA shall employ mechanisms to preclude unauthorized CMA functions. These mechanisms shall be described in the CMA's CPS.

4.5.7 Notification to Event-Causing Subject

There is no requirement to notify a subject that an event was audited. Real-time alerts are neither required nor prohibited by this policy.

4.5.8 Vulnerability Assessments

The CMA, system administrator, and other operating personnel shall be watchful for attempts to violate the integrity of the certificate management system, including the equipment, physical location, and personnel. The security audit data shall be reviewed by the security auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Security auditors shall check for continuity of the security audit data.

4.6 RECORDS ARCHIVAL

4.6.1 Types of Data Archived

CMA archive records shall be detailed enough to establish the validity of a signature and of the proper operation of the PKI. At a minimum, the following data shall be archived.

During ECA system initialization:

- CMA accreditation (if necessary);
- CPSs;
- Any contractual agreements to which the CMA is bound; and
- System equipment configuration.

During CMA operation:

- Modifications or updates to any of the above data items;
- Certificate requests and revocation requests;
- Certificate status requests and responses;
- Subscriber identity authentication documentation as required by Section 3.1.9;
- Documentation of receipt and acceptance of certificates as described in Section 4.3;

- Documentation of receipt of tokens as described in Section 3.1.7;
- All certificates and CRLs (or other revocation information) as issued or published;
- Security audit data (in accordance with Section 4.5);
- Other data or applications sufficient to verify archive contents; and
- All work related communications to or from the EPMA, other CMAs, and compliance auditors.

4.6.2 Retention Period for Archive

Archive records shall be kept for a period of at least ten years, six months without any loss of data. Prior to the end of the archive retention period, the ECA shall provide archived data to an EPMA approved archival facility. The ECA could itself own that facility.

Applications necessary to read these archives must be maintained for at least the applicable retention period above.

The ECA's CPS shall describe the medium and format for supplying the archive data to the EPMA approved facility. The format descriptions shall be sufficient to design and develop automated tools to view and interpret the archive data. The ECA's CPS shall also provide description (e.g., name and version number) of application software that can be used to view and interpret the archive data.

From time to time, EPMA may require the archive data that is under the control of the ECA. The ECA CPS shall describe the medium and format for supplying the archive data to the EPMA upon request.

4.6.3 Protection of Archive

No unauthorized ECA equipment operator shall be able to modify or delete the archive, but archived records may be moved to another medium. 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. No transfer of medium shall invalidate CMA applied signatures. The CMA shall maintain a list of people authorized to modify or delete the archive, and make this list available during CP compliance audits. Release of sensitive archive information will be as described in Section 2.8.

Archive media shall be stored in a separate, safe, secure storage facility. Prior to archive, archive records shall be labeled with the CMA's distinguished name, the date, and sensitivity.

4.6.4 Archive Backup Procedures

No stipulation.

4.6.5 Archive Collection System (Internal vs. External)

Archive data may be collected in any expedient manner.

4.6.6 Procedures to Obtain Archive Information

Procedures detailing how to create, package and send the archive information shall be published in an ECA procedures handbook or CPS. Only authorized ECA equipment operators shall be allowed to access the archive.

4.7 CA KEY CHANGEOVER

An ECA uses a signing (private) key for creating certificates; however, Relying Parties employ the ECA certificate for the life of the Subscriber certificate beyond that signing. Therefore, ECAs must not issue Subscriber certificates that extend beyond the expiration dates of their own certificates and public keys, and the ECA certificate validity period must extend one Subscriber certificate validity period (listed in Section 3.2) past the last use of the ECA private key. To minimize risk to the PKI through compromise of an ECA's key, the private signing key will be changed more frequently, and only the new key will be used for certificate signing purposes from that time. The older, but still valid, certificate will be available to verify old signatures until all of the Subscriber certificates signed under it have also expired. If the old private key is used to sign CRLs that contain certificates signed with that key, then the old key must be retained and protected. For a thorough discussion of key changeover, see *Certificate Management Protocol* [RFC2510].

The following table shows the maximum validity period of the ECA's signature certificate, and the maximum lifetime of the associated authority-signing key (used for certificate signature), separated by a slash. RA key lifetimes are as described for Subscribers in Section 3.2. Note that signature keys that have expired for the purposes of certificate signature may still be used for CRL signature. All values are in years.

	CA	**Intermediate CA**	**Root-CA**
Medium Assurance and Medium Hardware Assurance	6/3	11/5	36/25

4.8 COMPROMISE AND DISASTER RECOVERY

4.8.1 Compromise Recovery

In case of a CA key compromise, a superior CA shall revoke that CA's certificate, and the revocation information shall be published immediately in the most expedient manner. Subsequently, the CA installation shall be re-established as described in 4.8.2. If the CA is a

Root-CA, the trusted self-signed certificate must be removed from each Relying Party application, and a new one distributed via secure out-of-band mechanisms. Root-CAs shall describe their approaches to reacting to a Root-CA key compromise in their CPSs.

In case of a CSA key compromise, the CA that issued the CSA a certificate shall revoke that CSA's certificate, and the revocation information shall be published immediately in the most expedient manner. The CSA shall subsequently be re-keyed. If the CSA is a trust anchor, the trusted self-signed certificate must be removed from each Relying Party application, and a new one distributed via secure out-of-band mechanisms. The CSA's CPS shall describe the approach for reacting to a CSA key compromise.

4.8.2 Disaster Recovery

ECAs are required to maintain a Disaster Recovery Plan.

In the case of a disaster in which the ECA equipment is damaged and inoperative, the ECA operations shall be reestablished as quickly as possible, giving priority to the ability to revoke Subscriber's certificates. If the ECA cannot reestablish revocation capabilities prior to the next update field in the latest CRL issued by the CA, then the ECA must report to the EPMA. The EPMA shall decide whether to declare the ECA private signing key as compromised and reestablish the ECA keys and certificates, or allow additional time for reestablishment of the ECA's revocation capability.

