United States Department of Defense External Certification Authority X.509 Certificate Policy

Version 4.5

20 February 2019

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

1 INTRODUCTION

The United States (U.S.) Department of Defense (DoD) established the External Certification Authority (ECA) program to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations. The ECA program is designed to provide the mechanism for these entities to securely communicate with the DoD and authenticate to DoD Information Systems. This Certificate Policy (CP) governs the operation of the ECA Public Key Infrastructure (PKI), consisting of products and services that provide and manage X.509 certificates for public-key cryptography. Certificates identify the entity named in the certificate, and bind that entity to a particular public/private key pair. This Certificate Policy addresses the requirements for ECAs that will issue certificates to Subscribers who have a need to conduct business with a U.S. Government Agency. However, these certificates are not restricted to the conduct of business with the U.S. Government.

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 confidence in the 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).

Defining requirements on PKI activities, including the following, ensures the security of these services:

- 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 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 9.12.1, 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.

1.2 DOCUMENT NAME AND IDENTIFICATION

This CP defines multiple policies. Each policy 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-token	ID::= {id-eca-policies 3}
id-eca-medium-hardware	ID::= {id-eca-policies 2}
id-eca-medium-sha256	ID::= {id-eca-policies 4}
id-eca-medium-token-sha256	ID::= {id-eca-policies 5}
id-eca-medium-hardware-pivi	ID::= {id-eca-policies 6}
id-eca-cardauth-pivi	ID::= {id-eca-policies 7}
id-eca-contentsigning-pivi	ID::= {id-eca-policies 8}
id-eca-medium-device-sha256	ID::= {id-eca-policies 9}
id-eca-medium-hardware-sha256	ID::= {id-eca-policies 10}

The requirements stipulated in this CP apply to all assurance levels unless otherwise noted. Requirements for Medium SHA-256, Medium Token SHA-256, and Medium Hardware SHA-256 are identical to Medium, Medium Token, and Medium Hardware respectively, except for the hash algorithm used in generating certificate, CRL, and OCSP response signatures. Requirements for Medium Device SHA-256 are identical to Medium except for the hash algorithm and activation data.

End-Entity certificates issued to devices shall always assert the Medium Device SHA-256 or PIV-I Content Signing policy. All other policies defined in this document should be reserved for human subscribers when used in End-Entity certificates.

1.3 PKI PARTICIPANTS

The following sections introduce the PKI roles involved in issuing and maintaining public key certificates.

Both CAs and Registration Authorities (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 Status Protocol (OCSP) Responders and Server-based 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.

1.3.1 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;
- Accepting and processing applications from external PKIs desiring to cross-certify with the ECA PKI;
- Determining the mappings between ECA certificate policies and the external PKI certificate policies; and,
- Review the results of ECAs' compliance audits to determine if the CAs are meeting the stipulations of this CP and associated approved CPSs, 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.

1.3.2 Certification Authorities

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. A CA may also perform key escrow and support key recovery functions for the PKI. CA is an inclusive term and includes all types of CAs. CA, as used in this document, includes component parts which may be on the same hardware/software system or an integrated set of hardware and software within the control of a designated security boundary. Examples of components would be CA web servers/portals, databases, Key Escrow Systems (KES) and internal directories. All hardware, software and security requirements specified for CAs apply equally to the CA components. Any CA requirement expressed in this Policy applies to all CA types and components 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."

1.3.3 Card Management System

A Card Management System (CMS) is used as part of the process to issue Personal Identity Verification Interoperable (PIV-I) tokens which contain printed card elements, certificates and private keys, and other data objects including digitally signed biometrics. PIV-I issued credentials shall be managed only by authorized CMSs. In the context of this policy, requirements specified for CMSs are applicable for any CMS that supports the issuance of certificates that assert any of the PIV-I OIDs, specifically the Medium Hardware PIV-I and Card Authentication PIV-I OIDs. CMSs supporting digitally signed data elements use a Content Signing PIV-I certificate. If the CMS has a credential that allows it to access the CA and request certificate issuance or revocation, then requirements specified for RAs also apply to the CMS, and privileged users on the CMS who can direct it to perform certificate related actions are considered to be RAs.

1.3.4 Registration Authorities

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.

RAs register subscribers, approve certificate issuance, and perform key recovery operations. Not all RAs are authorized to perform all RA functions. An RA designated to perform key recovery operations may be referred to as a Key Recovery Authority (KRA). KRAs can be RAs from the organization operating the ECA CA or from the subscriber organization. The KRAs from subscriber organizations shall only be able to recover keys of subscribers from their organization. The specific privileges, duties and responsibilities of individual RAs within the PKI are identified in the appointment documentation.

1.3.5 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 U.S. government agency at local, state or Federal level;
- Employees of state and local governments conducting business with a .government agency at local, state or Federal level;
- Employees of foreign governments or organizations conducting business with a U.S. Government agency at local, state or Federal level;
- Individuals communicating securely with a U.S. 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 U.S. 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.

1.3.6 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.

1.3.7 Other Participants

1.3.7.1 Trusted Agents

ECAs may choose to use the services of Trusted Agents to assist CMAs in performing any identity verification and authorization verification tasks. 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 and/or authority of the Subscriber. Trusted Agents do not have privileged access to CMA functions, are considered agents of the CMA. Trusted agents are not considered CMA.

1.3.7.2 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 (e.g., routers, firewalls) in accordance with Section 3.2.3.3, and is responsible for meeting the obligations of Subscribers as defined throughout this document. PKI Sponsor is not considered a trusted role.

1.3.7.3 Affiliated Organization

An Affiliated Organization is an organization that has a relationship with a subscriber and sponsors that subscriber for obtaining a certificate. Affiliated Organizations are responsible for verifying the affiliation at the time of certificate application and requesting revocation of the certificate if the affiliation is no longer valid.

1.3.7.4 PKI Point of Contact

PKI Point of Contact (POC) is the person designated by the subscriber's organization to whom subscribers surrender their hardware cryptographic tokens when leaving the organization. PKI POC shall zeroize or destroy the hardware token promptly upon receipt. Using means that provide source authentication and integrity, the

PKI POC shall notify the CMA of the surrendered token destruction and request the revocation of all certificates associated with the surrendered token.

1.3.7.5 Group/Role Manager

A Group/Role Manager shall be responsible for managing the Group/Role as described in Section 3.2.5. A Group/Role Manager is not a trusted role.

1.3.7.6 Other 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.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

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, integrity, 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.

1.4.1.1 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.

1.4.1.2 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.

1.4.1.3 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 cyber attacks, environmental disasters, physical damage, system penetration, violation of authorization, human error, and communications monitoring or tampering.

1.4.1.4 General usage

This section contains definitions for the 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. Each Relying Party should carry out this risk analysis.

Medium and Medium Token Assurance: This level is intended for applications handling sensitive medium value information, with the exception of transactions involving issuance or acceptance of contracts and contract modifications. Examples of medium and medium token assurance applications 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 and Medium Hardware PIV-I 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. Examples of medium hardware assurance applications include:

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

Card Authentication PIV-I Assurance: This level is intended only for use in physical access situations to support high volume throughput. Because Card Authentication assurance certificates do not require activation data to unlock the private key, validation of a Card Authentication certificate provides only proof of the physical presence of the smart card token. It provides no proof of the identity of the individual in possession of the token. PIV-I cards and associated certificates are not intended to replace existing approval mechanisms for physical access, they may provide one layer of protection to identify the user.

Content Signing PIV-I Assurance: This level is intended only for use in digitally signing data objects on a PIV-I smart card and shall not be used for any other purpose. Content Signing PIV-I certificates shall only be issued to CMSs.

1.4.2 Prohibited Certificate Uses

No Stipulation.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

The EPMA is responsible for the definition, revision and promulgation of this policy. The EPMA is the Office of the DoD Chief Information Officer, and its designees.

1.5.2 Contact Person

Questions regarding this CP should be directed to:

ECA POLICY MANAGEMENT AUTHORITY
9800 SAVAGE ROAD SUITE 6699
FORT GEORGE G MEADE MD 20755-6699

1.5.3 Person Determining CPS Suitability for the Policy

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

1.5.4 CPS Approval Procedures

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

1.5.5 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.

1.6 DEFINITIONS AND ACRONYMS

See Sections 14 and 15.

2 PUBLICATIONS AND REPOSITORY RESPONSIBILITIES

2.1 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.

2.2 PUBLICATION OF CERTIFICATION 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;
- Certificates issued to the CA;
- A copy of this Policy, including any waivers granted to the CA by the EPMA; and,
- An abridged version of the CPS under which the ECA operates. The published version shall at least include the following topics covered under the ECA CP:
    - Section 1.5, ECA Contact Information;
    - Section 9, Other Business and Legal Matters;
    - Section 3.2, Initial Identity Validation;
    - Section 4.9, Certificate Revocation and Suspension; and,
    - Any additional information that ECA deems to be of interest to the Relying Parties (e.g., mechanisms to disseminate ECA trust anchor, to provide notification of revocation of ECA root or ECA certificate).

The procedures shall be designed to ensure CA certificates and CRLs are available for retrieval 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually. (Practice note: Where repository systems are distributed, the availability figures apply to the system as a whole, rather than each component. Availability targets exclude network outages.)

2.3 TIME OR FREQUENCY OF PUBLICATION

Certificates shall be published following Subscriber acceptance as specified in Section 4.4 and proof of possession of private key as specified in Section 3.2.1. The CRL is published as specified in Section 4.9.7. 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.

2.4 ACCESS CONTROLS ON REPOSITORIES

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

Certificates that contain the universally unique identifier (UUID) in the subject alternative name extension shall not be distributed via publicly accessible repositories using various protocols such as LDAP and HTTP.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

All CAs shall be able to generate and sign certificates that contain an X.500 Distinguished Name (DN). Certificate DNs shall conform to the format specified in the certificate profiles in Section 10.

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 of 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 User Principal Names (UPN) are used, they shall accurately reflect organizational structures and authorization to access the account.

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. ECAs shall not certify other CAs.

3.1.3 Anonymity or Pseudonymity of Subscribers

A CA shall not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are contained in the applicable certificate profile (see Section 7.1.4), and are established by the EPMA established naming authority.

3.1.5 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.

3.1.6 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.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 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.

3.2.2 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. Requests for certificates for Subscribers associated with an organization shall include the organization name, address and documentation of the existence of the organization, and the proof of the Subscribers' affiliation with 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 is prohibited, except for Group/Role certificates.

3.2.3 Authentication of Individual Identity

3.2.3.1 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. The CMA shall also verify citizenship of each applicant for all certificates so that citizenship can be included in the certificate. Finally, the CMA shall record the process that was followed for each certificate, including the mechanism used to verify applicant citizenship. At a minimum, process documentation must include:

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

For all policies except PIV-I, applicant identity proofing requires individual applicants to provide two official identification credentials, at least one of which must be a photo ID issued by a government authority with jurisdiction over the issuance of such credentials to the applicant (e.g., a driver's license). Each ECA shall specify in its CPS the forms of identification that will be accepted for each country for which the ECA will be performing identity proofing. 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 PIV-I policies, applicant identity proofing requires individual applicants to provide two identity source documents in original form which come from the list of acceptable documents included in *Form I-9, OMB No. 1115-0136, Employment Eligibility Verification*. At least one document shall be a valid U.S. State or Federal Government-issued picture identification (ID).

Applicant citizenship verification requires individual applicants to provide an official credential issued by a government authority with jurisdiction over the issuance of such credentials to the applicant. For U.S. citizenship, only the following credentials may be accepted:

- U.S. Passport
- Certified birth certificate issued by the city, county, or state of birth[1], in accordance with applicable local law
- Naturalization Certificate[2]
- Certificate of Citizenship[3]
- FS-240 – Consular Report
- DS-1350 – Certification of Report of Birth

When citizenship verification is performed within the US, for citizenship verification of non-U.S. citizens, the applicant must present a passport issued by the country of citizenship. When citizenship verification is performed outside the U.S. by authorized DoD employees, the applicant must present a passport or another document from the approved documents list. The approved documents list can be found on the ECA web site at iase.disa.mil/pki/eca.

Verification of citizenship is required for all certificates. For Medium and Medium Token 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;
- A U.S. notary public[4]; or,

[1] A certified birth certificate has a registrar's raised, embossed, impressed or multicolored seal, registrar's signature, and the date the certificate was filed with the registrar's office, which must be within 1 year of birth. A delayed birth certificate filed more than one year after birth is acceptable if it lists the documentation used to create it and is signed by the attending physician or midwife, or lists an affidavit signed by the parents, or shows early public records.

[2] A Naturalization Certificate is a document issued by U.S. Citizenship and Immigration Service (USCIS) since October 1, 1991 and the Federal Courts or certain State Courts on or before September 30, 1991 as proof of a person obtaining U.S. citizenship through naturalization.

[3] A Certificate of Citizenship is a document issued by U.S. Citizenship and Immigration Service (USCIS) is proof of a person having obtained U.S. citizenship through derivation or acquisition at birth (when born outside of the United States).

[4] Note that U.S. embassies and consulates provide notarial services for U.S. citizens residing outside the U.S.

- An individual authorized to perform identity proofing as described in Section 11 (note that identity proofing as described in Section 11 is not acceptable for PIV-I assurance certificates).

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, Medium Hardware PIV-I, and Card Authentication PIV-I 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.

For PIV-I certificates, application also requires the collection of an electronic facial image and two electronic fingerprints at the time of the applicant's appearance before the CMA or Trusted Agent. The electronic facial image shall be used for printing facial image on the card, as well as for performing visual authentication during card usage for physical access. A new facial image shall be collected each time a card is issued, and if a new card is being issued to an existing subscriber, existing biometrics shall be verified. Fingerprints shall be stored on the card for automated authentication during card usage. See Section 12 for additional biometric formatting information. The PIV-I identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV-I credential without the cooperation of another authorized person.

Minors and others not competent to perform face-to-face registration alone shall be accompanied by an authorized 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.

3.2.3.2 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 (see Section 3.3.1) except that the new certificate is valid concurrently with the existing certificate but with a potentially different expiration date.

3.2.3.3 Authentication of Component Identities

Some computing and communications components (e.g., routers, firewalls) may be named as certificate subjects, except for certificates asserting Medium Hardware PIV-I which can only be issued to human subscribers. In such cases, the component must have a human PKI Sponsor as described in Section 1.3.7.2.

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.

For Content Signing PIV-I certificates, the PKI Sponsor must either have their identity personally verified by a CMA or must have a Medium Hardware or Medium hardware PIV-I certificate issued by the ECA issuing the Content Signing PIV-I certificate. PKI Sponsors for Content Signing PIV-I certificates must also be appointed in writing by an approving authority or be party to a contract for PIV-I issuance services.

In the case a PKI Sponsor is changed, the new PKI Sponsor shall review the status of each component under his/her sponsorship to ensure it is still authorized to receive certificates.

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 3.2.3.

3.2.4 Non-Verified Subscriber Information

Certificates shall not contain information that is not verified.

3.2.5 Validation of Authority

Certificates that contain explicit or implicit organization affiliations shall be issued only after ascertaining the Subscriber has the authorizations to act on behalf of the organization in the implied capacity. Examples of these include CA, RA, and Group/Role certificates.

