X.509 Certificate Policy

For The

U.S. Federal PKI

Common Policy Framework

Version 3647 - 1.17

December 9, 2011

Signature Page

DEBORAH GALLAGHER

Digitally signed by DEBORAH GALLAGHER
DN: c=US, o=U.S. Government, ou=General Services Administration, cn=DEBORAH GALLAGHER, 0.9.2342.19200300.100.1.1=47001001545490
Date: 2011.12.09 11:35:12 -05'00'

Chair, Federal Public Key Infrastructure Policy Authority

9 December 2011
DATE

Revision History

Document Version	Document Date	Revision Details
1.0	May 7, 2007	Revised Common Policy (RFC 3647 format)
1.1	July 17, 2007	Alignment of Cryptographic Algorithm Requirements with SP 800-78-1
1.2	September 12, 2007	Requiring the inclusion of a subject DN in PIV Authentication Certificates
1.3	October 16, 2007	Accommodating legacy PKIs for PIV Authentication
1.4	April 3, 2008	§ 8.3 Assessor's Relationship to Assessed Entity
1.5	November 20, 2008	Include a provision for a role-based signature certificate
1.6	February 11, 2009	nextUpdate in Certificate Revocation Lists (CRL) published by legacy Federal PKIs
1.7	April 15, 2009	Allow the use of the PIV Authentication certificate as proof of identity and employment
1.8	January 21, 2010	Align key length requirements w/ SP 800-57 Remote Administration of Certification Authorities
1.9	March 15, 2010	Allowing inclusion of UUIDs in Card Authentication Certificates
1.10	April 8, 2010	§ 8.1 & 8.4
1.11	August 16, 2010	Clarify the archive definition and how its records are intended to be used
1.12	October 15, 2010	Allow Federal Legacy PKIs to Directly Cross Certify with Common Policy CA
1.13	November 18, 2010	Legacy use of SHA-1 during transition period Jan 1, 2011 to Dec 31, 2013

Document Version	Document Date	Revision Details
1.14	December 17, 2010	Clarify requirement to support CA Key Rollover
1.15	January 24, 2011	**2011-01**, CAs to assert policy OIDs in OCSP responder certificates for which the OCSP responder is authoritative
1.16	September 23, 2011	**2011-02**, Clarify requirements for device subscribers and certificates
1.17	December 13, 2011	**2011-03**, Remove Requirements for LDAP References in Certificates

FOREWORD

This is the policy framework governing the public key infrastructure (PKI) component of the Federal Enterprise Architecture. The policy framework incorporates seven specific certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, a policy for devices with software cryptographic modules, a policy for devices with hardware cryptographic modules, a high assurance user policy, a user authentication policy, and a card authentication policy. There are two Certification Authorities associated with the Common Policy Framework: The Federal Common Policy Root CA and the SHA-1 Federal Root CA.

The user policies apply to Federal employees, contractors, and other affiliated personnel requiring PKI credentials for access to Federal systems that have not been designated by law as national security systems. The device policies apply to hardware devices and software applications operated by or on behalf of federal agencies. These policies may be used by PKIs whose certification practice statement (CPS) and compliance audit have been approved by the Federal PKI Policy Authority (FPKIPA). Such PKIs may be agency operated or may be operated by approved providers.

This policy framework supports hierarchical PKI, mesh PKI, and single certification authority (CA) implementations of this certificate policy. As such, constraints are established for the secure distribution of self-signed certificates for use as trust anchors. These constraints apply only to CAs that choose to distribute self-signed certificates.

This policy framework requires the use of FIPS 140 validated cryptographic modules by Federal employees, contractors, other affiliated personnel and devices for all cryptographic operations and the protection of trusted public keys. Software and hardware cryptographic mechanisms are equally acceptable under this policy framework. The policies for users with hardware cryptographic modules mandate Level 2 validation.

For entities associated with the Federal Common Policy Root CA, this policy framework requires the use of either 2048 bit RSA keys or 256 bit elliptic curve keys along with the SHA-256 and SHA-384 hash algorithms. CAs are required to use 2048 bit RSA keys or 256 bit elliptic curve keys when signing certificates and CRLs that expire on or after December 31, 2010. CAs are required to use SHA-256 or SHA-384 when signing certificates that are issued after December 31, 2010. All subscriber signature keys in certificates that expire on or after December 31, 2008 must be at least 2048 bit RSA keys or 256 bit elliptic curve keys. Subscriber authentication keys in certificates that expire on or after December 31, 2013 must be at least 2048 bit RSA keys or 256 bit elliptic curve keys.