In the case of a disaster whereby an ECA installation is physically damaged and all copies of the ECA signature key are destroyed as a result, the ECA shall request that its certificates be revoked. The ECA installation shall then be completely rebuilt, by reestablishing the ECA equipment, generating new private and public keys, being re-certified, and re-issuing all cross certificates. Finally, all Subscriber certificates shall be re-issued. In such events, Relying Parties continue to use certificates signed with the destroyed private key at their own risk.

4.9 CA TERMINATION

ECA termination will be handled in accordance with Section 4.8 above. If the termination is for convenience, contract expiration, re-organization, or other non-security related reason, and provisions have been made to continue compromise recovery (including destruction or continued protection of signing key), compliance and security audit, archive, revocation, and data recovery services, then neither the terminated ECA's certificate, nor certificates signed by that ECA, need to be revoked.

If provisions for maintaining these services cannot be made, then the ECA termination will be handled as an ECA compromise in accordance with Section 4.8.1 above.

Upon ECA termination, ECA shall provide archived data to an EPMA approved archival facility. The ECA CPS shall describe the medium and format in which the archive data will be provided to the EPMA approved facility.

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS

The ECA equipment shall consist of equipment dedicated to the ECA function; it shall not perform non-CA related functions. This equipment includes, but is not limited to, the system running the CA software, CA hardware cryptographic module, and databases and directories located on the CA computer. In addition, databases and directories located on the CA computer shall not be accessible to the Subscribers and Relying Parties.

Unauthorized use of CMA equipment is forbidden. Physical security controls shall be implemented that protect the CMA hardware and software from unauthorized use. CMA cryptographic modules shall be protected against theft, loss, and unauthorized use.

5.1.1 Site Location and Construction

The location and construction of the facility that will house CMA equipment and operations shall be in accordance with that afforded the most sensitive business and financial information.

5.1.2 Physical Access

ECA and CSA equipment shall always be protected from unauthorized access.

RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The RA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. RA equipment in less secure environments will require additional protection commensurate with the level of risk.

Removable CMA cryptographic modules shall be inactivated prior to storage. When not in use, removable CMA cryptographic modules, and any activation information used to access or enable CMA cryptographic modules or CMA equipment, shall be placed in locked containers sufficient for housing equipment and information commensurate with the sensitivity or value of the information being protected by the certificates issued by the CMA. Activation data shall either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

A security check to the facility housing ECA and CSA equipment shall occur prior to leaving the facility unattended. The check shall verify that:

- 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");
- 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 are 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.

Facilities shall, if unattended for periods greater than 24 hours, be protected by an intrusion detection system. Additionally, a check shall be made at least once every 24 hours to ensure that no attempts to defeat the physical security mechanisms have been made.

5.1.3 Power and Air Conditioning (Environmental Controls)

The facility that houses the ECA equipment shall be supplied with power and air conditioning sufficient to create a reliable operating environment.

The ECA equipment shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. Subscribers or Relying Parties with needs for long operation hours or short response times may contract with an ECA for additional requirements for backup power generation.

5.1.4 Water Exposures

ECA equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors). Moisture detectors shall be installed in areas susceptible to flooding. ECA operators who have sprinklers for fire control shall have a contingency plan for recovery should the sprinklers malfunction, or cause water damage outside of the fire area.

5.1.5 Fire Prevention and Protection

A description of the CMA's approach for recovery from a fire disaster shall be included in the Disaster Recovery Plan as specified in Section 4.8.2.

5.1.6 Media Storage

Media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains security audit, archive, or backup information shall be stored in a location separate from the CMA equipment.

5.1.7 Waste Disposal

Media used to collect or transmit information discussed in Section 2.8 shall be destroyed, such that the information is unrecoverable, prior to disposal.

5.1.8 Off-site Backup

System backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in the CPS. Backups shall be performed and stored off-site not less than once per week or when the CA is operational, whichever is less frequent. At least one backup copy shall be stored at an offsite location (separate from the ECA 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 ECA system.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be diligent and trustworthy as described in the next section. The functions performed in these roles form the basis of trust in the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first approach is to ensure that the person filling the role is trustworthy and properly trained. The second is to distribute the functions of the role among several people, so that any malicious activity requires collusion. Requirements regarding the design and configuration of the technology to avoid mistakes and counter inappropriate behavior are described in Section 6.

The primary trusted roles defined by this policy are the ECA, the RA, and the CSA.

5.2.1.1 Certification Authority

All certificates asserting an ECA certificate policy must be issued by an ECA facility operating under the control of an ECA. The responsible person or body (e.g., board of directors) identified as the facility's ECA must be named, and made available during compliance audits.

Any ECA who asserts a certificate policy OID defined in this document is subject to the stipulations of this policy. The ECA's role and the corresponding ECA procedures shall be defined in a CPS. Primarily, the ECA's responsibilities are to ensure that the following functions occur according to the stipulations of this policy:

- RA functions as described in Section 5.2.1.2, if no separate RA is employed;
- Certificate generation and revocation;
- Posting of certificates and CRLs;
- Performance of the incremental database backups;
- Administrative functions such as compromise reporting and maintaining the database; and
- Hardware cryptographic module programming and management, if appropriate.

5.2.1.2 Registration Authority

Any RA that operates under this policy is subject to the stipulations of this policy, and of the EPMA approved CPS under which it operates. Primarily, a RA's responsibilities are:

- Verifying identity, either through personal contact, or via Trusted Agents or employees, when allowed by this policy;
- Entering Subscriber information, and verifying correctness;
- Securely communicating requests to and responses from the ECA; and
- Receiving and distributing Subscriber certificates.

The RA role is highly dependent on PKI implementations and local requirements. The responsibilities and controls for RAs shall be explicitly described in the CPS of an ECA if the ECA uses a RA.

5.2.1.3 Certificate Status Authority (CSA)

Any CSA that operates under this policy is subject to the stipulations of this policy, and of the EPMA approved CPS under which it operates. Primarily, a CSA is responsible for:

- Providing certificate revocation status and/or complete certification path validation (including revocation checking) to the Relying Parties; and
- Ensuring that the status and validation responses contain authentication and integrity services commensurate with the assurance level of the certificate being checked.