Group/Role certificates for each Group/Role may be issued to one or more individual members of the Group/Role provided the following requirements are met for each Group/Role:

- Group/Role Manager name shall be provided to the DoD PKI ECA Liaison Officer.
- Group/Role formation and its DN shall be approved by the DoD PKI ECA Liaison Officer based on the justification provided by the requesting organization.
- ECA shall authenticate the DoD PKI ECA Liaison Officer approval of the Group/Role formation and its DN prior to the issuance of certificates for that Group/Role.
- ECA shall authenticate the identity of the Group/Role Manager using the initial identity proofing process defined in this CP or using the ECA issued certificate of assurance level commensurate with the required assurance level for the Group/Role.
- When Group/Role Manager changes,
    - The new Group/Role Manager name shall be provided to the DoD PKI ECA Liaison Officer.
    - The new Group/Role Manager's identity shall be authenticated by the ECA using the initial identity proofing process defined in this CP or using the ECA issued certificate of assurance level commensurate with the required assurance level for the Group/Role.
    - The two Group/Role Managers (old and new) shall ensure that there is no gap in control of the private keys.

- All certificates issued to the Group/Role shall have the same unique Subject DN that meaningfully conveys the Group/Role name.
- Encryption certificates issued to the Group/Role may share a single key pair.
    - Members of the Group/Role may be issued a single encryption certificate or may be issued separate encryption certificates that have the same subject public key.
- A Group/Role signature certificate issued to an individual member of the Group/Role shall be distinct with distinct public key and shall contain the DN of the individual in the subject alternative name extension of the Group/Role signature certificate.
- Each individual member of the Group/Role shall be responsible for the decryption private keys and shall agree to the following in a signed statement:
    - To protect the private keys associated with their Group/Role signature and encryption certificates.
    - To not to share these keys with anyone, even other Group/Role members.
    - To not backup any private keys. Note: Group/Role member may obtain a new copy of the same private key from the Group/Role Manager, if the need arises, e.g., the copy of the Group/Role member private key is destroyed.
    - To maintain an up-to-date list of applications on which the decryption private key is installed.
- A Group/Role Manager shall be responsible for validating the authority of a Group/Role member to the ECA.
- A Group/Role Manager shall be responsible for ensuring control of decryption private keys.
- A Group/Role Manager shall maintain a list with the following information. The list shall be kept current on a daily basis, i.e., updated within one working day of the changes. Note that this list is a cumulative historical record of Group/Role membership and not merely a list of current members.
    - Individuals who are or have been the members of the Group/Role. The information shall include start date/time and end date/time.
    - Individuals who have been issued signature certificates for the Group/Role. The information shall include CA DN and certificate serial number for each individual for each certificate.
    - Individuals who have been issued or provided encryption certificates for the Group/Role. The information shall include CA DN and certificate serial number for each individual for each certificate.
    - Individuals who have been provided copies of the private key associated with the Group/Role encryption certificates. The information shall include date/time the keys were provided, CA DN, certificate serial number, and date/time the keys were returned (hardware or software) or destroyed (software) by the individual member.
    - Date/time the hardware module was zeroized or destroyed by the Group/Role Manager.
- The Group/Role Manager or an individual may request revocation of the signature certificate issued to the individual as a member of the Group/Role.
- The Group/Role Manager shall be responsible for determining whether to request revocation of all encryption certificate(s) issued to the Group/Role, e.g., when the key is compromised or when an individual leaves Group/Role[5].

[5] An example of revocation is when the Group/Role Manager is unsure if a departing Group/Role member has destroyed copies of the software decryption private keys installed in various applications.

3.2.6 Criteria for Interoperation

The Certificate and CRL Profile in this CP shall form a basis for assessing interoperability with the ECA PKI. However, the decision to cross certify with an external PKI shall reside with the EPMA as specified in Section 1 of this CP.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

Re-key requests for certificates can be authenticated on the basis of current valid Subscriber certificates as long as the validity period of the new certificate does not extend beyond the periodic in-person authentication requirements listed in the table below.

Policy	In-Person Authentication Requirement
Medium, Medium Device, Medium Token Assurance	Every 9 years
Medium Hardware, Card Authentication PIV-I, Medium Hardware PIV-I Assurance	Every 3 years

CA identity shall be validated through use of the current signature key or initial registration process. Identity shall be established through initial registration process at least once every three years.

For Medium Device SHA-256 certificates, identity may be established through the use of current signature key or using means commensurate with the strength of the certificate being requested.

3.3.2 Identification and Authentication for Re-Key After Revocation

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

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests must be authenticated (see Section 4.9.3). 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.

3.5 IDENTIFICATION AND AUTHENTICATION FOR KEY RECOVERY REQUEST

3.5.1 Subscriber Key Recovery Request

Subscribers are authorized to request the recovery of their own escrowed keys.
For automated self-recovery of private keys, the CA shall authenticate the Subscriber using a valid ECA PKI certificate at the same or higher strength policy OID as the policy OID in the certificate associated with the escrowed key.

Alternatively, the Subscriber may establish his or her identity to an RA, either through the use of a valid ECA PKI certificate at the same or higher strength policy OID as the policy OID in the certificate associated with the escrowed key, or by using the procedures specified in Section 3.2.3.1 for authenticating identity. If the authentication is not based on digital signatures that can be verified using public key certificates, the RA or TA shall personally verify the identity of the Subscriber prior to initiating the key recovery request.

If a TA is performing the requestor validation, the TA shall establish his or her identity to the RA based on a digital signature that can be verified using the public key certificate of the TA. The TA shall use a valid ECA PKI certificate at the same or higher strength policy OID as the policy OID in the certificate associated with the escrowed key.

3.5.2 Third Party Key Recovery Request

Entities other than the Subscribers (third parties) may request recovery of escrowed keys. All third party recovery requests shall be coordinated through an RA or TA, who shall validate the authorization of the requestor in consultation with organization management and/or legal counsel, as appropriate.

The requestor shall establish his or her identity to the RA or TA, either through the use of a valid ECA PKI certificate at the same or higher strength policy OID as the policy OID in the certificate associated with the escrowed key, or by using the procedures specified in Section 3.2.3.1 for authenticating identity. If the authentication is not based on digital signatures that can be verified using public key certificates, the RA or TA shall personally verify the identity and authority of the requestor prior to initiating the key recovery request.

If a TA is performing the requestor validation, the TA shall establish his or her identity to the RA based on a digital signature that can be verified using the public key certificate of the TA. The TA shall use a valid ECA PKI certificate at the same or higher strength policy OID as the policy OID in the certificate associated with the escrowed key.

4 CERTIFICATE LIFE-CYCLE 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.

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. A CA shall only recognize the RAs to whom it has issued certificates.

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.

4.1.1 Who Can Submit a Certificate Application

Certificate application may be submitted to the CA by the Subscriber, or an RA on behalf of the Subscriber.

4.1.2 Enrollment Process and Responsibilities

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 3.2);
- 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 3.2.1); and,
- Provide a point of contact for verification of any roles or authorizations requested.

Requests by ECAs for CA certificates shall be submitted to the EPMA using the contact provided in Section 1.5.2, 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* [RFC 3647].

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.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

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.

4.2.2 Approval or Rejection of Certificate Applications

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.

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.

4.2.3 Time to Process Certificate Applications

The entire process from applicant appearing before one of the required identity verifiers to certificate issuance shall take no more than 30 days.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions During Certificate Issuance

The CA shall authenticate a certificate request, ensure that the public key is bound to the correct Subscriber, obtain a proof of possession of the private key, then generate a certificate, and provide the certificate to the Subscriber. The CA shall publish the certificate to a repository in accordance with Section 4.4.2.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The Subscriber shall be notified of certificate issuance.

4.4 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 9.6.3;
- 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[6];
- Notify the Subscriber if their decryption private key is escrowed; and,
- Document the Subscriber's acceptance of its responsibilities and its certificate.

[6] This signature could be obtaining in conjunction with Subscriber Identity Declaration signature described in Section 3.2.3.1. For example, the Subscriber could sign one form that contains clauses for declaration of identity and for acceptance of Subscriber obligations.

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 (e.g., routers, firewalls), the PKI Sponsor (as defined in Section 1.3.7.2) shall perform the functions of the Subscriber.

4.4.1 Conduct Constituting Certificate Acceptance

Subscriber signature (wet or digital) on certificate application and lack of objection to published certificate shall constitute certificate acceptance. Subscriber signature shall be collected before a CA allows a Subscriber to make effective use of its private key.

4.4.2 Publication of the Certificate by the CA

CA certificates and Subscriber encryption certificates shall be published to the appropriate repositories.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

The Subscriber shall not use the signature private key after the associated certificate has been revoked or has expired.

The Subscriber may continue to use the decryption private key solely to decrypt previously encrypted information after the associated certificate has been revoked or has expired.

The use of the private key shall be limited in accordance with the key usage extension in the certificate.

If the extended key usage extension is present and implies any limitation on the use of the private key, those constraints shall also be observed. For example, the OCSP Responder private key shall be used only for signing OCSP responses.

4.5.2 Relying Party Public Key and Certificate Usage

The relying parties shall ensure that a public key in a certificate is used only for the purposes indicated by the key usage extension, if the extension is present.

If the extended key usage extension is present and implies any limitation on the use of the certificate, those constraints shall also be followed.

4.6 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.

4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if the certificate has not reached the end of its validity period, the certificate has not been revoked, the total life times of certificates issued (including the new certificate) for that public key do not exceed the next in-person identity proofing date, and the Subscriber name and attributes are still correct.

4.6.2 Who May Request Renewal

The Subscriber or RA may request the renewal of a Subscriber certificate. The Group/Role Manager may request the renewal of Group/Role encryption certificate.

4.6.3 Processing Certificate Renewal Requests

The renewal process shall be in accordance with the certificate issuance process described in Section 3.2. Identity validation may be in accordance with Section 3.2.3.1 or Section 3.2.3.2. If the current certificate does not contain citizenship, the citizenship must be verified and included in the certificate in accordance with Section 3.2.3.1.

4.6.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

See Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to other Entities

See Section 4.4.3.

4.7 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.

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 certificate lifetimes given are maximums. An ECA may always require shorter lifetimes. The following certificate lifetimes are for Subscribers; ECA certificate lifetimes are provided in Section 5.6.

Medium and Medium Token Assurance	Signature certificate re-key every three years Encryption certificate re-key every three years Identity established through use of current signature key or in-person; In-person identity must be established every 9 years and 30 days Must prove possession of corresponding private key For any certificate issued on a token with an expiration date physically printed on the token, certificate expiration for all certificates associated with the token shall not be later than the expiration date printed on the token
Medium Device	Signature certificate re-key every three years Encryption certificate re-key every three years Identity established through use of current signature key or through the PKI Sponsor process identified in Section 3.2.3.3; the PKI Sponsor identity establishment process must be performed every 9 years and 30 days Must prove possession of corresponding private key

Medium Hardware, Card Authentication PIV-I, and Medium Hardware PIV-I Assurance	Signature certificate re-key every three years Encryption certificate re-key every three years Authentication certificate re-key every three years Identity established through use of current signature key or in-person; In-person identity must be established every 3 years and 30 days Must prove possession of corresponding private key For any certificate issued on a token with an expiration date physically printed on the token, certificate expiration for all certificates associated with the token shall not be later than the expiration date printed on the token
Content Signing PIV-I	Certificate re-key every six years Identity established through the process identified in Section 3.2.3.3 each time a Content Signing PIV-I key is issued The certificate expiration date for a Content Signing PIV-I certificate used to sign data elements on a token shall be later than the expiration date printed on the token

4.7.1 Circumstance for Certificate Re-Key

A certificate shall be re-keyed when it can no longer be renewed.

A revoked certificate shall not be re-keyed.

A valid certificate when re-keyed, need not be revoked, but shall not be further re-keyed, renewed, or updated.

Requirements for CA re-key are described in Section 5.6.

4.7.2 Who May Request Certification of a New Public Key

The Subscriber or RA may request the re-key of a Subscriber certificate. The Group/Role Manager may request the re-key of Group/Role encryption certificate.

4.7.3 Processing Certificate Re-Keying Requests

The re-key process shall be in accordance with the certificate issuance process described in Section 3.2. Identity validation may be in accordance with Section 3.3. If the current certificate does not contain citizenship, the citizenship must be verified and included in the certificate in accordance with Section 3.2.3.1.

4.7.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See Section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

See Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.8 CERTIFICATE MODIFICATION

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.

When a root CA updates its private signature key and thus generates a new public key, the new trust anchor shall be provided to all CAs, RAs, and Subscribers in accordance with the requirements of Section 6.1.4.

When any other CA updates its private signature key and thus generates a new public key, the CA shall obtain a new certificate from the parent CA in accordance with the requirement of Section 4.1.

4.8.1 Circumstance for Certificate Modification

A certificate may be modified if some of the information other than the DN, such as the e-mail address or authorizations, has changed.

If the Subscriber name has changed, the Subscriber shall undergo the initial registration process.

4.8.2 Who May Request Certificate Modification

The Subscriber or RA may request the modification of a Subscriber certificate. The CA or RA shall validate any changes in the subscriber authorizations reflected in the certificate. The Group/Role Manager may request the modification of Group/Role encryption certificate.

4.8.3 Processing Certificate Modification Requests

The certificate modification process shall be in accordance with the certificate issuance process described in Section 3.2. Identity validation may be in accordance with Section 3.2.3.1 or Section 3.2.3.2. In addition, the CA or RA shall validate any changes in the subscriber authorizations reflected in the certificate. If the current certificate does not contain citizenship, the citizenship must be verified and included in the certificate in accordance with Section 3.2.3.1.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 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.

For all certificates that express an organizational affiliation, the ECA shall require that the Affiliated Organization inform the ECA of any changes in the Subscriber affiliation. If the Affiliated Organization no longer authorizes the affiliation of a Subscriber, the ECA shall revoke any certificates issued to that Subscriber containing the organization affiliation. If an Affiliated Organization terminates its relationship with the ECA such that it no longer provides updates to organizational affiliation information, the ECA shall revoke all certificates containing that Affiliated Organization's information.

4.9.2 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 revoke a Subscriber's certificate on behalf of any authorized party as specified in its CPS. The authorized parties shall include persons appointed by the EPMA to request revocation of any subscriber or CA certificate.

4.9.3 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). 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. Request can be authenticated using the certificate that is being requested to be revoked.

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 or PKI POC (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. Using means that provide source authentication and integrity, the PKI POC shall notify the CMA of token destruction and request the revocation of all certificates associated with the token. The security of source authentication and integrity shall be commensurate with the security provided by the key(s) being destroyed and certificates being revoked. 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 for the reason of key compromise.

4.9.4 Revocation Request 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 4.9.7.

4.9.5 Time Within Which CA Must Process the Revocation Request

The CA shall process all revocation requests within one hour of receipt. CRL issuance frequency is addressed in Section 4.9.7.

4.9.6 Revocation Checking Requirements for Relying Parties

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.

4.9.7 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 superseded 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. In order to ensure that relying parties obtain a current, valid CRL, ECA Root CA CRL "next update" will be past "this update" by CRL issuance frequency and 1 day. In other words, next update ≥ this update + CRL Issuance Frequency + 1 day. In order to ensure that relying parties obtain a relatively recent CRL, ECA Root CA CRL "next update" will not be past "this update" by more than 35 days. In other words, next update ≤ this update + 35 days.

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. In order to ensure that relying parties obtain a current, valid CRL, "next update" will be past "this update" by CRL issuance frequency and 4 hours. In other words, next update ≥ this update + CRL Issuance Frequency + 4 hours. In order to ensure that relying parties obtain a relatively recent CRL, "next update" will not be past "this update" by more than 7 days. In other words, next update ≤ this update + 7 days.

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.

4.9.8 Maximum Latency for CRLs

The CRL shall be posted upon generation, but within no more than four hours after generation.

4.9.9 On-Line Revocation/Status Checking Availability

In addition to CRLs, ECAs shall also support on-line status checking via OCSP Responders. Relying party software using on-line revocation checking need not obtain or process CRLs.