For entities associated with the SHA-1 Federal Root CA, subscriber certificates may assert a certificate policy OID that indicates the use of SHA-1, if issued before December 31, 2013. CAs that issue SHA-1 certificates after December 31, 2013 may not also issue SHA-256 certificates.

The certificate policies that comprise this policy framework are consistent with RFC 3647, the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practices Framework.

The terms and provisions of these certificate policies shall be interpreted under and governed by applicable Federal law.

Table of Contents

Introduction

This certificate policy (CP) includes seven distinct certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, a policy for devices with software cryptographic modules, a policy for devices with hardware cryptographic modules, a high assurance user policy, a user authentication policy, and a card authentication policy. In this document, the term "device" means a non-person entity, i.e., a hardware device or software application. Where a specific policy is not stated, the policies and procedures in this specification apply equally to all seven policies.

The use of SHA-1 to create digital signatures is deprecated beginning January 1, 2011. However, there are some applications in use within the federal government that cannot process certificates or certificate revocation information signed using SHA-256. Therefore this CP also includes five additional distinct certificate policies which indicate the use of the deprecated SHA-1 after December 31, 2010. These id-fpki-sha1 policies adhere to all the requirements of the associated id-common policy with the exception that the certificate is generated with a SHA-1 signature and the issuing CA may use SHA-1 for generation of PKI objects such as CRLs and OCSP responses until December 31, 2013. It should be noted that certificates issued on or after January 1, 2011 are not FIPS 201 compliant, and therefore do not meet the requirements of HSPD-12. CAs that issue SHA-1 certificates after December 31, 2010 may not also issue FIPS 201 compliant certificates.

The user policies apply to certificates issued to Federal employees, contractors, and other affiliated personnel for the purposes of authentication, signature, and confidentiality. This CP was explicitly designed to support access to Federal systems that have not been designated national security systems.

A PKI that uses this CP will provide the following security management services:

- Key generation/storage
- Certificate generation, modification, re-key, and distribution
- Certificate revocation list (CRL) generation and distribution
- Directory management of certificate related items
- Certificate token initialization/programming/management
- System management functions (e.g., security audit, configuration management, archive.)

The user policies require Federal employees, contractors, and other affiliated personnel to use FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys. The device policy also requires use of FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys.

This policy does not presume any particular PKI architecture. The policy may be implemented through a hierarchical PKI, mesh PKI, or a single certification authority (CA). Any CA that asserts this policy in certificates must obtain prior approval from the Federal PKI Policy Authority. CAs that issue certificates under this policy may operate simultaneously under other

policies. Such CAs must not assert the OIDs in this policy in certificates unless they are issued in accordance with all the requirements of this policy.

This policy establishes requirements for the secure distribution of self-signed certificates for use as trust anchors. These constraints apply only to CAs that chose to distribute self-signed certificates, such as a hierarchical PKI's root CA.

This CP is consistent with request for comments (RFC) 3647, the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practices Framework.

1.1 OVERVIEW

1.1.1. Certificate Policy (CP)

Certificates issued under this policy contain a registered certificate policy object identifier (OID), which may be used by a relying party to decide whether a certificate is trusted for a particular purpose. This CP applies only to CAs owned by or operated on behalf of the Federal government that issue certificates according to this policy.

1.1.2. Relationship between the CP and the CPS

This CP states what assurance can be placed in a certificate issued by the CA. The certification practice statement (CPS) states how the CA establishes that assurance. Each CA that issues certificates under this CP shall have a corresponding CPS.

1.1.3. Scope

This CP applies to certificates issued to CAs, devices, and Federal employees, contractors and other affiliated personnel. This CP does not apply to certificates issued to groups of people.

1.1.4. Interoperation with CAs Issuing under Different Policies

Except for legacy Federal PKIs, interoperation with CAs that issue under different policies will be achieved through policy mapping and cross-certification through the Federal Bridge Certification Authority. Legacy Federal PKIs may perform policy mapping and cross-certification with either the Common Policy Root CA or Federal Bridge Certification Authority at their discretion.