5.2.1.4 Other Trusted Roles

A CMA shall, in its CPS, define other trusted roles to which shall be allocated responsibilities that ensure the proper, safe, and secure operation of the CMA equipment and procedures. These responsibilities include:

- Initial configuration of the system, including installation of applications, initial setup of new accounts, configuration of initial host and network interface;
- Performance of compliance audit;
- Creation of devices to support recovery from catastrophic system loss;
- Performance of system backups, software upgrades and recovery;
- Secure storage and distribution of backups and upgrades to an off-site location;
- Change of the host or network interface configuration;
- Assignment of security privileges and access controls of Subscribers;
- Performance of archive and deletion functions of the security audit log and other archive data as described in Sections 4.5 and 4.6 of this document; and
- Review of the security audit log.

The CMA shall maintain lists, including names, organizations, and contact information, of those who act in these trusted roles, and shall make them available during compliance audits.

To ensure system integrity, the CMAs shall be prohibited from performing compliance audit for their own CMA facility.

5.2.1.5 Trusted Agent

A Trusted Agent is a person authorized to act as a representative of a CMA in providing Subscriber identity verification during the registration process. Trusted Agents do not have automated interfaces with CAs; they act on the behalf of the CA or the RA to only verify the identity of the Subscriber.

5.2.1.6 PKI Sponsor

A PKI Sponsor fills the role of a Subscriber for non-human system components and organizations that are named as public key certificate subjects. The PKI Sponsor works with the CMAs and, when appropriate, their Trusted Agents, to register components (routers, firewalls, etc.) in accordance with Section 3.1.10, and is responsible for meeting the obligations of Subscribers as defined throughout this document.

5.2.2 Separation of Roles

Under no circumstances shall the incumbent of a CMA role perform its own compliance or security auditor function.

5.3 PERSONNEL CONTROLS

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

Persons shall be selected for any CMA or other trusted role on the basis of loyalty to the United States, their trustworthiness, and integrity. All CMAs shall be US citizens. All persons filling trusted roles, including the CMAs, shall either hold a US security clearance or shall have completed a favorable background investigation described in Section 5.3.2 below.

ECA operations shall be administered by a person or body (e.g., a Board of Directors). This person or body shall be identified as the ECA as described in Sections 1.3.1 and 5.2.1.1. The operators and equipment for an ECA installation must be within the administrative control of the identified ECA.

Personnel appointed to operate CMA equipment shall:

- Have successfully completed an appropriate training program;
- Have demonstrated the ability to perform their duties;
- Be trustworthy;
- Have no other duties that would interfere or conflict with their duties as a CMA;
- Have not knowingly been previously relieved of CMA or other trusted duties for reasons of negligence or non-performance of duties;
- Have not knowingly been denied a security clearance, or had a security clearance revoked;
- Have not been convicted of a felony offense; and
- Be appointed in writing by an approving authority, or be party to a contract for PKI services.

5.3.2 Background Check Procedures

All persons filling trusted roles, including CMAs, shall either hold a US security clearance or have completed a favorable background investigation. The scope of the background check shall include the following items covering the past seven years:

- A criminal history check shall show no misdemeanor or felony conviction;
- A credit history check shall show that person has not committed any fraud or is otherwise financially trustworthy;
- Employment verification shall demonstrate that the person is competent, reliable and trustworthy;

- Professional references shall demonstrate that the person is competent, reliable and trustworthy;
- Residence checks shall demonstrate that the person was and is a trustworthy neighbor;
- Education verification of highest or most relevant degree;
- DMV records shall demonstrate no pattern of violations; and
- Social Security trace shall show that the person has a valid social security number[2].

The background checks shall be performed by qualified investigators.

The results of these checks shall not be released except as required in Section 2.8. Background check procedures shall be described in the CPS.

5.3.3 Training Requirements

All personnel involved in the CMA operation shall be appropriately trained. Topics shall include the operation of the CMA software and hardware, operational and security procedures, and the stipulations of this policy and local guidance. The specific training required will depend on the equipment used and the personnel selected. A training plan shall be established for a CMA installation, and training completed by the personnel shall be documented.

5.3.4 Retraining Frequency and Requirements

Those involved in filling PKI roles shall be aware of changes in the CMA operation. Any significant change to the CMA operation shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are ECA software or hardware upgrade, changes in automated security systems, and relocation of ECA equipment.

5.3.5 Job Rotation Frequency and Sequence

This policy makes no stipulation regarding frequency or sequence of job rotation. However, ECA shall provide for continuity and integrity of the PKI service.

[2] This check shall be required only if the country in which the duty is performed has social security number or similar identifier.

5.3.6 Sanctions for Unauthorized Actions

A CMA shall take appropriate administrative and disciplinary actions against personnel who violate this policy.

5.3.7 Contracting Personnel Requirements

PKI vendors who provide ECA services shall establish procedures to ensure that any subcontractors perform in accordance with the ECA's CPS and this policy.

5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

This policy does not preclude any source of key that has been generated in accordance with the stipulations of this policy and local security requirements. A private key is considered to be generated by the PKI entity that first comes into possession of it: a Subscriber, a RA, or a CA.

A private key must not appear outside of the module in which it was generated unless it is encrypted for local transmission or for processing or storage by a key recovery mechanism.

CA certificate signing and CSA certificate status response signing keys shall be generated in FIPS 140, Level 2 validated cryptographic hardware modules.

6.1.2 Private Key Delivery to Subscriber

See paragraph 4.2.1.

6.1.3 Key Sizes

Digital Signature Standard (DSS) keys shall use at least 160 bit private key (x) and at least 1024 bit prime modulus (p). Minimum Subscriber public key sizes (meaning modulus) shall be 1024 bits for Key Exchange Algorithm (KEA) and Rivest, Shamir, Adleman (RSA). Elliptic Curve Digital Signature Algorithm key prime field (*///p//*) shall be not less than 224, and the Binary Field (*m*) shall be not less than 233.