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

- Accurate and up-to-date information from the authorized CA is used to provide the revocation status;
- Latency of certificate status information shall meet or exceed the requirements for CRL issuance stated in Section 4.9.7;
- OCSP Responder shall process requests and provide responses compliant with *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol* [RFC 6960]; and,
- Revocation status responses provide authentication and integrity services commensurate with the assurance level of the certificate being checked.

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) are being authenticated by the CSA.

4.9.10 On-Line Revocation Checking Requirements

Relying Parties may optionally use on-line status checking. Since some relying parties may not be able to accommodate on-line communications, all CAs shall be required to support CRLs. Client software using on-line revocation checking need not obtain or process CRLs.

Relying parties (including CMAs) shall only rely upon OCSP Responders approved in accordance with the requirements of this CP.

4.9.11 Other Forms of Revocation Advertisements Available

An ECA is required to generate, issue and publish a CRL. An ECA is also required to provide OCSP Responder service. In addition, 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 and must meet issuance and latency requirements for CRLs stated in Sections 4.9.7 and 4.9.8.

4.9.12 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 4.9.3. Refer also to Sections 5.3.6 and 5.7.1.

4.9.13 Circumstances for Suspension

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

4.9.14 Who Can Request Suspension

Not Applicable.

4.9.15 Procedure for Suspension Request

Not Applicable.

4.9.16 Limits on Suspension Period

Not Applicable.

4.10 CERTIFICATE STATUS SERVICES

Certificate Status Authorities such as SCVP shall comply with the requirements of this CP and applicable Internet Standards.

4.10.1 Operational Characteristics

Certificate Status Authorities such as SCVP shall comply with the requirements of this CP and applicable Internet Standards.

4.10.2 Service Availability

Certificate Status Authorities such as SCVP shall comply with the requirements of this CP and applicable Internet Standards.

4.10.3 Optional Features

Certificate Status Authorities such as SCVP shall comply with the requirements of this CP and applicable Internet Standards.

4.11 END OF SUBSCRIPTION

Subscription is synonymous with the certificate validity period. The subscription ends when the certificate is revoked or expired.

4.12 KEY ESCROW AND RECOVERY

The ECA PKI supports key escrow and recovery for private keys associated with encryption certificates. The ECA PKI does not support key recovery using key encapsulation techniques.

4.12.1 Key Escrow

4.12.1.1 Circumstances for Key Escrow

Section 6.2.3 specifies the types of certificates that are allowed to be escrowed.

4.12.1.2 Escrowing Keys

Escrowed keys shall be stored in a protected KES using the physical, personnel, and technical security controls commensurate with those for the CA. All requirements for storage and transfer of private keys shall apply to the process of escrowing private keys.

Escrowed keys shall be maintained within the KES for a minimum of one year after the expiration of the certificate associated with the key. If the certificate associated with the key is renewed or modified without changing the key, the escrowed key shall be maintained within the KES for a minimum of one year after the expiration date of the renewed or modified certificate associated with the key. Escrowed keys shall be archived as described in Section 5.5. KES security audit requirements are specified in Section 5.4.

4.12.1.3 Notification of Key Escrow to Subscriber

As part of the key escrow process, all subscribers for whom the PKI escrows keys shall be notified that the private keys associated with their encryption certificates are being escrowed.

4.12.2 Key Recovery

The ECA PKI supports key escrow and recovery of an escrowed key where access to that key is a necessary condition for access to data. The ECA PKI does not provide a data recovery service, nor is this CP intended to change the authority of any individual or organization to access data.

Recovery of private keys associated with previously held encryption certificates may be performed as part of any certificate issuance process to ensure that earlier encryption private keys are available to Subscribers.

During delivery, escrowed keys shall be protected against disclosure to any party except the requestor and the trusted roles responsible for the recovery.

4.12.2.1 Circumstances for Key Recovery

Escrowed keys may be recovered to support the recovery of encrypted data for business, law enforcement or other requirements. In general, escrowed keys are recovered for the following purposes:

- The original copy of the escrowed key has been lost or damaged and the Subscriber cannot access data encrypted with the corresponding public key;

- The certificate is to be re-keyed and the earlier issued private keys are recovered to be included on the token containing the re-keyed certificate; or,
- An authorized third party (other than the PKI Sponsor) requires access to data encrypted with the corresponding public key.

4.12.2.2 Who May Request Key Recovery

Subscribers may request recovery of their own escrowed keys either through an RA or via an automated process direct to the CA.

RAs may request recovery of escrowed keys on behalf of the Subscriber as part of the re-key or re-issuance process.

Internal Requestor: An Internal requestor is any requestor who is in the subscriber's supervisory chain or otherwise authorized to obtain the subscriber's key for the organization. The intent of this CP is not to change the policy and procedures of the organization. The subscribers' organization shall appoint authorized requestors and the ECA shall implement the KES so that the existing organization policy regarding access and release of sensitive information can be met.

External Requestor: An External Requestor is an investigator or someone outside the subscribers' organization with authorized court order to obtain the decryption private key of the subscriber. An external requestor must work with an internal requestor unless the law requires the ECA to release the subscriber's private key without approval of the subscriber and subscriber's organization. Nothing in this document is intended to change the current procedures for obtaining information about individuals in connection with such requests. The ECA and subscribers' organizations shall appoint authorized personnel and implement the KES so that the existing organization policy regarding release of sensitive information can be met.

4.12.2.3 Processing Key Recovery Requests

Subscribers may electronically submit requests on their own behalf directly to an RA. Such requests shall be signed by a private key associated with a ECA PKI issued Identity or Signature certificate asserting the same or stronger policy OID as that of the certificate associated with the escrowed key.

Subscribers may use automated means to request their escrowed keys from the KES if they possess a valid ECA PKI issued Identity or Signature certificate asserting the same or stronger policy OID as that of the certificate associated with the escrowed key. The KES shall only provide escrowed keys to Subscribers via an automated means after performing all of the following:

- Verifying that the authenticated identity of the requestor is the same as the Subscriber associated with the escrowed keys being requested;
- Ensuring that the escrowed keys are being sent only to the authenticated Subscriber associated with the escrowed keys; and,
- Ensuring that the recovered keys are encrypted during transmission in accordance with Section 6.2.6 and that activation data used to protect access to the recovered keys is in accordance with Section 6.4.1.

Subscribers may submit a request, signed by hand, to either an RA or TA. The RA or TA shall validate the identity of the requestor. TAs shall forward the request via a digitally signed mechanism to an RA. The RA shall authenticate the information in the request.

Third party requestors shall submit requests to either an RA or a TA. Paper requests shall be hand-signed; electronic requests shall be digitally signed by a private key associated with a valid ECA PKI issued Identity or Signature certificate asserting the same or stronger policy OID. The RA or TA shall validate the identity of the requestor and the RA shall determine the authority of the requestor to recover the escrowed key in consultation with organization management and/or legal counsel, as appropriate. TAs shall forward information via a digitally signed and encrypted email to the RA. Third party key recovery operations shall be performed under the control of two RAs.

Third party requestors shall be bound, by legal and policy means, to the key protection and other provisions of this CP. The requestor shall sign a document prepared by the requestor, which includes the following statement: “I hereby state that I have legitimate and official need to recover this key in order to obtain (recover) the encrypted data that I have authorization to access. I acknowledge receipt of a recovered ECA encryption key associated with the subscriber identified here. I certify that I have accurately identified myself to the RA/TA, and truthfully described all reasons that I require access to data protected by the recovered key. I acknowledge my responsibility to use this recovered key only for the stated purposes, to protect it from further exposure, and to destroy all key materials or return them to the RA/TA when no longer needed. I understand that I am bound by subscriber’s organization policies, applicable laws and Federal regulations concerning the protection of the recovered key and any data recovered using the key.”

Once an RA has received and validated a key recovery request, the RA shall initiate the key recovery. The RA shall authenticate to the KES using a mechanism commensurate with the cryptographic strength of the strongest key stored in the KES.

All copies of recovered keys shall be continuously protected using mechanisms at least commensurate with the level of the data the key provides access to or protects by the recovering trusted roles during the recovery and delivery to the authenticated and authorized requestor. Recovered keys shall be protected during transmission in accordance with Section 6.2.6 and activation data used to protect access to the recovered keys shall be in accordance with Section 6.4.1.

4.12.2.4 Notification of Key Recovery to Subscriber

Subscribers shall be notified of all attempts to recover escrowed keys based on a request using a Subscriber’s private key.

There is no requirement to notify the Subscriber of key recovery requests made by parties other than the Subscriber.

4.12.2.5 Notification of Key Recovery by the CA to Other Entities

There is no requirement to notify other entities of key recovery requests.

5 FACILITY, MANAGEMENT, AND OPERATIONAL 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.

CMSs shall operate on machines dedicated to the issuance of PIV-I cards.

Unauthorized use of CMA or CMS equipment is forbidden. Physical security controls shall be implemented that protect the CMA or CMS hardware and software from unauthorized use. CMA and CMS 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 or CMS equipment and operations shall be in accordance with that afforded the most sensitive business and financial information.

5.1.2 Physical Access

ECA, CSA, and CMS equipment shall always be protected from unauthorized access. Physical access security shall include the following:

- Ensure no unauthorized access to the hardware is permitted;
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers;
- Ensure manual or electronic monitoring for unauthorized intrusion at all times;
- Ensure an access log is maintained and inspected periodically; and,
- Require two person physical access control to both the cryptographic module and computer systems.

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 and CMS cryptographic modules shall be inactivated prior to storage. When not in use, removable CMA and CMS cryptographic modules, and any activation information used to access or enable CMA and CMS cryptographic modules or CMA and CMS 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 or data managed by the CMS. 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, CSA, and CMS 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

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

The ECA or CMS 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 5.7.4.

5.1.6 Media Storage

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

5.1.7 Waste Disposal

Media used to collect or transmit information discussed in Section 9.4 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 the list of these individuals and the individuals themselves must be 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 when issuing RA certificates;
- 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;
- Hardware cryptographic module programming and management, if appropriate; and,
- Key escrow and recovery.

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 initial identity, either through personal contact, or via Trusted Agents or employees, when allowed by this policy;
- Verifying the identity and authorization of entities requesting recovery of escrowed key material;
- Authorizing and facilitating the recovery of escrowed key material;
- Recovering escrowed key material if assigned that responsibility by the ECA PKI;
- 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 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 5.4 and 5.5 of this document;
- Review of the security audit log; and,
- Operation of the CMS.

Trusted agents and PKI POCs are also considered trusted roles.

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.

5.2.1.4 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.

5.2.2 Number of Persons Required for Task

CA, CSA, Content Signing PIV-I and CMS (other than Diversified Keys) key generation, activation and backup shall be performed under two-person control.

Third party key recovery is performed under two-person control as specified in Section 6.2.2.
Where multiparty control for logical access to the CA (excluding key recovery operations) is required, at least one of the participants shall be an ECA Administrator. A CA Auditor or CSA Auditor shall not be considered as participant for multiparty control for logical access. All participants must serve in a trusted role as defined in Section 5.2.1.Identification and Authentication for Each Role.

Individuals shall identify and authenticate themselves before being permitted to perform any actions set forth above for that role or identity.

5.2.3 Roles Requiring Separation of Duties

An RA may not have any other role on the CA, CSA, or CMS (e.g., ECA administrator, CA Auditor, CSA Auditor).

An Auditor may not have any other role on the CA, CSA, or CMS.

The CA, RA, and CMS software and hardware shall identify and authenticate its users and shall enforce the above role separation.

An individual that performs any trusted role shall only have one identity on the CA, RA, CSA, or CMS.

5.3 PERSONNEL CONTROLS

5.3.1 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 U.S. citizens. All persons holding other trusted roles except TAs and PKI POCs shall be U.S. citizens.

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 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 and CMS 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 or CMS operator;
- Have not knowingly been previously relieved of CMA, CMS 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 and CMS operators, shall either hold a U.S. 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;
- Education verification of highest or most relevant degree; and,
- Social Security trace shall show that the person has a valid social security number[7].

Qualified investigators shall perform the background checks. Adjudication of the background investigation shall be performed by a competent adjudication authority using a process consistent with United States Executive Order 12968 August 1995, or equivalent.

The results of these checks shall not be released except as required in Section 9.4.4. Background check procedures shall be described in the CPS.

5.3.3 Training Requirements

All personnel involved in the CMA and CMS operation shall be appropriately trained. Topics shall include the operation of the CMA or CMS 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 or CMS 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 or CMS operation. Any significant change to the CMA or CMS operation shall have a training (awareness) plan, and the execution of such plan

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

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.

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 Independent Contractor 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 which defines duties and procedures for each role shall be provided to the personnel filling that role.

5.4 AUDIT LOGGING PROCEDURES

This section describes the security requirements of a CMA's certificate issuing system (including CMSs), which includes the equipment used to register Subscribers; generate, sign, and manage certificates; and generate, sign, and manage revocation information. In the case where CMA equipment operates in a virtual machine environment (VME), requirements in this section and subsections apply to both the host[8] and the hypervisor event logs.

5.4.1 Types of Events Recorded

Requirements applied to CA, CSA and RA equipment:
All audit requirements apply to trusted roles and CA, CSA, and RA equipment, and any machines that are used to administer or manage the CA or CSA and any CMA equipment operated in a VME, including both the host and hypervisor. All of these machines are considered CMA equipment.

Any security auditing capabilities of the underlying CMA equipment operating system shall be enabled during installation (including any changes to the audit parameters).

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

- CMA application access (including logon, any attempts to assume a role, and manual entry of secret keys used for authentication);
- Messages received from any source requesting CMA actions (certificate requests, certificate signing, certificate revocation, compromise notification, key escrow request and escrowed key recovery request, certificate status request) – CSAs are exempt from this audit requirement;
- Actions taken in response to requests for CMA actions (including approval or rejection of a certificate status change request);
- Physical access to, loading, zeroizing, transferring keys to or from, backing-up, acquiring or destroying CMA cryptographic modules (including all addition, deletion, or changes to the trusted public keys);
- Receipt, servicing (e.g., keying or other cryptologic manipulations), and shipping hardware cryptographic modules (including receipt of all hardware/software, shipment of tokens, and zeroizing of tokens);
- Posting of any material to a repository;

[8] The various operating systems executing on a hypervisor are referenced by one or more of the following terms which are considered synonymous in this CP: host, virtual machine (VM), and guest operating system.

- Anomalies, error conditions, software integrity check failures, receipt of improper or misrouted messages (including number of unsuccessful authentication attempts exceeding maximum authentication attempts during user logon); 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 (including unsuccessful requests for confidential and security-relevant information, Uninterruptible Power Supply failure, or violations of certification practice statements).

Requirements applied to ECA equipment:

The ECA equipment shall record server installation, access, and modification (including installation of the operating system, installation of the CA, system startup, installation/removal of hardware cryptographic modules, attempts to set/modify passwords, resetting of operating system clock and changes in configuration files, security profiles, administrator privileges, audit parameters, the value of maximum authentication attempts, type of authenticator, hardware configuration, software configuration, operating system configuration, and installation of patches).

The following ECA operations shall be recorded:

- ECA equipment access (including room access and server access);
- File manipulation and account management (including attempts to delete or modify audit logs; an Administrator unlocking an account that has been locked as a result of unsuccessful authentication attempts; all security-relevant data that is entered in the system; addition, deletion, or access control modification of role and user accounts);
- Changing the time on the CA;
- Posting of any material to a repository;
- Access to ECA databases (including access to certificate subject private keys retained within the ECA for key recovery and backing up/restoring CA internal database); and,
- Any use of the ECA signing key.