Note that interoperability may also be achieved through other means, such as trust lists, to meet local requirements.

1.2. DOCUMENT NAME AND IDENTIFICATION

This CP provides substantial assurance concerning identity of certificate subjects. Certificates issued in accordance with this CP and associated with the Federal Common Policy Root CA shall assert at least one of the following OIDs in the certificate policy extension:

Table 1 - id-fpki-common Policy OIDs

id-fpki-common-policy	::= {2 16 840 1 101 3 2 1 3 6}
id-fpki-common-hardware	::= {2 16 840 1 101 3 2 1 3 7}
id-fpki-common-devices	::= {2 16 840 1 101 3 2 1 3 8}
id-fpki-common-devicesHardware	::= {2 16 840 1 101 3 2 1 3 36}
id-fpki-common-authentication	::= {2 16 840 1 101 3 2 1 3 13}
id-fpki-common-High	::= {2 16 840 1 101 3 2 1 3 16}
id-fpki-common-cardAuth	::= {2 16 840 1 101 3 2 1 3 17}

Additionally, this CP provides moderate assurance concerning identity of certificate subjects when the following OIDs are expressed in certificate policy extensions of certificates issued after December 31, 2010, associated with the SHA-1 Federal Root CA, and signed using SHA-1.

Table 2 - id-fpki-SHA1 Policy OIDs

SHA1 Policy	OID	Corresponding id-fpki-common policy
id-fpki-SHA1-policy	::= {2 16 840 1 101 3 2 1 3 23}	id-fpki-common-policy id-fpki-certpcy-mediumAssurance
id-fpki-SHA1-hardware	::= {2 16 840 1 101 3 2 1 3 24}	id-fpki-common-hardware id-fpki-certpcy-mediumHardware
id-fpki-SHA1-devices	::= {2 16 840 1 101 3 2 1 3 25}	id-fpki-common-devices id-fpki-certpcy-mediumAssurance
id-fpki-SHA1-authentication	::= {2 16 840 1 101 3 2 1 3 26}	id-fpki-common-authentication id-fpki-certpcy-mediumHardware
id-fpki-SHA1-cardAuth	::= {2 16 840 1 101 3 2 1 3 27}	id-fpki-common-cardAuth

Certificates issued to CAs may contain any or all of these OIDs. Certificates issued to users, other than devices, to support digitally signed documents or key management may contain either id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-High. Subscriber certificates issued to devices under this policy that use FIPS 140 Level 2 or higher cryptographic modules shall include either id-fpki-common-deviceHardware, id-fpki-common-devices, or both. Subscriber certificates issued to devices under this policy using software cryptographic modules shall include id-fpki-common-devices.

This document includes two policies specific to the FIPS 201 Personal Identity Verification Card. Certificates issued to users supporting authentication but not digital signature may contain id-fpki-common-authentication. Certificates issued to users supporting authentication where the private key can be used without user authentication may contain id-fpki-common-cardAuth.

The requirements associated with a id-fpki-SHA1 policy are identical to those defined for the corresponding id-fpki-common policy, except that the certificates asserting id-fpki-SHA1-policies are signed with SHA-1, and the issuing CAs can use SHA-1 for generation of PKI objects such as CRLs and OCSP responses until December 31, 2013.

1.3. PKI PARTICIPANTS

The following are roles relevant to the administration and operation of CAs under this policy:

1.3.1. PKI Authorities

1.3.1.1 Federal Chief Information Officers Council

The Federal CIO Council comprises the Chief Information Officers of all cabinet level departments and other independent agencies. The Federal CIO Council has established the framework for the interoperable Federal PKI (FPKI) and oversees the operation of the organizations responsible for governing and promoting its use. In particular, this CP was established under the authority of and with the approval of the Federal CIO Council.

1.3.1.2 Federal PKI Policy Authority (FPKIPA)

The Federal PKI Policy Authority (FPKIPA) is a group of U.S. Federal Government Agencies (including cabinet-level Departments) chartered by the Federal CIO Council. The FPKIPA owns this policy and represents the interest of the Federal CIOs. The FPKIPA is responsible for:

- Maintaining this CP,
- Approving the CPS for each CA that issues certificates under this policy,
- Approving the compliance audit report for each CA issuing certificates under this policy, and
- Ensuring continued conformance of each CA that issues certificates under this policy with applicable requirements as a condition for allowing continued participation.