Use of Secure Socket Layer (SSL) or another protocol providing similar security to accomplish any of the requirements of this CP shall require, at a minimum, three key triple-Data Encryption Standard (triple-DES) or equivalent for the symmetric key algorithm.

6.1.4 Public Key Parameters Generation

Public key parameters shall always be generated and checked in accordance with the standard that defines the crypto-algorithm in which the parameters are to be used. For example, public key parameters for use with algorithms defined in the *Digital Signature Standard* [FIPS186-2] shall be generated and tested in accordance with [FIPS186-2]. Public key parameters for use with the RSA algorithm defined in [PKCS-1] shall be generated and checked in accordance with

[PKCS-1], and so on. Whenever a crypto-algorithm is described in [FIPS186-2], the parameter generation and checking requirements and recommendations of [FIPS186-2] shall be required of all entities generating key pairs whose public components are to be certified by the ECA.

6.1.5 Parameter Quality Checking

See Section 6.1.4.

6.1.6 Hardware/Software Key Generation

Medium hardware assurance encryption key pairs may be generated off the token as long as there are assurances that no copies other than authorized key escrow copies of the keys continue to exist after the generation and insertion process has completed.

Medium hardware assurance signature key pairs shall be generated on the token.

Intermediate keys and any pseudo-random numbers used for key generation shall be generated using a FIPS approved method.

6.1.7 Key Usage Purposes (per X.509 V3 Key Usage Field)

Public keys that are bound into certificates shall be certified for use in signing or encrypting, but not both, except as specified below. The use of a specific key is determined by the key usage extension in the X.509 certificate. This restriction is not intended to prohibit use of protocols (like the Secure Sockets Layer) that provide authenticated connections using encryption certificates.

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for Cryptographic Module

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [current version of FIPS140]. Cryptographic modules shall be validated to the FIPS 140 level identified in this section.

Subscribers shall use cryptographic modules that have been validated to meet at least the criteria specified for FIPS 140 Level 1. A higher level may be used if available or desired. A PKI should provide the option of using any acceptable cryptographic module to facilitate the management of Subscriber certificates.

Certificates shall be signed using a hardware cryptographic module that has been validated to meet FIPS 140 Level 2.

CSAs and RAs shall use hardware cryptographic modules that have been validated to meet FIPS 140 Level 2.

All cryptographic modules shall be operated such that the private asymmetric cryptographic keys shall never be output in plaintext. No private key shall appear unencrypted outside the CA equipment.

No one shall have access to a private signing key but the Subscriber. Any private encryption keys held by a CMA shall be held in strictest confidence and controlled as described in the ECA Key Recovery Policy (KRP).

Note that Section 6.1.1 stipulates cryptographic module requirements for key generation.

Medium Assurance	**Subscriber**	**RA, CSA, and CA**
FIPS 140 validation	Level 1	Level 2 (hardware)
Operational requirement	Shall not output private asymmetric key in plaintext	

Medium Hardware Assurance	**Subscriber**	**RA and CA**
FIPS 140 validation	Level 1 (software for generation; insertion onto Level 1 hardware)[3]	Level 2 (hardware)
Operational requirement	Shall not output private asymmetric key in plaintext	

6.2.2 Private Key Multi-Person Control

A single person shall not be permitted to activate the ECA signature key or access any cryptographic module containing the complete ECA private signing key. Access to ECA signing keys backed up for disaster recovery shall be under the same multi-person control as the original ECA signing key.

Private encryption keys requested by other than the subscriber/PKI sponsor may only be extracted from key recovery databases under two-person control. Subscribers are permitted to back-up their own encryption (but not signature) private keys. The names of the parties used for two-person control shall be maintained on a list that shall be made available for inspection during compliance audits.

[3] Level 1 hardware overall with Level 2 roles and services and Level 2 physical security.

6.2.3 Private Key Escrow

Under no circumstances shall a key used to support non-repudiation services be held in trust by a third party.

For some purposes (such as data recovery) it shall be necessary to provide key retrieval for the private component of the encryption certificate key pair. To facilitate this, the ECA shall offer a key escrow and recovery capability.

The method, procedures and controls which will apply to the storage, request for, extraction and/or retrieval, delivery, protection and destruction of the requested copy of an escrowed key shall be described in a key recovery practice statement (KRPS). The ECA shall submit the KRPS along with the CPS for the EPMA approval. High-level requirements for the KRPS are listed in an appendix. The ECA KRP is provided as a separate document. The ECA KRPS shall comply with the ECA KRP.

6.2.4 Private Key Backup

Subscribers are permitted to back-up their own encryption (but not signature) private keys. Backup of private signature keys for the sole purpose of key recovery shall not be made. Subscribers are permitted to make operational copies of private keys residing in software cryptographic modules for each of the Subscriber's applications or locations that require the key in a different location or format. Component PKI Sponsors (see Section 3.1.10) are authorized to make a single backup copy of the component private keys to support backup in cases where component malfunction results in key corruption. All key transfers shall be done from an approved cryptographic module, and the key shall be encrypted during the transfer. The Subscriber (PKI Sponsor for Component) is responsible for ensuring that all copies of private keys, including those that might be embedded in component backups, are protected, including protecting any workstation on which any of its private keys reside.

CA private signature keys may be backed up under the same multi-person control as the original signaure key. If such a backup is made, only a single copy of the signature key is to be kept at the CA location; a second copy may be kept at a backup location.

CSA private signature keys may be backed up under the same controls as the original signaure key. The backup module shall also meet the cryptographic module requirements for the CSA.

6.2.5 Private Key Archival

See Section 6.2.3 and Section 6.2.4.

6.2.6 Private Key Entry into Cryptographic Module

Private keys are to be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic module boundary.

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure. The protection of these keys must be commensurate with that provided the data protected by the certificate associated with the private key.

6.2.7 Method of Activating Private Key

Pass-phrases, PINs, biometric data, or other mechanisms of equivalent authentication robustness must be used to activate the private key in a cryptographic module. (Activation data generation requirements are specified in 6.4.1) Activation data may be distributed in person, or mailed to the Subscribers separately from the cryptographic modules that they activate. Entry of activation data must be protected from disclosure (e.g., the data should not be displayed while it is entered).