Requirements applied to Keyed CSA equipment:

The CSA equipment that sign responses (e.g., OCSP responses or SCVP responses) shall record server installation, access, and modification (including installation of the operating system, installation of the CA, system startup, installation/removal of hardware cryptographic modules, attempts to set/modify passwords, resetting of operating system clock and changes in configuration files, security profiles, administrator privileges, audit parameters, the value of maximum authentication attempts, type of authenticator, hardware configuration, software configuration, operating system configuration, and installation of patches).

The following events shall also be recorded:

- CSA equipment access (including room access and server access); and,
- File manipulation and account management (including attempts to delete or modify audit logs; an Administrator unlocking an account that has been locked as a result of unsuccessful authentication attempts; all security-relevant data that is entered in the system; addition, deletion, or modification of role and user accounts).

Requirements applied to CMS equipment:

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

- CMS application access (including logon and any attempts to assume a role);
- Messages received from any source regarding CMS actions;
- Actions taken in response to requests for CMS actions;
- Physical CMS equipment access (including room access and server access);

- Physical access to, loading, zeroizing, transferring keys to or from, backing-up, acquiring, or destroying CMS cryptographic modules; and,
- File manipulation and account management (including attempts to delete or modify audit logs; an Administrator unlocking an account that has been locked as a result of unsuccessful authentication attempts; all security-relevant data that is entered in the system; addition, deletion, or access control modification of role and user accounts).

Requirements applied to humans and physical operations:
The following events will be audited:

- Appointment of CMA or CMS personnel (including designation of personnel for multiparty control);
- Training of CMA or CMS personnel; and,
- Physical access to the ECA equipment.

For each auditable event, the CMA or CMS 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 5.4.3, and made available during compliance audits.

5.4.2 Frequency of Processing Log

Audit logs shall be reviewed at least once every two months.

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

The CMA or CMS shall explain all significant events in an audit log summary. Actions taken as a result of these reviews shall be documented. Audit summaries documenting significant events and resulting actions shall be provided to the EPMA.

5.4.3 Retention Period of Audit Log

The information generated on the CMA, CSA, or CMS equipment shall be kept on the equipment until the information is moved to an appropriate archive facility. Deletion of the security audit data from the equipment shall be performed by an entity other than the CMA. This entity shall be identified in the appropriate CPS. Audit logs shall be retained on-site until reviewed, then off-site as archive records in accordance with Section 5.5.2.

5.4.4 Protection of Audit Log

The security audit data, once generated, shall not be open for modification by any human, or by any automated process. The security audit data shall not be open for reading by any human, or by any automated process other than those that perform security audit processing. CMA, CSA and CMS 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, CSA, or CMS equipment.

5.4.5 Audit Log 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.

5.4.6 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 or CMS. 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 or CMS shall cease all operation except for revocation processing until the security audit capability can be restored. Under these circumstances, the CMA or CMS shall employ mechanisms to preclude unauthorized CMA or CMS functions. These mechanisms shall be described in the CPS.

5.4.7 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.

5.4.8 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.

5.5 RECORDS ARCHIVAL

In the case where CMA equipment operates in a VME, requirements in this section and subsections apply to both the host and the hypervisor event logs.

5.5.1 Types of Records 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 issuance, revocation, suspension, restoration and key recovery requests;
- Key recovery requestor identity authentication documentation as required by Section 3.5;
- Documentation of authority of the requestor, receipt and acceptance of recovered keys as required by Section 4.12.2;
- Escrowed keys;
- Certificate status requests and responses;
- Subscriber identity authentication documentation as required by Section 3.2.3.1;

- Documentation of receipt and acceptance of certificates as described in Section 4.4;
- Documentation of receipt of tokens as described in Section 6.1.2;
- All certificates and CRLs (or other revocation information) as issued or published;
- Security audit data (in accordance with Section 5.4);
- Other data or applications sufficient to verify archive contents; and,
- All work related communications to or from the EPMA, other CMAs, and compliance auditors.

At a minimum, the following CMS data shall be archived:

- CMS accreditation (if necessary);
- Any contractual agreements to which the CMS is bound;
- System equipment configuration, including modifications or updates;
- Security audit data (in accordance with Section 5.4);
- Other data or applications sufficient to verify archive contents; and
- All work related communications to or from the EPMA, other CMAs, and compliance auditors.

5.5.2 Retention Period of 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, the 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.

5.5.3 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 or CMS applied signatures. The ECA 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 9.4.4.

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 or CMS name, the date, and sensitivity.

5.5.4 Archive Backup Procedures

If archive data is backed up, the procedures shall be sufficient to ensure that the integrity of the archive data is not compromised and the backup copies shall be protected as specified in Section 5.5.3. Procedures shall be specified in the CPS.

5.5.5 Requirements for Time-Stamping of Records

CA and CMS archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6 Archive Collection System (Internal vs. External)

Archive data may be collected in any expedient manner.

5.5.7 Procedures to Obtain and Verify 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 individuals shall be allowed to access the archive.

5.6 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 4.7) 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 *Internet X.509 Public Key Infrastructure Certificate Management Protocol* [RFC 4210].

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 certificate lifetimes are as described for Subscribers in Section 4.7. Note that CA signature keys that have expired for the purposes of certificate signing may still be used for CRL signing and OCSP Responder certificate signing. All values are in years.

	CA	Root CA
All Assurance Levels	6/3	26/20

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

If a hacking attempt or other form of potential compromise of a CA becomes known, it shall be investigated in order to determine the nature and the degree of damage. If the CA key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed. Otherwise the scope of potential damage shall be assessed in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised.

In case of a CSA key compromise, all certificates issued to the CSA shall be revoked and the revocation information shall be published immediately in the most expeditious manner. Subsequently, the CSA shall be re-keyed.

The CMS that supports PIV-I credential issuance shall have documented incident handling procedures which have been approved by the head of the organization operating the CMS.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

The CA shall maintain backup copies of system, databases, and CA private keys in order to rebuild the CA capability in case of software and/or data corruption.

5.7.3 Entity Private Key Compromise Procedures

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 Section 5.7.4. 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.

In case of a RA key compromise, the CA that issued the RA a certificate shall revoke that RA's certificate, and the revocation information shall be published immediately in the most expedient manner. The compromise shall be investigated in order to determine the actual or potential date of the RA key compromise. All certificates approved by that RA since the date of actual or potential date of the RA key compromise shall be either revoked summarily, or their legitimacy ascertained and otherwise revoked.

In the case of a CMS compromise, any CA that issued the CMS a certificate, including any Content Signing certificates, shall immediately revoke those CMS certificates, and the revocation information shall be published immediately in the most expedient manner. The CMS shall be re-established with new certificates. Subsequently, all PIV-I cards containing content signed using the compromised key shall be recalled and the data resigned using the new key. Any cards that cannot be recalled shall be revoked, and all certificate associated with those cards shall be revoked.

The CA governing body shall also investigate and report to the EPMA what caused the compromise or loss, and what measures have been taken to preclude recurrence.

5.7.4 Business Continuity Capabilities After a Disaster

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.

5.8 CA OR RA TERMINATION

ECA termination will be handled in accordance with Section 5.7. 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 5.7.1.

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.

In the event of a CMS termination, if all copies of private keys associated with Content Signing certificates used by that CMS are either maintained in protected environment or destroyed with verification of their destruction,

Content Signing certificates do not need to be revoked. However, if the secure environment of Content Signing private keys is not maintained prior to their destruction or expiration of the associated certificates, then the termination shall be treated as a compromise and the procedures identified in Section 5.7.3 for CMS compromise shall be followed.

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, an 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 keys shall be generated in *Security Requirements for Cryptographic Modules* [FIPS140-2] (current version) Level 3 validated cryptographic hardware modules in accordance with the *Digital Signature Standard* [FIPS186-4].

CSA certificate status response signing keys shall be generated in [FIPS140-2] Level 2 validated cryptographic hardware modules in accordance with [FIPS186-4].

Medium Token, Medium Hardware, and Medium Hardware PIV-I assurance encryption key pairs may be generated off the token as long as they are generated on a [FIPS140-2] Level 2 or higher hardware cryptographic module and 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 Token, Medium Hardware, and Medium Hardware PIV-I assurance signature key pairs and Medium Hardware PIV-I card authentication key pairs shall be generated on the subscriber token.

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

CA and CSA key pair shall be generated under two person control. CA and CSA key pair generation shall create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used. The key pair generation process shall be validated by an independent third party by witnessing the key generation or by examining the signed and documented record of the key generation.

Content Signing PIV-I keys, CMS Master keys, and diversified keys shall be generated in a [FIPS140-2] Level 2 or higher hardware cryptographic module.

Medium Assurance key pairs shall be generated in a [FIPS140-2] Level 1 validated cryptographic modules.

6.1.2 Private Key Delivery 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, and that the token is not activated prior to receipt by the proper Subscriber. 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

Personal Identification Number (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 encryption certificates recovered from the KES shall be transmitted or delivered to the requestor encrypted using a method that provides protection commensurate with the strength of the private key being protected and the delivery shall be accomplished in a way that ensures that the recovered key is only provided to the correct requestor. The CMA must maintain a record of receipt of the recovered key by the requestor. When any mechanism that includes a shared secret (e.g., a password) is used to protect the key in transit, the mechanism shall ensure that the requestor and the transmitting CMA are the only holder of this shared secret.

Only those authorized by the ECA's Key Recovery Practice Statement (KRPS) may access private keys associated with encryption certificates.

6.1.3 Public Key Delivery 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.

6.1.4 CA Public Key Delivery to Relying Parties

The ECA Root CA, ECAs, RAs, and Subscribers shall work together to ensure the authenticated and integral delivery of the Root CA certificate (also called a "Trusted Certificate") to them. The Root CA CPS shall describe how the Root CA certificate is provided to the ECAs. The ECA CPS shall describe how the Root CA certificate is provided to the RAs and Subscribers. 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.

6.1.5 Key Sizes

All ECA keys shall be at least 2048 bit RSA or at least 256 bit Elliptic Curve DSA (ECDSA).

CAs that do not issue certificates or possess certificates asserting the Medium SHA-256, Medium Token SHA-256, Medium Hardware SHA-256, or any of the PIV-I OIDs shall use SHA-1 or stronger hash algorithm when generating digital signatures on certificates, CRLs, and OCSP responses.

CAs issuing certificates or possessing certificates with Medium SHA-256, Medium Token SHA-256, Medium Device SHA-256, Medium Hardware SHA-256, or any of the PIV-I OIDs shall use the SHA-256 hash algorithm when generating digital signatures on certificates, CRLs, and OCSP responses.

CSAs shall sign responses using the same signature algorithm, key size, and hash algorithm as used by the CA to sign CRLs. CSAs that are authoritative for status of certificates with Medium SHA-256, Medium Token SHA-256, Medium Device SHA-256, Medium Hardware SHA-256, or any of the PIV-I OIDs shall sign all responses using the SHA 256 hash algorithm.

CMSs shall sign content using the SHA-256 hash algorithm.

Use of Transport Layer Security (TLS) protocol or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum three key, triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys through 30 June 2011. Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for the symmetric key, at least 2048 bit RSA or equivalent for the asymmetric keys, and SHA-256 (if commercially available as part of TLS) after 30 June 2011. In addition, cryptographic protocols such as TLS, CMS, S/MIME shall use cipher suite at least as strong as any keys transported using the protocol.

6.1.6 Public Key Parameters Generation and Quality Checking

The requirements in this section shall apply to all entities generating key pairs whose public components are to be certified by the ECA. All key pairs, including the prime numbers shall be generated in accordance with [FIPS186-3], including primality tests. RSA public exponent shall be in the range specified in [FIPS186-4], e.g., public exponent shall be at least $2^{16} + 1$.

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

The use of a specific key is determined by the key usage extension in the X.509 certificate. A certificate to be used for signing or authentication asserts a key usage of Digital Signature. A certificate that is to be used for encryption asserts a key usage of Key Encipherment or Key Agreement.

Except as stated below, public keys that are bound into certificates shall be certified for use in signing or encrypting, but not both. Some applications are not able to use separate signing and encryption certificates, either because of the application design or because the certificate will be used with a protocol such as TLS that provides authenticated connections using encryption certificates. To support these applications, a CA may issue certificates to components that support both signing and encryption.

Certificates that are used for encryption shall not assert a key usage of non-repudiation. Certificates that are used only for signing or authentication may assert a key usage of non-repudiation.

Content Signing PIV-I certificates shall include an extended key usage of *id-fpki-pivi-content-signing* as described in the certificate profile in Section 10.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is [FIPS140-2]. Cryptographic modules shall be validated to the [FIPS140-2] levels identified in this section.

For Medium assurance certificates, subscribers shall use cryptographic modules that have been validated to meet at least the criteria specified for [FIPS140-2] 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.

For Medium Token and Medium Hardware assurance certificates, subscribers shall use hardware cryptographic modules that have been validated to meet at least the criteria specified for [FIPS140-2] Level 2. 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.

For PIV-I certificates, PIV-I Cards shall only be issued using card stock that has been tested and approved by the *Personal Identity Verification (PIV) of Federal Employees and Contractors* [FIPS201-2] Evaluation Program and listed on the GSA Approved Products List (APL). Card stock that has been removed from the APL may continue to be issued for no more than one year after GSA approved replacement card stock is available. PIV-I cards issued using the deprecated card stock may continue to be used until the current subscriber certificates expire, unless otherwise notified by the Federal PKI Policy Authority. On an annual basis, for each PIV Card

Issuer configuration used (as defined by the [FIPS 201-2] Evaluation Program), one populated, representative sample PIV-I Card shall be submitted to the [FIPS201-2] Evaluation Program for testing. In addition, hardware tokens shall meet all requirements specified in Section 12.

Content Signing keys and CMS Master Keys shall be contained in hardware tokens that have been validated to meet at least the criteria specified for [FIPS140-2] Level 2. Card Diversified Keys shall be protected by hardware tokens that have been validated to meet at least the criteria specified for [FIPS140-2] Level 2. Keys shall be protected from unauthorized disclosure and distribution. Card management shall be configured such that only the authorized CMS can manage issued cards.

Certificates shall be signed using a hardware cryptographic module that has been validated to meet [FIPS140-2] Level 3.

CSAs and RAs shall use hardware cryptographic modules that have been validated to meet [FIPS140-2] 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.

When a single cryptographic module has the private keys of more than one entity, the private keys shall be protected in a cryptographic module validated at [FIPS140-2] Level 2 hardware or higher. When a single cryptographic module is controlled by a single entity and has multiple private keys for certificates of different types or with different DNs that have been issued to or provided to that entity by the PKI, this requirement shall not apply.

No one shall have access to a private signing key but the Subscriber. Private encryption keys shall only be held by the Subscriber or and parties authorized to request recovery as specified in Section 4.12.2.2. Key recovery requestors shall protect recovered keys as described in Section 4.12.2.3.

Section 6.1.1 stipulates cryptographic module requirements for key generation.

Medium Assurance	**Subscriber**	**RA and CSA**	**CA**
FIPS 140-2 validation	Level 1	Level 2 (hardware)	Level 3 (hardware)
Operational requirement	Shall not output private asymmetric key in plaintext		

Medium Token, Medium Hardware, Medium Hardware PIV-I Card Authentication, and Content Signing Assurance	**Subscriber**	**RA, CSA, and CMS**	**CA**
FIPS 140-2 validation	Level 2 Hardware	Level 2 (hardware)	Level 3 (hardware)
Operational requirement	Shall not output private asymmetric key in plaintext		

6.2.2 Private Key (n out of m) Multi-Person Control

A single person shall not be permitted to activate the ECA, CSA, or Content Signing PIV-I signature key, activate the CMS Master Key, or access any cryptographic module containing the complete ECA or CSA private signing key. Access to ECA and CSA signing keys backed up for disaster recovery shall be under the same multi-person control as the original ECA and CSA signing key.