1.3.1.3 FPKI Management Authority (FPKI MA)

The FPKI Management Authority is the organization that operates and maintains the Common Policy Root CA and the SHA-1 Federal Root CA on behalf of the U.S. Government, subject to the direction of the FPKIPA. All of the requirements for the SHA1 Federal Root CA are identical to the Common Policy Root CA except that the SHA-1 Federal Root CA asserts id-fpki-sha1 policies and shall use SHA-1 for generation of PKI objects such as certificates, Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) responses after December 31, 2010 and before December 31, 2013.

1.3.1.4 FPKI Management Authority Program Manager

The Program Manager is the individual within the FPKI Management Authority who has principal responsibility for overseeing the proper operation of the Common Policy Root CA including the Common Policy Root CA repository, and selecting the FPKI Management Authority staff. The Program Manager is selected by the FPKI Management Authority and reports to the FPKIPA. The FPKI Management Authority Program Manager must hold a Top Secret security clearance.

1.3.1.5 Agency Policy Management Authority

Agencies that operate a CA under this policy, or contract for the services of a CA under this policy, shall establish a management body to manage any agency-operated components (e.g., RAs or repositories) and resolve name space collisions. This body shall be referred to as an Agency Policy Management Authority, or Agency PMA.

1.3.1.6 Certification Authority

The CA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to subscribers. The CA is responsible for the issuing and managing certificates including:

- The certificate manufacturing process
- Publication of certificates
- Revocation of certificates
- Generation and destruction of CA signing keys
- Ensuring that all aspects of the CA services, operations, and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.7 Certificate Status Servers

PKIs may optionally include an authority that provides status information about certificates on behalf of a CA through on-line transactions. In particular, PKIs may include OCSP responders to provide on-line status information. Such an authority is termed a certificate status server (CSS). Where the CSS is identified in certificates as an authoritative source for revocation information, the operations of that authority are considered within the scope of this CP. A Certificate Status Server (CSS) shall assert all the policy OIDs for which it is authoritative. Examples include OCSP servers that are identified in the authority information access (AIA) extension. OCSP servers that are locally trusted, as described in RFC 2560, are not covered by this policy.

1.3.2. Registration Authorities

The registration authorities (RAs) collect and verify each subscriber's identity and information that is to be entered into the subscriber's public key certificate. The RA performs its function in accordance with a CPS approved by the FPKIPA. The RA is responsible for:

- Control over the registration process

- The identification and authentication process.

1.3.3. Trusted Agents

The trusted agent is a person who satisfies all the trustworthiness requirements for an RA and who performs identity proofing as a proxy for the RA. The trusted agent records information from and verifies biometrics (e.g., photographs) on presented credentials for applicants who cannot appear in person at an RA. The CPS will identify the parties responsible for providing such services, and the mechanisms for determining their trustworthiness.

1.3.4. Subscribers

A subscriber is the entity whose name appears as the subject in a certificate. The subscriber asserts that he or she uses the key and certificate in accordance with the certificate policy asserted in the certificate, and does not issue certificates. For this policy, subscribers are limited to Federal employees, contractors, affiliated personnel, and devices operated by or on behalf of Federal agencies. CAs are sometimes technically considered "subscribers" in a 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 or certificate status information.

There is a subset of human subscribers who will be issued role-based certificates. These certificates will identify a specific role on behalf of which the subscriber is authorized to act rather than the subscriber's name and are issued in the interest of supporting accepted business practices. The role-based certificate can be used in situations where non-repudiation is desired. Normally, it will be issued in addition to an individual subscriber certificate. A specific role may be identified in certificates issued to multiple subscribers, however, the key pair will be unique to each individual role-based certificate (i.e. there may be four individuals carrying a certificate issued in the role of "Secretary of Commerce" however, each of the four individual certificates will carry unique keys and certificate identifiers). Roles for which role-based certificates may be issued are limited to those that are held by a unique individual within an organization (e.g. *Chief Information Officer, GSA* is a unique individual whereas *Program Analyst, GSA* is not).