6.2.8 Method of Deactivating Private Key

Cryptographic modules, which have been activated, must not be left unattended or otherwise open to unauthorized access. After use, they must be deactivated, e.g. via a manual logout procedure, or by a passive timeout. Hardware cryptographic modules shall be removed and stored in accordance with Section 5.1.2, when not in use.

6.2.9 Method of Destroying Private Key

Private keys shall be destroyed when they are no longer needed or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a "zeroize" command. Physical destruction of hardware should not be required.

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.

6.3.2 Usage Periods for the Public and Private Keys

The key usage periods for keying material are described in Section 3.2 and Section 4.7.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

A pass-phrase, PIN, biometric data, or other mechanism of equivalent authentication robustness shall be used to protect access to use of a private key. The activation data may be Subscriber selected. Any pass-phrase or PIN shall be generated in conformance with [FIPS112].

If the activation data must be transmitted, it shall be via a channel of appropriate protection, and distinct in time and place from the associated cryptographic module. If this is not done by hand, the Subscriber shall be advised of the shipping date, method of shipping, and expected delivery date of any activation data. As part of the delivery method, Subscribers will sign and return a delivery receipt. In addition, Subscribers should receive (and acknowledge) a Subscriber advisory statement to help to understand responsibilities for use and control of the cryptographic module.

6.4.2 Activation Data Protection

Activation data for cryptographic modules should be memorized, not 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.

Activation data for private keys associated with certificates asserting individual identities shall never be shared. Activation data for private keys associated with certificates asserting organizational identities shall be restricted to those in the organization authorized to use the private keys.

The activation data protection mechanism for CA equipment or applications shall include a facility to temporarily lock out further access attempts, after a predetermined number of failed login attempts as set forth in the CA's CPS.

6.4.3 Other Aspects of Activation Data

If a CMA cryptographic module requires a PIN or pass-phrase as activation data, the PIN or pass-phrase shall be changed no less than once every three months.

6.5 COMPUTER SECURITY CONTROLS

CA and CSA equipment shall use operating systems that:

- Require authenticated logins;
- Provide discretionary access control; and
- Provide a security audit capability

When CA and CSA equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as received the evaluation rating.

6.6 LIFE CYCLE TECHNICAL CONTROLS

Equipment (hardware and software) procured to operate a PKI shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with, such as random selection. Equipment developed for a PKI shall be developed in a controlled environment.

All hardware and software that has been identified as supporting a CA must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the location where it has been identified as supporting a CMA function to the using facility. CA software, when first loaded, shall be verified as being that supplied by the vendor, with no modifications, and be the version intended for use.

CA and CSA equipment shall be dedicated to administering a PKI. The configuration of CA and CSA systems, as well as any modifications and upgrades, shall be documented. CA and CSA systems shall not have installed applications or component software that are not part of CA or CSA configurations. They shall have a capability installed and operating to detect unauthorized modifications to CA and CSA systems software or configurations.

Reasonable care shall be taken to prevent malicious software from being loaded on RA equipment. Only applications required to perform the organization's mission shall be loaded on RA computers, and all such software shall be obtained from sources authorized by the ECA. Data on RA equipment shall be scanned for malicious code on first use and periodically afterward.

Equipment updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

Medium Assurance and Medium Hardware Assurance	Purchase in manner to reduce likelihood of tampering, or develop in controlled environment Protective packaging, accountable delivery method

6.7 NETWORK SECURITY CONTROLS

CMA equipment shall be located on internal networks behind boundary/perimeter network defenses and afforded protections consistent with commercial electronic commerce practices for network security. Services allowed to and from the CA and CSA equipment shall be limited to those required to perform CMA functions. Other CMA equipment may enable additional services consistent with local policy.

Protection of CMA equipment shall be provided against known network attacks. All unused network ports and services shall be turned off. Any network software present on the CMA equipment shall be necessary to the functioning of the CMA application. Root CA equipment shall be stand-alone (off-line) configurations.

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. Firewalls shall meet the security functional requirements as specified in the DoD medium robustness Firewall Protection Profile [FWPP]. Boundary control devices shall include an Intrusion Detection capability that meets the security functional requirements as specified in the Intrusion Detection System Protection Profile [IDSPP].

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

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

7 CERTIFICATE AND CRL PROFILES

Appendix A contains the formats for the various certificates and CRLs.

7.1 CERTIFICATE PROFILE

7.1.1 Version Numbers

ECA shall issue X.509 Version 3 certificates only.

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles. These profiles are written to prescribe an appropriate amount of control over an infrastructure, yet be flexible enough to meet the needs of the various CAs and communities. ECAs shall use certificate profiles described in this CP. These profiles are based on the *Federal PKI Certificate and CRL Profile* [FPKI-E]. Any variance to these profiles shall be approved by the EPMA, and documented in the associated CPS. Whenever private extensions are used, they shall be identified in the CPS. Critical private extensions shall be interoperable in their intended community of use.

Access control information may be carried in the subjectDirectoryAttributes extension. If this is desired, the syntax is defined in detail in [SDN702].

7.1.3 Algorithm Object Identifiers

Certificates under this Policy will use the following 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}
ecdsa-with-SHA1	{iso(1) member-body(2) us(840) ansi-x9-62 (10045) signatures (4) 1 }

Certificates under this Policy will use the following 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}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public-key-type (2) 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}

ECAs shall certify only public keys associated with the crypto-algorithms identified above, and shall only use the signature crypto-algorithms described above to sign certificates, certificate revocation lists and any other PKI product, including other forms of revocation such as OCSP responses.

7.1.4 Name Forms

DNs will be used by the ECAs in the issuer and in subject fields of the certificates. X.500 Directories use the DN for lookups. All PKIs shall have the ability to generate and process DNs. Some communities or installations may choose to use other names, for example certificates used to implement a hardware protocol, where device addresses are most useful and certificate lookup is not performed. In this case, an alternate name form may be included in the subjectAltName extension. Any name form defining GeneralName in [ISO9594-8] may be used, in accordance with the required profile (Section 7.1.2).