Private encryption keys requested by anyone 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.

Access to an escrowed private key as part of key recovery and subsequent delivery to a third-party requestor shall be under two-person control.

6.2.3 Private Key Escrow

CA private keys shall not be escrowed.

The private key associated with any certificate that asserts a key usage of digital signature or non-repudiation shall not be escrowed.

For some purposes (such as data recovery) it may 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 the ECA CPS.

6.2.4 Private Key Backup

For Medium Token, Medium Hardware, Medium Hardware PIV-I, and Card Authentication PIV-I Subscriber private signature keys may not be backed up or copied.

For Medium assurance only, subscribers are permitted to back-up their own encryption (but not signature) private keys. The backup private keys shall be stored on a removable media and shall not be kept online.

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. However, private keys stored in each of these applications or locations must be in cryptographic modules that have been validated at [FIPS140-2] Level 1 and must be held in the Subscriber's control.

For Medium and Medium Device SHA-256 assurance only, component PKI Sponsors (see Section 1.3.7.2) 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. The backup private key shall be stored on a removable media and shall not be kept online.

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 and CSA private signature keys and CMS Master Keys may be backed up under the same multi-person control as the original signature key. If such a backup is made, only a single copy is to be kept at the primary location; a second copy may be kept at a backup location. No more than two backup copies shall be made. The backup module shall also meet the cryptographic module requirements for the CA, the CSA, or CMS.

6.2.5 Private Key Archival

See Sections 6.2.3 and 6.2.4.

6.2.6 Private Key Transfer Into or From a 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.

Card Master Keys and Diversified Keys shall be protected from disclosure. They shall not be exposed outside of the CMS HSM and, for Diversified keys only, the PIV-I smart card associated with that key.

6.2.7 Private Key Storage on Cryptographic Module

The private key stored in the cryptographic module shall be protected from unauthorized access and use in accordance with the [FIPS140-2] requirements applicable for the module.

6.2.8 Method of Activating Private Key

Except for Card Authentication PIV-I and Medium Device SHA-256 certificates, passwords, 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 Section 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).

6.2.9 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.

6.2.10 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.

6.2.11 Cryptographic Module Rating

Requirements for cryptographic modules are as stated above in Section 6.2.1.

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 Certificate Operational Periods and Key Pair Usage Periods

The key usage periods for keying material are described in Sections 4.7 and 5.6.

6.3.3 Subscriber Private Key Usage Environment

The subscribers shall use their private keys only on the machines that are protected and managed using commercial best practices.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

A password, 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 password or PIN shall be generated in conformance with [FIPS140-2].

Subscriber (to include CMA and CMS) PINs, when used, shall be 6-8 digits at a minimum. Randomly generated PINs shall be used when possible. If this is not possible, Subscribers who create their own PINs shall be instructed to select PINs that are not related to their personal identity, history, or environment. Sequences, repeated numbers, social security numbers, and date formats, or other easily guessed numbers shall not be

used. When alphanumeric pass-phrases are used, an interspersed mix of 8 characters, including at least two interspersed digits, shall be used. The activation data shall not resemble dictionary words; they shall differ from words or names by at least two characters that are not simple number-for-letter substitutions and shall not consist of words or names followed by 1-4 digits. The activation data shall not contain sequences, repeated characters, date formats, or license plate formats. To the extent practicable, technical means shall be used to verify that the activation data meets all of the requirements in this section.

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. Activation data for keys associated with CSA and CMS shall be restricted to authorized CSA and CMS operations staff.

Activation data protection for the CA shall include a capability to temporarily lock the account, or terminate the application, after a predetermined number of failed logon attempts as set forth in the CPS.

6.4.3 Other Aspects of Activation Data

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

For Medium Hardware PIV-I certificates, in the event activation data must be reset, a successful biometric 1:1 match of the applicant against the biometrics collected in Section 3.2.3.1 is required. This biometric 1:1 match shall be conducted by a CMA or trusted agent of the issuer.

Where a single cryptographic module has the private keys of more than one entity, remote activation shall require authentication commensurate with the assurance level of the certificate of the key being activated.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

CA, CSA, and CMS equipment shall use operating systems that:

- Require authenticated logins;
- Provide discretionary access control;
- Provide a security audit capability;
- Provide operating system self-protection;
- Provide process isolation; and,
- Support recovery from key or system failure.

When CA, CSA, and CMS 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 that received the evaluation rating.

For CMA equipment operated in a VME, the requirements above shall be applied to the hypervisor where applicable.

6.5.2 Computer Security Rating

No Stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

CAs shall be developed using the following system development controls:

- For commercial off-the-shelf software, the software shall be designed and developed under a formal, documented development methodology.
- For hardware and software developed specifically for a particular CA, the applicant shall demonstrate that security requirements were achieved through a combination of software verification & validation, structured development approach, and controlled development environment.
- Where open source software has been utilized, the applicant shall demonstrate that security requirements were achieved through software verification & validation and structured development/life-cycle management.
- Hardware and software procured to operate the CA shall be purchased and shipped in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- The CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications; hardware devices, network connections, or component software installed which are not part of the CA operation.
- Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Hardware and software shall be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

CMA and CMS software, when first loaded, shall be verified as being that supplied by the vendor, with no modifications, and be the version intended for use. CMSs shall operate on machines dedicated to the issuance of PIV-I cards. A formal configuration management methodology shall be used for installation and ongoing maintenance of the CMS. Any modifications and upgrades to the CMS shall be documented and controlled. There shall be a mechanism that is installed and operating for detecting unauthorized modification to the CMS.

CA and CSA equipment, including the hypervisor and the underlying hardware in a VME, 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.

6.6.3 Life Cycle Security 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 refraining from identifying intended use on order forms/paperwork or randomly selecting from existing inventory.

All hardware and software that has been identified as supporting a CMA or CMS 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 or CMS function to the using facility.

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

For All Assurance Levels	Purchase in manner to reduce likelihood of tampering, or develop in controlled environment Protective packaging, accountable delivery method

6.7 NETWORK SECURITY CONTROLS

CMA and CMS 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, CSA, and CMS equipment shall be limited to those required to perform CMA functions. Other CMA, CSA, or CMS equipment may enable additional services consistent with local policy.

Protection of CMA, CSA, or CMS 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, CSA, or CMS equipment shall be necessary to the functioning of the CMA, CSA, or CMS application. Root CA equipment shall be stand-alone (off-line) configurations.

Boundary control devices shall be used to protect the network on which PKI equipment is hosted and 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 contain the following security features:

- Audit of security events;
- Protection of security audit log;
- Identification & Authentication with Secure action upon authentication failure;
- If data is communicated with Intrusion Detection System (IDS) components, confidentiality and integrity of this data;
- Non by-passable and self-protection; and,
- Ability to filter packets based on source, destination and port number.

The ECA vendor shall use a firewall that has successfully undergone Common Criteria evaluation against a NIAP-approved Protection Profile by a NIAP recognized scheme.

The boundary shall also be protected by an IDS that provides the following security features:

- Audit of security events;
- Protection of security audit log;
- Identification & Authentication with Secure action upon authentication failure;
- Confidentiality and integrity of data communicated among the IDS and other components;
- Non by-passable and self-protection;
- Ability to collect security relevant events;

- Ability to process and output security relevant events in human readable form; and,
- Ability to protect security relevant events against unauthorized access, modification or deletion.

The ECA vendor shall use an IDS that has been successfully undergone Common Criteria evaluation against a NIAP-approved Protection Profile by a NIAP recognized scheme, the vendor shall use such an IDS.

The EPMA may approve alternate boundary protection (i.e., firewalls and IDS) products.

6.8 TIME STAMPING

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events (see Section 5.4.1).

7 CERTIFICATE, CRL, AND OCSP PROFILES

Section 10 contains the formats for the various certificates and CRLs.

7.1 CERTIFICATE PROFILE

7.1.1 Version Number(s)

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 in accordance with *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* [RFC 5280], and approved by the EPMA, and documented in the associated CPS. Whenever private extensions are used, they shall be identified in the CPS. No CA certificates may include critical private extensions. In addition, any variance that would impact interoperability shall not be approved.

End-Entity certificates shall always contain the Extended Key Usage extension and that extension shall not contain the *anyExtendedKeyUsage* {2.5.29.37.0} OID. Extended Key Usage OIDs shall be consistent with key usage bits asserted.

End-Entity certificates shall only contain Key Usage and Extended Key Usage that are intended for the certificate and shall not contain any other Key Usage or Extended Key Usage.

7.1.3 Algorithm Object Identifiers

Certificates under this Policy shall use the following OIDs for signatures:

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2}
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3}
ecdsa-with-SHA512	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4}

Certificates under this Policy shall use the following OIDs for identifying the algorithm for which the subject key was generated:

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public key-type (2) 1}
id-ecDH	{iso(1) identified-organization(3) certicom(132) schemes(1) ecdh(12)}

For certificates that contain an elliptic curve public key, the parameters shall be specified as one of the following named curves. In order to provide cryptographic separation for a closed community, when the subject public key is of the form id-ecDH, a private OID may be asserted to indicate a different base point on one of these curves:

ansip256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}
ansip384r1	{iso(1) identified-organization(3) certicom(132) curve(0) 34}
ansip521r1	{iso(1) identified-organization(3) certicom(132) curve(0) 35}

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 *Information Technology – Open Systems Interconnection – The Directory: Authentication Framework* (Part 8: Public-key and attribute certificate frameworks) [ISO9594-8] may be used, in accordance with the required profile (see Section 7.1.2).

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

For attribute values other than domain component: All CA Distinguished Names (in various fields, e.g., Issuer, Subject, Subject Alternative Name, Name constraints) shall be encoded as printable strings. All subscriber DN portions that name constraints apply to shall be encoded as printable string. Other portions of the subscriber DN shall be encoded as printable strings, if possible. If a portion cannot be encoded as a printable string, then and only then shall it be encoded using a different format and that format shall be UTF8.

For domain component attribute values: All domain component attribute values shall be encoded as an IA5 string.

7.1.5 Name Constraints

Not Applicable.

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

Not Present.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this policy may contain the following policy qualifiers: .user notice and CP/CPS pointer.

7.1.9 Processing Semantics for the Critical Certificate Policies 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.

7.1.10 Inhibit Any Policy Extention

Not Present.

7.2 CRL PROFILE

7.2.1 Version Number(s)

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 described in Section 10. Any variance to these profiles shall be approved by the EPMA and documented in a CPS.

7.3 OCSP PROFILE

Section 10 contains the format (profile) for OCSP requests and responses.

7.3.1 Version Number(s)

See OCSP request and response profiles in Section 10.

7.3.2 OCSP Extensions

See OCSP request and response profiles in Section 10.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT

All CAs shall conduct an annual compliance audit; the scope of audits shall include its CMAs. 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.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

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.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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.

8.4 TOPICS COVERED BY ASSESSMENT

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, as well as any MOAs between the ECA PKI and any other PKI.

8.5 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 8.6 of the discrepancy; and,
- The CMA shall 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.

8.6 COMMUNICATIONS OF RESULTS

The compliance auditor shall report the results of a compliance audit to the EPMA. The results shall 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.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

Subscription fees to be paid by Subscribers may be published or established contractually by ECAs.

9.1.2 Certificate Access Fees

ECAs shall make current certificates information available to Relying Parties at no charge.

9.1.3 Revocation or Status Information Access Fees

ECAs shall make current revocation information (including but not limited to CRL and OCSP responses) available to Relying Parties at no charge.

9.1.4 Fees for Other Services

ECAs may charge fees to Relying Parties for providing archived certificates and archived revocation information.

9.1.5 Refund Policy

No Stipulation.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

No Stipulation.

9.2.2 Other Assets

No Stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No Stipulation.

9.2.4 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.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Business Confidential Information

Not applicable. The ECA shall not collect business confidential information.

9.3.2 Information Not Within the Scope of Business Confidential Information

Not applicable. The ECA shall not collect business confidential information.

9.3.3 Responsibility to Protect Business Confidential Information

Not applicable. The ECA shall not collect business confidential information.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

All Subscriber identifying information shall be protected. All Subscriber identifying information shall be maintained in accordance with applicable laws.

9.4.2 Information Treated as Private

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 9.4.4.

9.4.3 Information Not Deemed Private

A certificate should only contain information that is relevant and necessary to effect secure transactions with the certificate. Thus, information in a certificate is not considered private or privacy act information.

9.4.4 Responsibility to Protect Private Information

A CA shall not disclose any personal information collected to meet the requirements of this Policy (e.g., certificate related, background check) to any third party unless authorized by this Policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. The CA shall authenticate any request for release of information. This does not prevent the CA from disclosing the certificate and certificate status information (e.g., CRL, OCSP requests and responses).

9.4.5 Notice and Consent to Use Private Information

All notices shall be in accordance with the applicable laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

All disclosure shall be in accordance with applicable laws.

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 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 the subscribers and their organizations. This stipulation, however, shall not prevent ECA from offering key escrow services for private encryption keys.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

A CA who issues certificates that assert a policy OID 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 9.6.3, 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 9.6.6.2, 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 8.5.

9.6.2 RA Representations and Warranties

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.

9.6.3 Subscriber Representations and Warranties

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;
- Use their private keys only on the machines that are protected and managed using commercial best practices;
- 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;
- Notify, in a timely manner, the CMA that issued their certificates of any changes to the information contained in their certificates; 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 1.3.7.2) assume the obligations of Subscribers for the certificates associated with their components.

9.6.4 Relying Party Representations and Warranties

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);
- Establish trust in the certificate using certification path validation procedures described in [RFC 5280], prior to reliance; and,
- 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.

9.6.5 Representations and Warranties of Affiliated Organizations

Affiliated Organizations shall authorize the affiliation of subscribers with that organization, and shall immediately inform the ECA of any severance of affiliation with any currently affiliated subscriber.

9.6.6 Representations and Warranties of Other Participants

9.6.6.1 ECA Representations and 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.

9.6.6.2 Repository Representations and Warranties

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 2.4.

9.6.6.3 Trusted Agent Representations and Warranties

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.

9.6.6.4 CSA Representations and Warranties

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 8.5.

9.6.6.5 PKI Point of Contact Representations and Warranties

An ECA Subscriber organization may appoint a PKI POC to provide a single trusted point of contact with the ECA vendors. The PKI POC shall comply with the stipulations of this policy and comply with a CPS approved by the EPMA for use with this policy. The PKI POC may request revocation of certificates issued to the Subscribers

within the POC organization. The PKI POC may receive Subscriber hardware tokens for zeroization and/or destruction.

A PKI POC who is found to have acted in a manner inconsistent with the stipulations of this CP and the associated ECA vendor's CPS is subject to removal as PKI POC. Failure to address the deficiencies of the PKI POC may result in revocation of any or all certificates issued to the Subscriber organization.

9.7 DISCLAIMERS OF WARRANTIES

Other than the warranties included in Section 9.6.6.1, 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.

9.8 LIMITATIONS OF LIABILITY

9.8.1 Loss Limitation

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 or improper use of a recovered key, if the certificate was issued in accordance with this CP and the ECA's CPS.

9.8.2 Other Exclusions

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

9.8.3 U.S. Federal Government Liability

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

9.9 INDEMNITIES

Agents of an ECA (e.g., RA, Trusted Agents) assume no financial responsibility for improperly used certificates or improper use of a recovered key by the Subscriber or a third party requestor.

9.10 TERM AND TERMINATION

9.10.1 Term

This CP shall remain in effect until either a new ECA CP is approved by the PMA or the ECA PKI is terminated.