> Practice Note: When determining whether a role-based certificate is authorized, consider whether the role carries inherent authority beyond the job title. Role-based certificates may also be used for individuals on temporary assignment, where the temporary assignment carries an authority not shared by the individuals in their usual occupation, for example: "*Watch Commander, Task Force 1*".

1.3.5. Relying Parties

A relying party is the entity that relies on the validity of the binding of the subscriber's name to a public key. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The relying party can use the 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. A

relying party may use information in the certificate (such as CP identifiers) to determine the suitability of the certificate for a particular use.

For this certificate policy, the relying party may be any entity that wishes to validate the binding of a public key to the name (or role) of a federal employee, contractor, or other affiliated personnel.

1.3.6. Other Participants

The CAs and RAs operating under this CP may require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The CPS will identify 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 sensitivity of the information processed or protected using certificates issued by the CA will vary significantly. Organizations must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each organization for each application and is not controlled by this CP.

This CP is intended to support the use of validated public keys to access Federal systems that have not been designated national security systems. While a validated public key is not generally sufficient to grant access the key may be sufficient when supplemented by appropriate authorization mechanisms. Credentials issued under this CP may also be used for key establishment. This policy is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to federal statues and regulations.

Credentials issued under the id-fpki-common-policy policy are intended to meet the requirements for Level 3 authentication, as defined by the OMB E-Authentication Guidance. [E-Auth] Credentials issued under the id-fpki-common-hardware, id-fpki-common-authentication, and id-fpki-common-High policies meet the requirements for Level 4 authentication, as defined by the OMB E-Authentication Guidance. [E-Auth]

In addition this policy may support signature and confidentiality requirements for Federal government processes.

The digital signatures on certificates issued under this policy may be generated using SHA-1 only when one or more of the id-fpki-SHA1 policy OIDs is used. The use of SHA-1 to create digital signatures is deprecated beginning January 1, 2011. As such, use of SHA-1 certificates issued under this policy should be limited to applications for which the risks associated with the use of a deprecated cryptographic algorithm have been deemed acceptable.

1.4.2. Prohibited Certificate Uses

Certificates that assert id-fpki-common-cardAuth shall only be used to authenticate the hardware token containing the associated private key and shall not be interpreted as authenticating the presenter or holder of the token.

1.5. POLICY ADMINISTRATION

1.5.1. Organization Administering the Document

The Federal PKI Policy Authority is responsible for all aspects of this CP.

1.5.2. Contact Person

Questions regarding this CP shall be directed to the Chair of the Federal PKI Policy Authority, whose address can be found at http://www.idmanagement.gov/fpkipa

1.5.3. Person Determining CPS Suitability for the Policy

The FPKIPA shall approve the CPS for each CA that issues certificates under this policy.

1.5.4. CPS Approval Procedures

CAs issuing under this policy are required to meet all facets of the policy. The FPKIPA will not issue waivers.

The FPKIPA shall make the determination that a CPS complies with this policy. The CA and RA must meet all requirements of an approved CPS before commencing operations. In some cases, the FPKIPA may require the additional approval of an authorized agency. The FPKIPA will make this determination based on the nature of the system function, the type of communications, or the operating environment.

In each case, the determination of suitability shall be based on an independent compliance auditor's results and recommendations. See section 8 for further details.

1.6. DEFINITIONS AND ACRONYMS

See sections 11 and 12.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

All CAs that issue certificates under this policy are obligated to post all CA certificates issued by or to the CA and CRLs issued by the CA in a repository that is publicly accessible through all Uniform Resource Identifier (URI) references asserted in valid certificates issued by that CA. Specific requirements are found in *Shared Service Provider Repository Service Requirements* [SSP REP]. CAs may optionally post subscriber certificates in this repository in accordance with agency policy, except as noted in section 9.4.3. To promote consistent access to certificates and

CRLs, the repository shall implement access controls and communication mechanisms to prevent unauthorized modification or deletion of information.

Posted certificates and CRLs may be replicated in additional repositories for performance enhancement. Such repositories may be operated by the CA or other parties (e.g., Federal agencies).