Use of alternate name forms shall be defined in a CPS, including criticality, types, and name constraints.

7.1.5 Name Constraints

N/A

7.1.6 Certificate Policy Object Identifier

Certificates issued under this policy shall assert the OID appropriate to the level of assurance with which it was issued, as defined in Section 1.2.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this policy shall not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

This policy does not require the certificatePolicies extension to be critical. Relying Parties whose client software does not process this extension do so at their own risk.

7.2 CRL PROFILE

7.2.1 Version Numbers

CRLs issued under this Policy shall assert a version number as described in the X.509 standard [ISO9594-8]. CRLs shall assert Version 2.

7.2.2 CRL and CRL Entry Extensions

Detailed CRL profiles covering the use of each extension are available in described in Appendix A. Any variance to these profiles shall be approved by the EPMA and documented in a CPS.

7.3 OCSP REQUEST – RESPONSE FORMAT

Appendix A contains the format (profile) for OCSP requests and responses.

8 CERTIFICATE POLICY ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

The EPMA shall review this policy at least once every year. The EPMA shall maintain and publish a Certificate Policy Plan that describes anticipated changes to this CP. Errors, updates, or suggested changes to this document shall be communicated to the contact in Section 1.4. Such communication must 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 EPMA shall be disseminated to interested parties (see Section 8.2) for a period of at least one month.

The EPMA shall accept, accept with modifications, or reject the proposed change after completion of the review period.

8.2 PUBLICATION AND NOTIFICATION POLICIES

The EPMA for this policy shall publish information (including this policy) on a web site.

The EPMA will maintain a list of ECAs asserting this policy (this responsibility may be delegated to a Root- or Intermediate-CA in practice). Proposed changes to the policy and policy updates shall be sent to those ECAs. The CMA shall notify its Subscribers of any changes to the certificate policy via a mechanism described in its CPS.

8.3 CPS AND EXTERNAL POLICY APPROVAL PROCEDURES

The EPMA shall make the determination that a CPS complies with this policy for a given level of assurance. The CMA must have and meet all requirements of an approved CPS prior to commencing operations.

8.4 WAIVERS

Normally, the EPMA shall decide that variation in CMA practice is acceptable under a current policy, or the CMA shall request a permanent change to the policy. Policy waivers may be granted by the EPMA to meet urgent, unforeseen ECA operational requirements. When a waiver is granted, the EPMA shall post the waiver on a web site accessible by Relying Parties, and shall either initiate a permanent change to the policy, or shall place a specific time limit, not to exceed one year, on the waiver.

APPENDIX A: CERTIFICATE AND CRL FORMATS

A.1 ECA ROOT CA SELF-SIGNED CERTIFICATE

Field	ECA Root CA Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	cn=ECA Root CA, ou=ECA, o=U.S. Government, c=US
Validity Period	36 years from date of issue in Generalized Time format
Subject Distinguished Name	cn=ECA Root CA, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA Root CA's public key information)
subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA Root CA's public key information)
key usage	c=yes; digitalSignature, keyCertSign, cRLSign
Extended key usage	Not Present
Private key usage period	Not Present
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 1}, {2 16 840 1 101 3 2 1 12 2}
Policy Mapping	Not Present
subject Alternative Name	Not Present
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	c=yes; cA=True; no path length constraint
Name Constraints	Not Present
Policy Constraints	Not Present
CRL Distribution Points	Not Present

A.2 SUBORDINATE CA CERTIFICATE

Field	Subordinate CA Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	cn=ECA Root CA, ou=ECA, o=U.S. Government, c=US
Validity Period	6 years from date of issue in UTCT format
Subject Distinguished Name	<cn=ECA CA name>, <ou=ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA Root CA's public key information)
subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA public key information)
key usage	c=yes; digitalSignature, keyCertSign, cRLSign
Extended key usage	Not Present
Private key usage period	Not Present
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 1}, {2 16 840 1 101 3 2 1 12 2}
Policy Mapping	Not Present
subject Alternative Name	Not Present
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	c=yes; cA=True; path length constraint = 0
Name Constraints	C=no; permitted subtrees: ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Policy Constraints	Not Present
Authority Information Access	C=no; optional; pointer to OCSP Responder
CRL Distribution Points[4]	c = no; always present

[4] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

A.3 IDENTITY CERTIFICATE

Field	Identity Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Distinguished Name	<cn=ECA CA name>, <ou=ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Validity Period	3 years from date of issue
Subject Distinguished Name	<cn=Subscriber Name>, <ou=Subscriber Company Name >, <ou=ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption
authority key identifier[5]	c=no; octet string
subject key identifier[6]	c=no; octet string
key usage	c=yes;digitalSignature, nonRepudiation
Extended key usage	Not Present
Private key usage period	Not Present
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 1} or {2 16 840 1 101 3 2 1 12 1}, {2 16 840 1 101 3 2 1 12 2}
Policy Mapping	Not Present
subject Alternative Name	c=no; always present, contains RFC822 email address
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	C=no; optional; pointer to OCSP Responder
CRL Distribution Points[7]	c = no; always present

[5] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[6] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

[7] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

A.4 ENCRYPTION CERTIFICATE

Field	Encryption Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Distinguished Name	<cn=ECA CA name>, <ou=ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Validity Period	3 years from date of issue
Subject Distinguished Name	<cn=Subscriber Name>, <ou=Subscriber Company Name >, <ou=ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption
authority key identifier[8]	c=no; octet string
subject key identifier[9]	c=no; octet string
key usage	c=yes; keyEncipherment
Extended key usage	Not Present
Private key usage period	Not Present
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 1} or {2 16 840 1 101 3 2 1 12 1}, {2 16 840 1 101 3 2 1 12 2}
Policy Mapping	Not Present
subject Alternative Name	c=no; always present, contains RFC822 email address
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	C=no; optional; pointer to OCSP Responder
CRL Distribution Points[10]	c = no; always present

[8] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[9] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