9.10.2 Termination

This CP shall survive any termination of the CA. The requirements of this CP remain in effect through the end of the archive period for the last certificate issued.

9.10.3 Effect of Termination and Survival

The responsibilities for protecting business confidential and personal information, and for protecting the Government's intellectual property rights shall survive termination of this CP.

Intellectual property rights shall survive this CP in accordance with the IP laws of the United States.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

All parties shall use commercially reasonable methods to communicate with each other.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

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 1.5.2. 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 9.12.2) 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.

9.12.2 Notification Mechanism and Period

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

The EPMA shall 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.

9.12.3 Circumstances Under Which OID Must be Changed

The policy OID shall only change if the change in the CP results in a material change to the trust by the relying parties.

9.13 DISPUTE RESOLUTION PROVISIONS

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

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.

9.14 GOVERNING LAW

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

9.15 COMPLIANCE WITH APPLICABLE LAW

No stipulation.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

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 9.12. Responsibilities, requirements, and privileges of this document are merged to the newer edition upon release of that newer edition.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.

10 CERTIFICATE AND CRL FORMATS

When used as URI, Universally Unique Identifier (UUID) used in certificates shall conform to *A UUID URN Namespace* [RFC 4122] requirement. When used as a Serial Number attribute, the UUID shall be encoded using the UUID string representation defined in Section 3 of RFC 4122 (e.g., "f81d4fae-7dec-11d0-a765-00a0c91e6bf6"). Since UUID is associated with a PIV-I card, when used, the same UUID shall be asserted in all applicable certificates and in all applicable other signed objects on a PIV-I card.

None of the certificates (including Root CAs), CRL or OCSP Responses that are valid beyond 31 December 2030 shall be signed using or contain 2048 bit or lower security RSA keys.

10.1 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} or sha256WithRSAEncryption
Issuer Distinguished Name	cn=ECA Root CA[9], ou=ECA, o=U.S. Government, c=US
Validity Period	26 years or less from date of issue in Generalized Time format[10]
Subject Distinguished Name	Same as the Issuer Distinguished Name
Subject Public Key Information	2048 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} or sha256WithRSAEncryption
Extensions	
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	Not Present
Subject Information Access	c=no; optional, access method=caRepository (1.3.6.1.5.5.7.48.5), pointer to CA certificates issued.
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

The following fields are different for the ECA Root ECDSA certificate:

Field	Value
Issuer Signature Algorithm	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}

[9] The Common Name may optionally include generation/version number.

[10] The first ECA Root certificate issued on June 14, 2004 has a 36 year validity period stated in the self-signed certificate, but the private key shall not be used to issue certificates beyond June 13, 2024. The relying parties shall be instructed to delete this root prior to June 13, 2030.

Field	Value
Subject Public Key Information	Algorithm OID: ecPublicKey {1 2 840 10045 2 1} Parameters: namedCurve P-256 {1 2 840 10045 3 1 7} SubjectPublic Key: Uncompressed EC Point
Issuer's Signature	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}

10.2 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} or sha256WithRSAEncryption
Issuer Distinguished Name	cn=ECA Root CA[11], ou=ECA, o=U.S. Government, c=US
Validity Period	6 years or less from date of issue in UTCT format
Subject Distinguished Name	cn=<ECA CA name>, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 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} or sha256WithRSAEncryption
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
Inhibit Any Policy	Not Present
Private key usage period	Not Present
Certificate policies	c=no; one or more of certificate policy OIDs from Section 1.2 as appropriate
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
Policy Constraints	Not Present
Name Constraints	Not Present[12]
Authority Information Access	c=no; pointer to ECA Root certificate (optional); pointer to OCSP Responder (optional)
CRL Distribution Points[13]	c=no; always present

The following fields are different for the Subordinate CA ECDSA certificate:

Field	Value

[11] The Common Name may optionally include generation/version number.

[12] This is a temporary change because technical mechanisms do not currently exist across all applications used by subscribers and relying parties to implement the Name Constraints extension for distinguished names in accordance with the X.509 standard. This change is in effect until October 2008.

[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).

Field	Value
Issuer Signature Algorithm	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Subject Public Key Information	Algorithm OID: ecPublicKey {1 2 840 10045 2 1} Parameters: namedCurve P-256 {1 2 840 10045 3 1 7} SubjectPublic Key: Uncompressed EC Point
Issuer's Signature	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}

10.3 SIGNATURE CERTIFICATE

Field	Signature Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption
Issuer Distinguished Name	cn=<ECA CA name>, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	3 years or less from date of issue
Subject Distinguished Name	cn=<Subscriber Name>, ou=<Subscriber Company Name > | unaffiliated, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption or sha256WithRSAEncryption
Extensions	
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=no; mandatory. Shall contain a minimum of one key purpose OID consistent with intended usage. Shall not contain *anyExtendedKeyUsage* {2.5.29.37.0}
Private key usage period	Not Present
Certificate policies	c=no; one or more of certificate policy OIDs from Section 1.2 as appropriate
Policy Mapping	Not Present
subject Alternative Name	c=no; always present, contains RFC822 email address
Issuer Alternative Name	Not Present
Subject Directory Attributes	c=no; {id-pda-countryOfCitizenship AttributeType :: {1 3 6 1 5 5 7 9 4}[16] CountryOfCitizenship ::= PrintableString (SIZE (2) -- ISO 3166 Country Code}
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	c=no; pointer to ECA certificate (required); pointer to OCSP Responder (required)
CRL Distribution Points[17]	c=no; always present

The following fields are different for the Signature ECDSA certificate:

[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 system shall be capable of asserting multiple citizenships using the CountryOfCitizenship OID multiple times.

[17] 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).

Field	Value
Issuer Signature Algorithm	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Subject Public Key Information	Algorithm OID: ecPublicKey {1 2 840 10045 2 1} Parameters: namedCurve P-256 {1 2 840 10045 3 1 7} SubjectPublic Key: Uncompressed EC Point
Issuer's Signature	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}

10.4 ENCRYPTION CERTIFICATE

Field	Encryption Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption
Issuer Distinguished Name	cn=<ECA CA name>, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	3 years or less from date of issue
Subject Distinguished Name	cn=<Subscriber Name>, ou=<Subscriber Company Name > | unaffiliated, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption or sha256WithRSAEncryption
Extensions	
authority key identifier[18]	c=no; octet string
subject key identifier[19]	c=no; octet string
key usage	c=yes; keyEncipherment
Extended key usage	c=no; mandatory. Shall contain a minimum of one key purpose OID consistent with intended usage. Shall not contain *anyExtendedKeyUsage* {2.5.29.37.0}
Private key usage period	Not Present
Certificate policies	c=no; one or more of certificate policy OIDs from Section 1.2 as appropriate
Policy Mapping	Not Present
subject Alternative Name	c=no; always present, contains RFC822 email address
Issuer Alternative Name	Not Present
Subject Directory Attributes	c=no; {id-pda-countryOfCitizenship AttributeType ::= {1 3 6 1 5 5 7 9 4}[20] CountryOfCitizenship ::= PrintableString (SIZE (2) -- ISO 3166 Country Code}
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	c=no; pointer to ECA certificate (required); pointer to OCSP Responder (required)
CRL Distribution Points[21]	c=no; always present

The following fields and extensions are different for the Subscriber Encryption EC certificate. Algorithm OID and EKU may be changed based on testing:

[18] 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.

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

[20] The system shall be capable of asserting multiple citizenships using the CountryOfCitizenship OID multiple times.

[21] 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).

Field	Value
Issuer Signature Algorithm	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Subject Public Key Information	Algorithm OID: ecDH {1 3 132 1 12} Parameters: namedCurve P-256 {1 2 840 10045 3 1 7} SubjectPublic Key: Uncompressed EC Point
Issuer's Signature	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Key Usage	c=yes; Required: keyAgreement; Prohibited: All Others
Extended Key Usage	c=yes; Required: Client Authentication {1 3 6 1 5 5 7 3 2} Secure E Mail {1 3 6 1 5 5 7 3 4}

10.5 SUBSCRIBER MEDIUM HARDWARE PIV-I AUTHENTICATION CERTIFICATE

Field	Medium Hardware PIV-I Authentication **Certificate Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption
Issuer Distinguished Name	cn=<ECA CA name>, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	3 years or less from date of issue
Subject Distinguished Name	cn=<Subscriber Name>, ou=<Subscriber Company Name > | unaffiliated, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha256WithRSAEncryption
Extensions	
authority key identifier[22]	c=no; octet string
subject key identifier[23]	c=no; octet string
key usage	c=yes; digitalSignature
Extended key usage	c=no;mandatory. Shall contain a minimum of one key purpose OID consistent with intended usage. Shall not contain *anyExtendedKeyUsage* {2.5.29.37.0}
Private key usage period	Not Present
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 6}
Policy Mapping	Not Present
subject Alternative Name	c=no; always present, contains RFC822 email address; Required: URI[24] urn:uuid:<32 character hex representing 128 bit UUID>
Issuer Alternative Name	Not Present
Subject Directory Attributes	c=no; {id-pda-countryOfCitizenship AttributeType ::= {1 3 6 1 5 5 7 9 4}[25] CountryOfCitizenship ::= PrintableString (SIZE (2) -- ISO 3166 Country Code}
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	c=no; pointer to ECA certificate (required); pointer to OCSP Responder (required)

[22] 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.

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

[24] Note this name form is tagged [6] and encoded as IA5String.

[25] The system shall be capable of asserting multiple citizenships using the CountryOfCitizenship OID multiple times.

Field	Medium Hardware PIV-I Authentication **Certificate Value**
CRL Distribution Points[26]	c=no; always present

The following fields are different for the Medium Hardware PIV-I Authentication ECDSA certificate:

Field	Value
Issuer Signature Algorithm	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Subject Public Key Information	Algorithm OID: ecPublicKey {1 2 840 10045 2 1} Parameters: namedCurve P-256 {1 2 840 10045 3 1 7} SubjectPublic Key: Uncompressed EC Point
Issuer's Signature	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}

10.6 CARD AUTHENTICATION PIV-I CERTIFICATE

Field	Card Authentication PIV-I **Certificate Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption
Issuer Distinguished Name	cn=<ECA CA name>, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	3 years or less from date of issue
Subject Distinguished Name	sn=<GUID>, ou=<Subscriber Company Name > | unaffiliated, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha256WithRSAEncryption
Extensions	
authority key identifier[27]	c=no; octet string
subject key identifier[28]	c=no; octet string
key usage	c=yes; digitalSignature
Extended key usage	c=yes; id-PIV-cardAuth {2.16.840.1.101.3.6.8}
Private key usage period	Not Present
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 7}
Policy Mapping	Not Present
subject Alternative Name	c=no; always present, URI[29] urn:uuid:<32 character hex representing 128 bit UUID>
Issuer Alternative Name	Not Present
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	c=no; pointer to ECA certificate (required); pointer to OCSP Responder (required)
CRL Distribution Points[30]	c=no; always present

[26] 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).

[27] 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.

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

[29] Note this name form is tagged [6] and encoded as IA5String.

The following fields are different for the Card Authentication PIV-I ECDSA certificate:

Field	Value
Issuer Signature Algorithm	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Subject Public Key Information	Algorithm OID: ecPublicKey {1 2 840 10045 2 1} Parameters: namedCurve P-256 {1 2 840 10045 3 1 7} SubjectPublic Key: Uncompressed EC Point
Issuer's Signature	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}

10.7 COMPONENT CERTIFICATE

Field	Component & Web Server Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption
Issuer Distinguished Name	cn=<ECA CA name>, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	3 years or less 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	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption or sha256WithRSAEncryption
Extensions	
authority key identifier[31]	c=no; octet string
subject key identifier[32]	c=no; octet string
key usage	c=yes; keyEncipherment, digitalSignature
Extended key usage	c=no; mandatory. Shall contain a minimum of one key purpose OID consistent with intended usage. Shall not contain *anyExtendedKeyUsage* {2.5.29.37.0}
Private key usage period	Not Present
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 9}, may also contain one or more other certificate policy OIDs from Section 1.2 as appropriate except for PIV-I certificate policy OIDs
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; pointer to ECA certificate (required); pointer to OCSP Responder (required)
CRL Distribution Points[33]	c=no; always present

[30] 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).

[31] 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.

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

[33] 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

The following fields and extensions are different for the component EC certificate. Algorithm OID and EKU may be changed based on testing:

Field	Value
Issuer Signature Algorithm	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Subject Public Key Information	Algorithm OID: ecDH {1 3 132 1 12} Parameters: namedCurve P-256 {1 2 840 10045 3 1 7} SubjectPublic Key: Uncompressed EC Point
Issuer's Signature	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Key Usage	c=yes; Required:digitalSignature; Optional keyAgreement; Prohibited: All Others
Extended Key Usage	c=yes; Required: Client Authentication {1 3 6 1 5 5 7 3 2} Server Authentication {1 3 6 1 5 5 7 3 1}

10.8 CODE SIGNING CERTIFICATE

Field	Code Signing Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption
Issuer Distinguished Name	cn=<ECA CA name>, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	3 years or less 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	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption or sha256WithRSAEncryption
Extensions	
authority key identifier[34]	c=no; octet string
subject key identifier[35]	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 2}, {2 16 840 1 101 3 2 1 12 3}, {2 16 840 1 101 3 2 1 12 5}
Policy Mapping	Not Present
subject Alternative Name	always present; c=no; cn=<Name>, ou=<Code Signer Company Name, ou=<ECA Company Name>, ou=ECA, 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; pointer to ECA certificate (required); pointer to OCSP Responder (required)

contain the issuer distribution point extension).

[34] 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.

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

Field	Code Signing Certificate Value
CRL Distribution Points[36]	c=no; always present

The following fields are different for the code signing ECDSA certificate:

Field	Value
Issuer Signature Algorithm	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Subject Public Key Information	Algorithm OID: ecPublicKey {1 2 840 10045 2 1} Parameters: namedCurve P-256 {1 2 840 10045 3 1 7} SubjectPublic Key: Uncompressed EC Point
Issuer's Signature	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}

10.9 GROUP/ROLE SIGNATURE CERTIFICATE

Field	Group/Role Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption
Issuer Distinguished Name	cn=<ECA CA name>, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	3 years or less from date of issue
Subject Distinguished Name	cn=<Group/Role Name >, ou=<Group/Role Company Name >, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption or sha256WithRSAEncryption
Extensions	
authority key identifier[37]	c=no; octet string
subject key identifier[38]	c=no; octet string
key usage	c=yes; digitalSignature, nonRepudiation
Extended key usage	c=no; mandatory. Shall contain a minimum of one key purpose OID consistent with intended usage. Shall not contain *anyExtendedKeyUsage* {2.5.29.37.0}
Private key usage period	Not Present
Certificate policies	c=no; one or more of certificate policy OIDs from Section 1.2 as appropriate except for PIV-I certificate policy OIDs
Policy Mapping	Not Present
subject Alternative Name	always present; c=no; DN of person controlling the private key in the following form cn=<Name>, ou=<Group/Role Company Name, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US ; RFC 822 e-mail address for the Group/Role
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present

[36] 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).

[37] 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.