2.2. PUBLICATION OF CERTIFICATION INFORMATION

2.2.1. Publication of Certificates and Certificate Status

The publicly accessible repository system shall be designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually. Where applicable, the certificate status server (CSS) shall be designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually.

2.2.2. Publication of CA Information

The Common Policy CP shall be publicly available on the FPKIPA website (see http://www.idmanagement.gov/fpkipa). The CPS for the Common Policy Root CA will not be published; a redacted version of this CPS will be publicly available from the FPKIMA website (See http://www.idmanagement.gov/fpkima).

> Practice Note: There is no requirement for the publication of CPSs of other CAs that issue certificates under this policy.

2.2.3. Interoperability

Where certificates and CRLs are published in directories, standards-based schemas for directory objects and attributes shall be used as specified in the *Shared Service Provider Repository Service Requirements* [SSP-REP].

2.3. TIME OR FREQUENCY OF PUBLICATION

This CP and any subsequent changes shall be made publicly available within thirty days of approval.

Publication requirements for CRLs are provided in sections 4.9.7 and 4.9.12

2.4. ACCESS CONTROLS ON REPOSITORIES

The CA shall protect information not intended for public dissemination or modification. CA certificates and CRLs in the repository shall be publicly available through the Internet. Direct and/or remote access to other information in the CA repositories shall be determined by agencies pursuant to their authorizing and controlling statutes. The CPS shall detail what information in the repository shall be exempt from automatic availability and to whom, and under which conditions the restricted information may be made available.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

For certificates issued under id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-High, id-fpki-common-devices and id-fpki-common-devicesHardware the CA shall assign X.501 distinguished names to all subscribers. These distinguished names may be in either of two forms: a geo-political name or an Internet domain component name.

All geo-political distinguished names assigned to federal employees shall be in the following directory information tree:

- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*]

The organizational units *department* and *agency* appear when applicable and are used to specify the federal entity that employs the subscriber. At least one of these organizational units must appear in the DN. The additional organizational unit *structural_container* is permitted to support local directory requirements, such as differentiation between human subscribers and devices. This organizational unit may not be employed to further differentiate between subcomponents within an agency.

The distinguished name of the federal employee subscriber shall take one of the three following forms:

- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*nickname lastname*
- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*firstname initial. lastname*
- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*firstname middlename lastname*

In the first name form, *nickname* may be the subscriber's first name, a form of the first name, middle name, or pseudonym (e.g., Buck) by which the subscriber is generally known. A generational qualifier, such as "Sr." or "III", may be appended to any of the common name forms specified above.

Distinguished names assigned to federal contractors and other affiliated persons shall be within the same directory information tree. The distinguished name of the federal contractor subscribers and affiliate subscribers will take one of the three following forms:

- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*nickname lastname* (affiliate)
- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*firstname initial. lastname* (affiliate)
- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*firstname middlename lastname* (affiliate)

For names assigned to federal contractors and other affiliated persons, generational qualifiers may be inserted between *lastname* and "(affiliate)".

Common name fields shall be populated as specified above.

Distinguished names based on Internet domain component names shall be in the following directory information trees:

- dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*]
- dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*]

The default Internet domain name for the agency, [*orgN*.]…[*org0*].gov or [*orgN*.]…[*org0*].mil, will be used to determine DNs. The first domain component of the DN will either be dc=gov or dc=mil. At a minimum, the *org0* domain component must appear in the DN. The *org1* to *orgN* domain components appear, in order, when applicable and are used to specify the federal entity that employs the subscriber.

The distinguished name of the federal employee subscriber shall take one of the three following forms when their agency's Internet domain name ends in .gov:

- dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*nickname lastname*
- dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*firstname initial. lastname*
- dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*firstname middlename lastname*

The distinguished name of the federal contractors and affiliated subscribers shall take one of the three following forms when the agency's Internet domain name ends in .gov:

- dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*nickname lastname* (affiliate)
- dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*firstname initial. lastname* (affiliate)
- dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*firstname middlename lastname* (affiliate)

The distinguished name of the federal employee subscriber shall take one of the three following forms when their agency's Internet domain name ends in .mil:

- dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*nickname lastname*
- dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*firstname initial. lastname*
- dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*firstname middlename lastname*