[10] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

A.5 COMPONENT CERTIFICATE

Field	Component & Web Server Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Distinguished Name	<cn=ECA CA name>, <ou=ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Validity Period	3 years from date of issue
Subject Distinguished Name	<cn=Host URL | IP Address | Host Name>, <ou=Host Company Name >, <ou=ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption
authority key identifier[11]	c=no; octet string
subject key identifier[12]	c=no; octet string
key usage	c=yes; keyEncipherment, digitalSignature
Extended key usage	Not Present
Private key usage period	Not Present
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 1}
Policy Mapping	Not Present
subject Alternative Name	c=no; always present, Host URL | IP Address | Host Name
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	C=no; optional; pointer to OCSP Responder
CRL Distribution Points[13]	c = no; always present

[11] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[12] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

[13] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

A.6 CODE SIGNING CERTIFICATE

Field	Code Signing Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Distinguished Name	<cn=ECA CA name>, <ou=ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Validity Period	10 years from date of issue
Subject Distinguished Name	cn=CS.<Code Signer Organization Name>.<optional number>, <ou=Code Signer Company Name >, <ou=ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption
authority key identifier[14]	c=no; octet string
subject key identifier[15]	c=no; octet string
key usage	c=yes; digitalSignature, nonRepudiation
Extended key usage	c=yes; { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-kp(3) id-kp-codesigning (3) }
Private key usage period	Not Present
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 1}, {2 16 840 1 101 3 2 1 12 2}
Policy Mapping	Not Present
subject Alternative Name	always present; c=no; cn=Name, ou=CompanyName (optional), ou=ECA-n, ou=Contractor, ou=PKI, ou=DoD, o=U.S. Government, c=US
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	C=no; optional; pointer to OCSP Responder
CRL Distribution Points[16]	c = no; always present

[14] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[15] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

[16] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

A.7 OCSP RESPONDER SELF-SIGNED CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	cn=<OCSP Responder Name>, <ou=ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Validity Period	36 years from date of issue in Generalized Time format
Subject Distinguished Name	cn=<OCSP Responder Name>, <ou=ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extensions	Not Present

A.8 OCSP RESPONDER CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	<cn=ECA CA name>, <ou=ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Validity Period	One month from date of issue in UTCT format
Subject Distinguished Name	cn=<OCSP Responder Name>, <ou=ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA CA's public key information)
subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of thed OCSP Responder public key information)
key usage	c=yes; nonRepudiation, digitalSignature
Extended key usage	C=yes; id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 1}, {2 16 840 1 101 3 2 1 12 2}
subject Alternative Name	HTTP URL for the OCSP Responder
No Check	id-pkix-ocsp-nocheck; {1 3 6 1 5 5 7 48 1 5}

A.9 ECA ROOT CA CRL

Field	Root CA CRL Value
Version	V2 (1)
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Distinguished Name	cn=ECA Root CA, ou=ECA, o=U.S. Government, c=US
thisUpdate	UTCT
nextUpdate	UTCT; thisUpdate + 28 days
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (in UTCT)
CRL extensions	
CRL Number	Integer
Authority Key Identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA Root CA's public key information)
CRL entry extensions	
Invalidity Date	optional
Reason Code	Always Present; Will not include certificateHols

A.10 SUBORDINATE CA CRL

Field	Subordinate CA CRL Value
Version	V2 (1)
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Distinguished Name	<cn=ECA CA name>, <ou=ECA Company Name>, ou=ECA, o=U.S. Government, c=US
thisUpdate	UTCT
nextUpdate	UTCT; thisUpdate + 7 days
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (in UTCT)
CRL extensions	
CRL Number	Integer
Authority Key Identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA public key information)
CRL entry extensions	
Invalidity Date	optional
Reason Code	Always Present; Will not include certificateHols

A.11 OCSP REQUEST FORMAT

The OCSP requests are not expected to be signed. The OCSP Responder will not check the signature on the request. See RFC2560 for detailed syntax. The following table lists which fields are expected by the OCSP Responder.

Field	Expected Value
Version	V1 (0)
Requester Name	Not Required
Request List	List of certificates – generally this should be the list of two certificates: ECA certificate and end entity certificate
Signature	Not Required
Extensions	Not Required

A.12 OCSP RESPONSE FORMAT

See RFC2560 for detailed syntax. The following table lists which fields are populated by the OCSP Responder.

Field	Expected Value
Response Status	Successful | Malformed Request | Internal Error | Try Later
Response Type	id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Version	V1 (0)
Responder ID	Hash of Responder public key
Produced At	Generalized Time
List of Responses	Each response will contain certificate id; certificate status[17], thisUpdate, nextUpdate[18],
Extension	
Nonce	Will be present if nonce extension is present in the request
Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Signature	Present
Certificates	Applicable certificates issued to the OCSP Responder

[17] If the certificate is revoked, the OCSP Responder will provide revocation time and revocation reason from CRL entry and CRL entry extension.

[18] The OCSP Responder will use thisUpdate and nextUpdate from CA CRL.

APPENDIX B: ELEMENTS OF KEY RECOVERY POLICY AND PRACTICES

The ECA KRPS shall address the following topics. The KRPS must be approved by the EPMA prior to ECA issuing encryption certificates. ECAs must follow the format and contents of the KRP, which provides a more detailed and concrete list of security requirements the key escrow and recovery system must satisfy in order to be approved by the EPMA. The following is a list of high-level topics that must be addressed:

- Verification of the identity and validation of authorization of the key recovery requestor;
- Multi-person (at least two) control on third party key recovery;
- Security of the escrowed keys in storage;
- Security of key escrow process, including keys in transit;
- Security of key recovery process, including keys in transit;
- Audit and archive of security relevant events;
- Compromise recovery;
- Physical, personnel, procedural and technical security controls for key escrow and recovery systems; and
- Compliance audit of the key escrow and recovery systems and processes.

APPENDIX C: REFERENCES

The following documents contain information that provides background, examples, or details about the contents of this policy.