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

Field	Group/Role Certificate Value
Authority Information Access	c=no; pointer to ECA certificate (required); pointer to OCSP Responder (required)
CRL Distribution Points[39]	c=no; always present

The following fields are different for the Group/Role Signature ECDSA certificate:

Field	Value
Issuer Signature Algorithm	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Subject Public Key Information	Algorithm OID: ecPublicKey {1 2 840 10045 2 1} Parameters: namedCurve P-256 {1 2 840 10045 3 1 7} SubjectPublic Key: Uncompressed EC Point
Issuer's Signature	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}

10.10 GROUP/ROLE ENCRYPTION CERTIFICATE

Field	Group/Role Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption
Issuer Distinguished Name	cn=<ECA CA name>, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	3 years or less from date of issue
Subject Distinguished Name	cn=<Group/Role Name >, ou=<Group/Role Company Name >, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption or sha256WithRSAEncryption
Extensions	
authority key identifier[40]	c=no; octet string
subject key identifier[41]	c=no; octet string
key usage	c=yes; keyEncipherment
Extended key usage	c=no; mandatory. Shall contain a minimum of one key purpose OID consistent with intended usage. Shall not contain *anyExtendedKeyUsage* {2.5.29.37.0}
Private key usage period	Not Present
Certificate policies	c=no; one or more of certificate policy OIDs from Section 1.2 as appropriate except for PIV-I certificate policy OIDs
Policy Mapping	Not Present
subject Alternative Name	always present; c=no; RFC 822 e-mail address for the Group/Role
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present

[39] 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).

[40] 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.

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

Field	Group/Role Certificate Value
Authority Information Access	c=no; pointer to ECA certificate (required); pointer to OCSP Responder (required)
CRL Distribution Points[42]	c=no; always present

The following fields and extensions are different for the Group/Role Encryption EC certificate. Algorithm OID and EKU may be changed based on testing:

Field	Value
Issuer Signature Algorithm	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Subject Public Key Information	Algorithm OID: ecDH {1 3 132 1 12} Parameters: namedCurve P-256 {1 2 840 10045 3 1 7} SubjectPublic Key: Uncompressed EC Point
Issuer's Signature	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Key Usage	c=yes; Required: keyAgreement; Prohibited: All Others
Extended Key Usage	c=yes; Required: Client Authentication {1 3 6 1 5 5 7 3 2} Secure E Mail {1 3 6 1 5 5 7 3 4}

10.11 CONTENT SIGNING PIV-I CERTIFICATE

Field	Medium Hardware PIV-I Authentication **Certificate Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption
Issuer Distinguished Name	cn=<ECA CA name>, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	6 years or less from date of issue
Subject Distinguished Name	cn=<Descriptive CMS Name>, ou=<CMS Operations Company Name >, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha256WithRSAEncryption
Extensions	
authority key identifier[43]	c=no; octet string
subject key identifier[44]	c=no; octet string
key usage	c=yes; digitalSignature
Extended key usage	c=yes; id-fpki-pivi-content-signing; {2.16.840.1.101.3.8.7}
Private key usage period	Not Present
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 8}
Policy Mapping	Not Present
subject Alternative Name	c=no; optional
Issuer Alternative Name	Not Present
Basic Constraints	Not Present
Name Constraints	Not Present

[42] 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).

[43] 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.

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

Field	Medium Hardware PIV-I Authentication **Certificate Value**
Policy Constraints	Not Present
Authority Information Access	c=no; pointer to ECA certificate (required); pointer to OCSP Responder (required)
CRL Distribution Points[45]	c=no; always present

The following fields are different for the Content Signing PIV-I ECDSA certificate:

Field	Value
Issuer Signature Algorithm	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Subject Public Key Information	Algorithm OID: ecPublicKey {1 2 840 10045 2 1} Parameters: namedCurve P-256 {1 2 840 10045 3 1 7} SubjectPublic Key: Uncompressed EC Point
Issuer's Signature	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}

10.12 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} or sha256WithRSAEncryption
Issuer Distinguished Name	DN
Validity Period	20 years or less from date of issue in Generalized Time format
Subject Distinguished Name	DN
Subject Public Key Information	2048 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} or sha256WithRSAEncryption
Extensions	**Not Present**

The following fields are different for the OCSP Responder ECDSA certificate:

Field	Value
Issuer Signature Algorithm	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Subject Public Key Information	Algorithm OID: ecPublicKey {1 2 840 10045 2 1} Parameters: namedCurve P-256 {1 2 840 10045 3 1 7} SubjectPublic Key: Uncompressed EC Point
Issuer's Signature	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}

10.13 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} or sha256WithRSAEncryption
Issuer Distinguished Name	cn=<ECA CA name>, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	One month from date of issue in UTCT format

[45] 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).

Field	Value
Subject Distinguished Name	cn=<OCSP Responder Name>, ou=<OCSP Responder Company Name>, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 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} or sha256WithRSAEncryption
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 the 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; all certificate policies from Section 1.2 that the issuing CA issues certificates under
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}
Authority Information Access	c=no; pointer to ECA certificate (required)

The following fields are different for the OCSP Responder ECDSA certificate:

Field	Value
Issuer Signature Algorithm	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Subject Public Key Information	Algorithm OID: ecPublicKey {1 2 840 10045 2 1} Parameters: namedCurve P-256 {1 2 840 10045 3 1 7} SubjectPublic Key: Uncompressed EC Point
Issuer's Signature	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}

10.14 ECA ROOT CA CRL

Field	Root CA CRL Value
Version	V2 (1)
Issuer Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption
Issuer Distinguished Name	cn=ECA Root CA[46], ou=ECA, o=U.S. Government, c=US
thisUpdate	UTCT
nextUpdate	UTCT; thisUpdate + 35 days ≥ nextUpdate ≥ thisUpdate + CRL Issuance Frequency + 1 day
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (in UTCT)
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256WithRSAEncryption
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	Must be present if one of the following: key compromise; CA compromise; affiliation changed; superseded; and cessation of operations. Absent otherwise.

[46] The Common Name may optionally include generation/version number.

The following fields are different for the ECA Root CA CRL:

Field	Value
Issuer Signature Algorithm	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Subject Public Key Information	Algorithm OID: ecPublicKey {1 2 840 10045 2 1} Parameters: namedCurve P-256 {1 2 840 10045 3 1 7} SubjectPublic Key: Uncompressed EC Point
Issuer's Signature	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}

10.15 SUBORDINATE CA CRL

Field	Subordinate CA CRL Value
Version	V2 (1)
Issuer Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption
Issuer Distinguished Name	cn=<ECA CA name>, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
thisUpdate	UTCT
nextUpdate	UTCT; thisUpdate + 7 days ≥ nextUpdate ≥ thisUpdate + CRL Issuance Frequency + 4 hours
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (in UTCT)
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256WithRSAEncryption
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	Must be present if one of the following: key compromise; CA compromise; affiliation changed; superseded; and cessation of operations. Absent otherwise.

The following fields are different for the Subordinate CA CRL:

Field	Value
Issuer Signature Algorithm	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Subject Public Key Information	Algorithm OID: ecPublicKey {1 2 840 10045 2 1} Parameters: namedCurve P-256 {1 2 840 10045 3 1 7} SubjectPublic Key: Uncompressed EC Point
Issuer's Signature	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}

10.16 OCSP REQUEST FORMAT

The OCSP requests are not expected to be signed. The OCSP Responder will not check the signature on the request. See [RFC 6960] 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**

10.17 OCSP RESPONSE FORMAT

See [RFC 6960] 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[47], thisUpdate, nextUpdate[48]
Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256WithRSAEncryption
Signature	Present
Certificates	Applicable certificates issued to the OCSP Responder
Extensions	
Nonce	Will be present if nonce extension is present in the request

The following fields are different for the ECDSA OCSP Response:

Field	Value
Signature Algorithm	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}

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

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

11 IDENTITY PROOFING OUTSIDE THE U.S.

All identity proofing for U.S. citizens and non-U.S. citizens located outside the U.S. must be carried out in accordance with this Section. Identity proofing for Medium Hardware PIV-I must be carried out in accordance with Section 3.2.3; processes in this section are not acceptable for this assurance level.

Identity proofing for non-U.S. citizens located in the U.S. must be carried out in accordance with Section 3.2.3 of this CP.

11.1 IDENTITY PROOFING BY U.S. CONSULAR OFFICERS AND JUDGE ADVOCATE GENERAL OFFICERS

U.S. citizens located outside the U.S. can use the notarial services provided by U.S. consular offices and embassies, and Judge Advocate General (JAG) Officers, for identity proofing purposes under this CP. Non-U.S. citizens of those countries identified in Section 11.1.3 may also use these services for identity proofing when identity proofing is performed in one of these countries. Non-U.S. citizens who are not citizens of the countries identified in Section 11.1.3 must either comply with the requirements of Section 11.2 to obtain their identity proofing, or they must be located in the U.S. and must follow the procedures in Section 3.2.3.1 of this CP.

11.1.1 Procedures for Identity Proofing by U.S. Consular Officers or JAG Officers

Consular and JAG officers may act as notaries public for the purpose of performing identity proofing for ECA certificate applicants. Consular Officers at U.S. embassies and consulates abroad and JAG officers have the authority to administer to or take from any person any oath, affirmation, affidavit, or deposition, and to perform any other notarial act which any notary public is required or authorized by law to do within the United States. When identity proofing is performed by U.S. consular and JAG officers, all CP requirements for identity proofing by notaries must be met. In addition, applicants must present a current valid passport for proof of citizenship and as one of the documents proving identity.

Locations of U.S. consular offices and embassies may be found at:

- http://travel.state.gov/travel/tips/embassies/embassies_1214.html

See also 22 CFR 92.1-92.35. Consular officers are required to establish the identity of persons executing notarized statements. See 22 CFR 92.31 (c) which says: "(c) Satisfactory identification of grantor(s). The notarizing officer must be certain of the identity of the parties making an acknowledgment. If he is not personally acquainted with the parties, he should require from each some evidence of identity, such as a passport, police identity card, or the like. The laws of some States and Territories require that the identity of an acknowledger be proved by the oath of one or more ‘credible witnesses’, and that a statement regarding the proving of identity in this manner be included in the certificate of acknowledgment. Mere introduction of a person not known to the notarizing officer, without further proof of identity, is not considered adequate identification for acknowledgment purposes."

11.1.2 ECA Requirements

In addition to meeting all other requirements of this CP, including identity proofing using a notary, all certificates issued based on identity proofing performed by a U.S. consular or JAG officer must assert the country of citizenship of the applicant. The ECA vendor must verify that the documentation received contains the seal of a consular or JAG officer from one of the countries identified in Section 11.1.3. The ECA vendor must also verify that the applicant presented a passport as one of the identity documents and for proof of citizenship.

11.1.3 Participating Countries

- Australia
- Canada
- New Zealand
- United Kingdom

11.2 IDENTITY PROOFING BY AUTHORIZED DOD EMPLOYEES

Some DoD entities may need ECA certificates to be issued to individuals who require access to DoD web sites, but who do not reside in or are not citizens of the countries listed in Section 11.1.3. To facilitate certificate issuance to these individuals, the following process may be used when a DoD employee who interacts regularly with the certificate applicant is available and can be authorized to assist with the required identity proofing. All data exchanges that are part of this process must be authenticated by the data recipient, and the process used for this authentication must be commensurate with the strength of the certificate being issued.

Identity proofing is subject to compliance audit requirements as outlined in Section 8 of the CP. Procedures followed by authorized DoD employees are subject to compliance audit only by the EPMA at the discretion of the DoD PKI ECA Liaison Officer.

11.2.1 Process for Authorizing Issuance of ECA Certificates When Identity Proofing Is Performed by Authorized DoD Employees Outside the U.S.

A DoD Component or Program that desires to sponsor applicants for ECA certificates must complete the following steps:

- Ensure that a formal agreement, such as a Memorandum of Understanding (MOU), exists between the DoD and the foreign government, which requires the need for information exchange with local nationals in that country or with citizens of that country to accomplish the goals of the agreement.
- Submit a formal request in a digitally signed email to their DoD Component PKI POC, requesting participation in the program, and including the following:
    - A statement of the requirement to exchange information,
    - Information about the agreement(s) that exist, and,
    - A statement that the DoD Program Sponsor will follow the procedures outlined in Section 11 of the ECA CP for performing identity proofing.
- Provide the list of sponsored applicants and countries to the DoD PKI ECA Liaison Officer and DoD Component PKI POC in a digitally signed email. The Program Sponsor shall either have personal knowledge of the sponsored applicants or shall obtain this information in an authenticated manner from an authorized local representative. This list must be on file with the DoD PKI ECA Liaison Officer. The DoD PKI ECA Liaison Officer and DoD Component PKI POC may vet the list.
- Coordinate in an authenticated manner with the DoD PKI ECA Liaison Officer and DoD PKI Component POC to ensure there are authorized DoD Employees who can support the identity proofing of sponsored applicants.

The DoD Component PKI POC must complete the following steps:

- Agree to follow the procedures outlined in Section 11 of the ECA CP for performing identity proofing.
- Coordinate with the DoD PKI ECA Liaison Officer to identify and establish authorized DoD Employees
- Each authorized DoD employee must:
    - Be a U.S. citizen,
    - Have a SECRET or higher clearance granted by the U.S.,
    - Have a Common Access Card (CAC) containing an identity certificate issued by the DoD PKI,
    - Be authorized to perform identity proofing for a specified set of countries, and,
    - Review the procedures in Section 11.2.2 for performing identity proofing of non-U.S. Citizens and submit a digitally signed statement to the DoD PKI ECA Liaison Officer, acknowledging the DoD employee's roles and responsibilities. [Note: Familiarity with passports and all other approved proof of citizenship documents in the country must be one of the enumerated responsibilities.]

- Provide the list of authorized DoD employees to the DoD PKI ECA Liaison Officer in a digitally signed email. This list must contain the CAC signature certificate subject distinguished name for each authorized DoD employee and state which employees are authorized to perform identity proofing for which foreign countries. The DoD Component must keep this list current and must, at a minimum, provide an updated list quarterly.
- Validate the program, the Program Sponsor, and the authority of the Program Sponsor POC to speak for the program.
- Decide whether or not to approve requests from validated Program Sponsors.
- Provide a list of approved program sponsors and a POC for each program to the DoD PKI ECA Liaison Officer in an authenticated manner

The DoD PKI ECA Liaison Officer must complete the following steps:

- Maintain a list of current DoD Component PKI POCs,
- Maintain a list of authorized DoD Employees for each country,
- Provide the list of authorized DoD Employees to approved Program Sponsors in a digitally signed email,
- Maintain the list of approved applicants, including vetting the list of countries and applicants,
- Provide the list of approved applicants to the authorized DoD Employees in a digitally signed email, and;
- Provide the list of authorized DoD Employees, along with their certificate information, to appropriate ECAs in a digitally signed email.

11.2.2 Identity Proofing Procedures to Be Used by Authorized DoD Employees for ECA Certificates

Once DoD employees have been authorized using the process identified in Section 11.2.1, they must adhere to the following requirements for performing identity proofing of non-U.S. citizens applying for ECA certificates:

- The authorized DoD employee must have a copy of the list of individuals of the country who are authorized to receive certificates, which shall include assertion of their citizenship. The authorized DoD employee must authenticate the list and may only accept it if the source is the ECA Liaison Officer.
- The authorized DoD employee must have the list of approved proof of citizenship documents and be able to recognize legitimate versions of identity documentation that will be provided by the applicant.
- The applicant must appear, in person, before the authorized DoD employee. The authorized DoD employee must verify that the applicant is on the list of individuals.
- The applicant must present two forms of identification, at least one of which must be a proof of citizenship, either a passport or another document from the approved list, and both of which forms of identification must be recognized as legitimate identity documents by the authorized DoD employee.
- The applicant and the authorized DoD employee must exchange sufficient information for the ECA vendor to ensure that the binding of the identity proofing to the certificate request is unambiguous and accurate. This information (e.g., certificate request number, certificate request password) may vary among ECAs, but must be specifically defined by the ECA in its CPS as part of its certificate request process.
- The applicant must sign a copy of the ECA's subscriber agreement form in the presence of the authorized DoD employee.
- The authorized DoD employee must also sign the ECA's subscriber agreement form. The authorized DoD employee must retain a copy and provide a copy of the signed form to the applicant. DoD Components may choose to maintain subscriber agreements in a centralized location, in which case the DoD Component PKI POC must provide the authorized DoD employees with instructions for transferring the forms to the centralized location.