The distinguished name of the federal contractors and affiliated subscribers shall take one of the three following forms when the agency's Internet domain name ends in .mil:

- dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*nickname lastname* (affiliate)
- dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*firstname initial. lastname* (affiliate)
- dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*firstname middlename lastname* (affiliate)

The CA may supplement any of the name forms for users specified in this section by including a dnQualifier, serial number, or user id attribute. When any of these attributes are included, they may appear as part of a multi-valued relative distinguished name (RDN) with the common name or as a distinct RDN that follows the RDN containing the common name attribute. Generational qualifiers may optionally be included in common name attributes in distinguished names based on Internet domain names. For names assigned to employees, generational qualifiers may be appended to the common name. For names assigned to federal contractors and other affiliated persons, generational qualifiers may be inserted between *lastname* and "(affiliate)".

Signature certificates issued under id-fpki-common-hardware or id-fpki-common-High may be issued with a common name that specifies an organizational role, such as the head of an agency, as follows:

- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*role* [, *department/agency*]
- dc=gov, dc=…, [ou=*structural_container*], cn=*role* [, *department/agency*]

The combination of organizational role and agency must unambiguously identify a single person. (That is, widely held roles such as *Computer Scientist* or *Procurement Specialist* cannot be included since they do not identify a particular person. *Chief Information Officer, AgencyX* could be included as it specifies a role held by a single person.)

Where the [department/agency] is implicit in the role (e.g., Secretary of Commerce), it should be omitted. Where the role alone is ambiguous (e.g., Chief Information Officer) the department/agency must be present in the common name. The organizational information in the common name must match that in the organizational unit attributes.

> Practice Note: In the case of "Chief Information Officer", use of department/agency in the common name is redundant but is included for usability purposes. Display of the common name is widely supported in applications. Other attributes may or may not be presented to users.

Devices that are the subject of certificates issued under this policy shall be assigned either a geo-political name or an Internet domain component name. Device names shall take one of the following forms:

- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=*structural_container*], cn=*device name*
- dc=gov, dc=*org0*, [*dc=org1*], …, [dc=*orgN*], [ou=*structural_container*], [cn=*device name*]
- dc=mil, dc=*org0*, [*dc=org1*], …, [dc=*orgN*], [ou=*structural_container*], [cn=*device name*]

where *device name* is a descriptive name for the device. Where a device is fully described by the Internet domain name, the common name attribute is optional.

This policy does not restrict the directory information tree for names of CAs and CSSs. However, CAs that issue certificates under this policy must have distinguished names. CA and CSS distinguished names may be either a geo-political name or an Internet domain component name.

CA and CSS geo-political distinguished names shall be composed of any combination of the following attributes: country; organization; organizational unit; and common name. Internet domain component names are composed of the following attributes: domain component; organizational unit; and common name.

For certificates issued under id-fpki-common-authentication, assignment of X.500 distinguished names is mandatory. For certificates issued under this policy by a CA operating as part of the Shared Service Providers program, distinguished names shall follow either the rules specified above for id-fpki-common-hardware or the rules specified below for including a non-NULL subject DN in id-fpki-common-cardAuth. For legacy Federal PKIs only, distinguished names may follow established agency naming conventions. Certificates issued under id-fpki-common-authentication shall include a subject alternative name. At a minimum, the subject alternative name extension shall include the pivFASC-N name type [FIPS 201-1]. The value for this name shall be the FASC-N [PACS] of the subject's PIV card.

Certificates issued under id-fpki-common-cardAuth shall include a subject alternative name extension that includes the pivFASC-N name type. The value for this name shall be the FASC-N of the subject's PIV card. Certificates issued under id-fpki-common-cardAuth may also include a UUID [RFC 4122] in the subject alternative name extension, if the UUID is included as specified in Section 3.3 of [SP 800-73-3(1)]. Certificates issued under id-fpki-common-cardAuth shall not include any other name in the subject alternative name extension but may include a non-NULL name in the subject field. If included, the subject distinguished name shall take one of the following forms:

- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], serialNumber=*FASC-N*
- dc=gov, dc=*org0*, [*dc=org1*], …, [dc=*orgN*], [ou=*structural_container*], serialNumber=*FASC-N*
- dc=mil, dc=*org0*, [*dc=org1*], …, [dc=*orgN*], [ou=*structural_container*], serialNumber=*FASC-N*
- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], serialNumber=*UUID*
- dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], serialNumber=*UUID*
- dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], serialNumber=*UUID*