Number	Title	Revision	Date
ABADSG	*Digital Signature Guidelines* http://www.abanet.org/scitech/ec/isc/dsgfree.html		1 August 1996
FIPS140	*Security Requirements for Cryptographic Modules* http://csrc.nist.gov/publications/index.html		21 May 2001
FIPS112	*Password Usage* http://csrc.nist.gov/		5 May 1985
FIPS186-2	*Digital Signature Standard* http://csrc.nist.gov/fips/fips186-2.pdf		20 January 2000
FOIAACT	*5 U.S.C. 552, Freedom of Information Act* http://www4.law.cornell.edu/uscode/5/552.html		
FPKI-Prof	*Federal PKI Certificate and CRL Extensions Profile* http://csrc.nist.gov/pki/		31 May 2002
FWPP	*U.S. Department of Defense Traffic-FilterFirewall Protection Profile for Medium Robustness Environments* *http://www.iatf.net*	Version 1.4	1 May 2000
IDSPP	*Intrusion Detection System System Protection* *http://www.iatf.net*	Version 1.4	4 February 2002
ISO9594-8	*Information Technology – Open Systems Interconnetion – The Directory: Authentication Framework* ftp://ftp.bull.com/pub/OSIdirectotry/ITU/97x509final.doc		1997
ITMRA	*40 U.S.C. 1452, Information Technology Management Reform Act* http://www4.law.cornell.edu/uscode/40/1452.html		
NAG69C	*Information System Security Policy and Certification Practice Statement for Certification Authorities,*	Revision C	November 1999
NS4009	*NSTISSI 4009, National Information Systems Security Glossary*		January 1999
NSD42	*National Policy for the Security of National Security Telecom and Information Systems* http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)		5 July 1990
PKCS-1	*PKCS #1 v2.0: RSA Cryptography Standard* http://www.rsa,com		1 October 1998
PKCS-12	*Personal Information Exchange Syntax Standard* http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html		April 1997
ECAKRP	*Key Recovery Policy for External Certification Authorities*	Version 1.0	4 June 2002

Number	Title	Revision	Date
RFC2510	*Certificate Management Protocol,* Adams and Farrell http://www.ietf.org/rfc/rfc2510.txt		March 1999
RFC2527	*Certificate Policy and Certification Practices Framework,* Chokhani and Ford http://www.ietf.org/rfc/rfc2527.txt		March 1999
SDN702	*SDN.702, Abstract Syntax for Utilization with Common Security Profile (CSP), Version 3 X.509 Certificates and Version 2 CRLs* http://www.armadillo.Huntsville.al.us/Forteza_docs/sdn702rev3.pdf	Revision 3	31 July 1997

APPENDIX D: ACRONYMS AND ABBREVIATIONS

CA	Certification Authority
CMA	Certificate Management Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
CSOR	Computer Security Objects Registry
DES	Data Encryption Standard
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECA	External Certification Authority
EPMA	ECA Policy Management Authority
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standard
FPKI	(US) Federal Public Key Infrastructure
FTP	File Transfer Protocol
I&A	Identification and Authentication
ID	Identity (also, a credential asserting an identity)
IP	Internet Protocol
ISO	International Organization for Standards
IT	Information Technology
KEA	Key Exchange Algorithm
KRP	Key Recovery Policy
KRPS	Key Recovery Practices Statement
MD	Maryland
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RD	Road
RFC	Request For Comment
RSA	Rivest, Shamir, Adleman (encryption and digital signature algorithm)

S/MIME	Secure Multipurpose Internet Mail Extensions
SCVP	Simple Certificate Validation Protocol
SDN	Secure Data Network
SSL	Secure Socket Layer
US	United States
USC	United States Code
USD	United States Dollar
WWW	World Wide Web

APPENDIX E: GLOSSARY

The primary source is *NSTISSI 4009, National Information Systems Security Glossary*; other sources were used if NSTISSI 4009 had no entry for the term, or if another source gave a definition more appropriate to PKI. If no reference is given, the definition is ad hoc.

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 IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
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 a CMA, 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"]
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]
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 person.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
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.
Certification Authority (CA)	An authority trusted by one or more users to create and assign certificates. [ISO9594-8]
CA facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
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]

certificate-related information	Information, such as a Subscriber's postal address, that is not included in a certificate, but that may be used by a CA in certificate management.
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.
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]
confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
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]
dual use certificate	A certificate that is intended for use with both digital signature and data encryption services.
e-commerce	The use of network technology (especially the Internet) to buy or sell goods and services
encryption certificate	A certificate containing a public key that is used to encrypt or decrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. The process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate is sometimes referred to as key management.
External Policy Management Authority (EPMA)	Authority that oversees the creation and update of Certificate Policies, reviews Certification Practice Statements, reviews the results of CA audits for policy compliance, evaluates non-domain policies for acceptance within the domain, and generally oversees and manages the PKI certificate policies.
firewall	Gateway that limits access between networks in accordance with local security policy. [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]
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.
key escrow	The retention of the private component of the key pair associated with a subscriber's encryption certificate to support key recovery.
key exchange	The process of exchanging public keys (and other information) in order to establish secure communication.
key generation material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
naming authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
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]

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.
PKI Sponsor	Fills the role of a Subscriber for non-human system components or organizations that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this document.
privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	Entity responsible for identification and authentication of certificate subjects that has automated equipment for the communication of applicant data to Certification Authorities and does not sign or directly revoke certificates.
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.
re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application.
Relying Party	A person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them. [ABADSG]
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 trustworthy system for storing and retrieving certificates or other information relevant to certificates. [ABADSG]
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.
server	A system entity that provides a service in response to requests from clients.
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.
subordinate CA	In a hierarchical PKI, a CA whose certificate signing key is certified by another CA, and whose activities are constrained by that other CA. (see superior CA)
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate. [ABADSG]. **Current subscribers** possess valid ECA-issued certificates.
superior CA	In a hierarchical PKI, a CA who has certified the certificate signing 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.
technical non-repudiation	The contribution public key mechanisms make 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 a Certificate Management Authority in providing 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, 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.
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]
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.
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. [FIPS140]