- The authorized DoD employee must send an email that is digitally signed with the employee's CAC signature certificate to the ECA, containing:
    - The name of the applicant,
    - A statement that the authorized DoD employee has performed identity proofing for this applicant in accordance with the ECA CP,
    - The citizenship of the applicant, and,
    - The information binding the identity proofing to the certificate request for the applicant.

11.2.3 ECA Requirements

In addition to meeting all other requirements of this CP, ECAs must adhere to the following requirements when accepting identity proofing performed by authorized DOD employees:

- Specify in their CPS the information exchanged among the ECA, the applicant, and the authorized DoD employee to ensure that the binding of the identity proofing to the certificate request is unambiguous and accurate.
- Obtain in an authenticated manner the list of authorized DoD employees from the DoD PKI ECA Liaison Officer.
- Receive, prior to each certificate issuance, an email digitally signed by a CAC-based signature certificate of the authorized DoD employee, asserting that the identity proofing has taken place. This email must contain information sufficient to accurately and unambiguously match the individual's identity proofing with the pending certificate request. The ECA shall verify the signature on the email, including full certification path validation, as described in [RFC 5280]. The ECA shall also verify that the signer of the email is on the list of authorized DoD employees.
- Provide a copy of the ECA subscriber agreement to all applicants.
- Provide the email address that authorized DoD employees must use when sending to the ECA the confirmation that identity proofing has taken place.
- Assert the country of citizenship of the applicant for all certificates issued based on identity proofing performed by an authorized DoD employee.

11.2.4 Participating Countries

ECA vendors may issue ECA certificates to qualified local nationals, except nationals of countries otherwise proscribed by law and regulation at the time of the application for the certificate. Relevant laws and regulations that may be applicable include:

- Department of Commerce Export Administration Regulations (EAR), 15 C.F.R. Section 730 et. seq., including specifically, but not limited to, Parts 736, 738, 740, 744 Spir, and 746. See http://www/access.gop.gov/bis/ear/ear_data.html.

  Export License D1135970 (Department of Commerce, Bureau of Industry and Security). As required by EAR 762.2 (a)(11), ECA vendors shall: (a) retain copies of all records pertaining to each ECA certificate exported to an individual under Export License D1135970 who supports DoD contracts and requires access to DoD Information Systems and networks; and (b) provide the records upon written request within the timeframe specified in the requesting document, to DISA, DoD and/or to the Department of Commerce's Bureau of Industry and Security.
- Department of the Treasury Regulations issued pursuant to the International Emergency Economic Powers Act (IEEPA), 50 U.S. Code Ch. 35. See 1701 et. seq. or other laws identifying prohibited countries or people or entities, including the Office of Foreign Assets Control (OFAC) Listing of Specifically Designated Nationals and Blocked Persons (SDN List) and OFAC Country Sanctions Programs. For more information, see specifically:

  http://www.treas.gov/offices/enforcement/ofac/index.shtml and
  http://www.treas.gov/offices/enforcement/lists.

The ECA vendor is required, at the time of issuing an ECA certificate, to review all relevant laws and regulations, including those cited above, to determine whether the subscriber is a local national or entity, or from a country proscribed by law or regulation. The ECA vendor may not issue a certificate to any applicant determined to be ineligible.

11.3 IDENTITY PROOFING BY ECA REGISTRATION AUTHORITY OR TRUSTED AGENT

U.S. citizens located outside the U.S. requiring Medium Software assurance, Medium Token assurance, and Medium Hardware assurance certificates may have identity verification performed by an ECA Registration Authority (RA) or Trusted Agent (TA) who is located outside the U.S. All requirements specified in this CP for an ECA RA and TA shall apply. Non-U.S. citizens of the countries listed in Section 11.1.3 may also use an ECA RA or TA for identity proofing when identity proofing is performed in one of these countries. Note that per Section 5.3.1 of this CP, RAs must be U.S. citizens. TAs must be U.S. citizens unless the identity proofing is carried out in one of the countries listed in Section 11.1.3. In that case, the TA must either be a U.S. citizen or a citizen of the country where the identity proofing is performed.

11.3.1 Procedures for Identity Proofing by ECA RA or TA

The RA or TA shall meet the CP requirements specified in Section 3.2.3.1 for in-person authentication of Subscribers. When identity proofing is performed by an RA or TA, applicants must present a current valid passport for proof of citizenship and as one of the documents proving identity.

11.3.2 ECA Requirements

In addition to meeting all other requirements of this CP, all certificates issued based on identity proofing performed by an RA or TA must assert the country of citizenship of the applicant. The RA or TA must also verify that the applicant presented a passport as one of the identity documents and for proof of citizenship.

12 PIV-INTEROPERABLE SMART CARD DEFINITION

To support technical interoperability of PIV-I cards with Federal Agency PIV implementations, certificates asserting any of the PIV-I policies must comply with the technical specifications used for Federal Agency issued PIV cards. Hardware tokens used for Medium Hardware PIV-I and Card Authentication PIV-I certificates and the systems used to create them shall meet all of the following requirements.

- To ensure interoperability with Federal systems, PIV-I Cards shall use a smart card platform that is on GSA's *Personal Identity Verification (PIV) of Federal Employees and Contractors* [FIPS201-2] Evaluation Program APL and uses the PIV application identifier (AID).
- PIV-I Cards shall conform to NIST Special Publication 800-73, *Interfaces for Personal Identity Verification* [SP800-73], ensuring that PIV-I UUID requirements are met.
- PIV-I Cards shall contain an authentication certificate that conforms to the Medium Hardware PIV-I policy and the profile specified in Section 10.
- PIV-I Cards shall contain a card authentication certificate that conforms to the Card Authentication PIV-I policy, [SP800-73], and the profile specified in Section 10.
- PIV-I Cards shall contain an electronic representation (as specified in [SP800-73] and NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification* [SP800-76] of the Cardholder Facial Image printed on the card.
- PIV-I Cards shall contain an electronic representation (as specified in [SP800-76] of the fingerprint images collected during card registration.
- PIV-I Cards shall contain signature and encryption certificates that conform to the Medium Hardware PIV-I policy and the profile specified in Section 10.
- PIV-I Cards shall be visually distinguishable from Federal PIV Cards to ensure no suggestion of attempting to create a fraudulent Federal PIV Card. At a minimum, images or logos on a PIV-I Card shall not be placed entirely within Zone 11, Agency Seal, as defined by [FIPS201-2].
- The PIV-I Card physical topography shall include, at a minimum, the following items on the front of the card:
    a. Cardholder facial image;
    b. Cardholder full name;
    c. Organizational Affiliation, if exists; otherwise the issuer of the card; and
    d. Card expiration date.
- PIV-I Cards shall have an expiration date not to exceed 3 years after issuance date.
- Expiration of the PIV-I Card shall not be later than expiration of Content Signing PIV-I certificate used to sign the content on the card.
- The digital signature certificate that is used to sign objects on the PIV-I Card (e.g., CHUID, Security Object) shall contain the Content Signing PIV-I policy OID, and shall conform to the profile in Section 10.
- The Content Signing PIV-I certificate and corresponding private key shall be managed within a trusted CMS.
- At issuance, the RA shall activate and release the PIV-I Card to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.1.
- To activate the card for personalization or update, the card management system shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73]. When cards are personalized, card diversified keys shall be set to be specific to each PIV-I Card. That is, each PIV-I Card shall contain a unique card diversified key. Card diversified keys shall meet the algorithm and key size requirements stated in NIST Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification* [SP800-78]. At a minimum, the Secure Channel specification version 02 with three key 3DES along with a plan to transition to AES shall be implemented.

- When the Card Management System is used for PIV-I issuance, the Card Management Master Key shall conform to NIST SP 800-78.

13 REFERENCES

The following documents are referenced in this policy:

Number	Title	Date
ABADSG	*Digital Signature Guidelines*	1 August 1996
CNSSI 4009	CNSS Instruction 4009, *Committee on National Security Systems Glossary*	6 April 2015
FIPS140-2	*Security Requirements for Cryptographic Modules*	25 May 2001
FIPS186-4	*Digital Signature Standard*	July 2013
FIPS201-2	*Personal Identity Verification (PIV) of Federal Employees and Contractors*	August 2013
FPKI-E	*Federal PKI Certificate and CRL Profile*	5 May 2015
ISO9594-8	*Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*	2017
RFC 3647	*Certificate Policy and Certification Practices Framework,* Chokhani, et al.	November 2003
RFC 4122	*A Universally Unique IDentifier (UUID) URN Namespace*	July 2005
RFC 4210	*Internet X.509 Public Key Infrastructure Certificate Management Protocol*	September 2005
RFC 5280	*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*	May 2008
RFC 6960	*X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*	June 2013
SP800-73	*Interfaces for Personal Identity Verification, Version 4*	May 2015 (Updated February 2016)
SP800-76	*Biometric Data Specification for Personal Identity Verification*	July 2013

14 ACRONYMS AND ABBREVIATIONS

AES	Advanced Encryption Standard
AID	Application Identifier
APL	Approved Product List
CA	Certification Authority
CMA	Certificate Management Authority
CMS	Card Management System
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
ECDSA	Elliptic Curve Digital Signature Algorithm
EPMA	ECA Policy Management Authority
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standard
FPKI	(U.S.) Federal Public Key Infrastructure
FTP	File Transfer Protocol
ID	Identity (also, a credential asserting an identity)
IP	Internet Protocol
ISO	International Organization for Standards
IT	Information Technology
JAG	Judge Advocate General
KEA	Key Exchange Algorithm
KES	Key Escrow System
KRA	Key Recovery Authority
KRP	Key Recovery Policy
KRPS	Key Recovery Practice Statement
MD	Maryland
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification Interoperable
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
POC	Point of Contact
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest, Shamir, Adleman (encryption and digital signature algorithm)
S/MIME	Secure Multipurpose Internet Mail Extensions

SCVP	Server-based Certificate Validation Protocol
SHA	Secure Hash Algorithm
TA	Trusted Agent
TLS	Transport Layer Security
UPN	User Principal Name
US	United States
USD	United States Dollar
UUID	Universally Unique Identifier
VME	Virtual Machine Environment
WWW	World Wide Web

15 GLOSSARY

The primary source is the *Committee on National Security Systems Glossary* [CNSSI 4009]; other sources were used if [CNSSI 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. [CNSSI 4009]
access control	The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances). [CNSSI 4009]
accreditation	Formal declaration by a designated accrediting authority (DAA) or principal accrediting authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. [CNSSI 4009]
Affiliated Organization	An organization that has a relationship with a subscriber and sponsors that subscriber for obtaining a certificate. Affiliated Organizations are responsible for verifying the affiliation at the time of certificate application and requesting revocation of the certificate if the affiliation is no longer valid.
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 and ensure compliance with established policies and operational procedures. [CNSSI 4009]
audit data	1. A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result. 2. A record showing who has accessed an information technology (IT) system and what operations the user has performed during a given period. [CNSSI 4009, "audit trail"]
authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. [CNSSI 4009]
backup	A copy of files and programs made to facilitate recovery, if necessary. [CNSSI 4009]
binding	Process of associating two related elements of information. [CNSSI 4009]
biometric	A measurable biological (anatomical or physiological) and behavioral characteristic that can be used for automated recognition.
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. [CNSSI 4009]
confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [CNSSI 4009]

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. [FIPS140-2]
Diversified Key	A unique key for each card that is generated using the Master Key and the card identifying elements
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. An encryption certificate asserts a key usage of key encipherment or key agreement.
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	A gateway that limits access between networks in accordance with local security policy. [CNSSI 4009]
Group/Role Manager	A person who is responsible for managing the Group/Role, including assigning individuals to the Group/Role membership and maintaining the list of Group/Role members and public key certificates issued to them
Hypervisor	Computer software, firmware or hardware that creates and runs virtual machines. A hypervisor uses native execution to share and manage hardware, allowing for multiple environments which are isolated from one another, yet exist on the same physical machine. Also known as an isolation kernel or virtual machine monitor.
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	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [CNSSI 4009]
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.
Key Recovery Authority	A Registration Authority designated to perform key recovery operations.
Master Key	The key required to unlock the Open Platform Key and allow changes to the contents of the card. Each card is shipped with a Manufacturer Master Key, which may optionally be changed for a Client Master Key as part of the card initialization step.
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	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message. [CNSSI 4009]
OCSP Responder	A trusted entity that provides on-line revocation status of certificates to Relying Parties. The OCSP Responder is either explicitly trusted by the Relying Party, or through the CA that issued the certificate whose revocation status is being sought.
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. [CNSSI 4009]
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	The continuous surveillance and control of material at all times by a minimum of two authorized individuals, each capable of detecting incorrect or unauthorized procedures with respect to the task being performed and each familiar with established security requirements. [CNSSI 4009]
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.
Virtual Machine Environment	A computer system that provides the functionality of a physical machine in a platform-independent environment. It provides the functionality needed to execute an entire operating system.
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. [FIPS140-2]

16 SUMMARY OF CHANGES TO ECA CERTIFICATE POLICY, VERSION 4.1

Version 4.2, 2 February 2011

Change	Sections	Change Summary
2010-01	6.1.5	Aligned the ECA CP with the DoD CP in not specifying a date for the transition from SHA-1 to SHA-256 hashes in certificates and CRLs.

Version 4.3, 4 January 2012

Change	Sections	Change Summary
2011-01	3.2.3.1 11.2.1, 11.2.2	Streamlined the identity proofing process for issuing ECA certificates to local nationals outside the United States.
2011-02	Multiple	Added OIDs and associated requirements to meet Federal Bridge SHA-256, Device, and PIV-I requirements.

Version 4.4, 1 October 2015

Change	Sections	Change Summary
2013-01	Multiple	Clarified ECA CP requirements for compliance to the Federal Bridge CP.
2015-01	1.2, 6.1.5	Added a Medium Hardware SHA-256 Policy OID.
2015-02	11.2.4	Removed the restriction for issuing certificates in ITAR-controlled countries and referenced Bureau of Industry and Security export license.
2015-03	3.2.3.3, 5.4.1, 6.1.7, 6.2.3, 15	Updated text to align with changes to DoD CP text.
2015-04	2.4,10.3,10.4	Removed UUID from signature and encryption certificates.

Version 4.5, 20 February 2019

Change	Sections	Change Summary
2018-01	1.2, 10.7	Restricted CAs to only issue Version 2 Certificate Revocation Lists.
2018-02	Multiple	Added new certificate policy OIDs and requirements for issuing certificates with 192 bits of security.
2018-03	Multiple	Deprecated the use of the FORTEZZA certificate policy OID.
2018-04	6.2.1, 12	Added new certificate policy OID and requirements for issuing certificates that identify system administrators.
2018-05	6.2.1, 6.4.3	Added new certificate policy OIDs and requirements for the DoD Internal NPE PKI.
2018-06	Multiple	Added requirements for protecting private keys for multiple end entities when aggregated in a single cryptographic module.
2018-07	7.1.7, 7.1.10, 10.2	Added specific controls for the use of a Virtual Machine Environment to support CA or RA systems.
2018-08	11.2.4	Changed the requirement for direct CMA action to perform revocation to allow for more flexibility in how revocations are processed.
2018-09	Multiple	Editorial updates and changes required by updates to referenced documents.