Practice Note: The FASC-N [PACS] consists of 40 decimal digits that are encoded as a 25-byte binary value. This 25-byte binary value may be encoded directly into the pivFASC-N name type in the subject alternative name extension, but when included in the subject field the FASC-N must be encoded as a PrintableString that is at most 64 characters long. This policy does not mandate any particular method for encoding the FASC-N within the serial number attribute as long as the same encoding method is used for all certificates issued by a CA. Acceptable methods for encoding the FASC-N within the serial number attribute include encoding the 25-byte binary value as 50 bytes of ASCII HEX or encoding the 40 decimal digits as 40 bytes of ASCII decimal.

Practice Note: When the UUID appears in the subjectAltName extension of a certificate, it must be encoded as a uniformResourceIdentifier as specified in Section 3 of [RFC 4122]. An example of a UUID encoded as a URI, from RFC 4122, is "urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6". This policy does not mandate any particular method for encoding the UUID within the serial number attribute as long as the same encoding method is used for all certificates issued by the CA and it is encoded as a PrintableString that is at most 64 characters long, however, it is recommended that the string representation from Section 3 of [RFC 4122] be used. An example would be "f81d4fae-7dec-11d0-a765-00a0c91e6bf6".

3.1.2. Need for Names to Be Meaningful

The subscriber certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by relying parties. Names used in the certificates must identify in a meaningful way the subscriber to which they are assigned.

The common name in the DN must represent the subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name, so the preferred common name form is

cn=*firstname initial. lastname*

While the issuer name in CA certificates is not generally interpreted by relying parties, this CP still requires use of meaningful names by CAs issuing under this policy. If included, the common name should describe the issuer, such as:

cn=*AgencyX CA-3*

The subject name in CA certificates must match the issuer name in certificates issued by the subject, as required by RFC 3280.

3.1.3. Anonymity or Pseudonymity of Subscribers

The CA shall not issue anonymous certificates. Pseudonymous certificates may be issued by the CA to support internal operations. CAs may also issue pseudonymous certificates that identify

subjects by their organizational roles, as described in section 3.1.1. CA certificates issued by the CA shall not contain anonymous or pseudonymous identities.

3.1.4. Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in X.501. Rules for interpreting e-mail addresses are specified in [RFC 2822]. Rules for interpreting the pivFASC-N name type are specified in [PACS].

3.1.5. Uniqueness of Names

Name uniqueness for certificates issued by each CA must be enforced. Each CA and its associated RAs shall enforce name uniqueness within the X.500 name space. When other name forms are used, they too must be allocated such that name uniqueness is ensured for certificates issued by that CA. Name uniqueness is not violated when multiple certificates are issued to the same entity.

> Practice Note: For distinguished names, name uniqueness is enforced for the entire name rather than a particular attribute (e.g., the common name).

The CPS shall identify the method for the assignment of subject names. Directory information trees may be assigned to a single CA, or shared between CAs. Where multiple CAs share a single directory information tree, the FPKIPA shall review and approve the method for assignment of subject names.

3.1.6. Recognition, Authentication, and Role of Trademarks

CAs operating under this policy shall not issue a certificate knowing that it infringes the trademark of another. The FPKIPA shall resolve disputes involving names and trademarks.

3.2. INITIAL IDENTITY VALIDATION

3.2.1. Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys, that party shall be required to prove possession of the private key, which corresponds to the public key in the certificate request. For signature keys, this may be done by the entity using its private key to sign a value supplied by the CA. The CA shall then validate the signature using the party's public key. The FPKIPA may allow other mechanisms that are at least as secure as those cited here.

In the case where key generation is performed under the CA or RA's direct control, proof of possession is not required.

3.2.2. Authentication of Organization Identity

Requests for CA certificates shall include the CA name, address, and documentation of the existence of the CA. Before issuing CA certificates, an authority for the issuing CA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the CA.

3.2.3. Authentication of Individual Identity

This policy allows a certificate to be issued only to a single entity. Certificates shall not be issued that contain a public key whose associated private key is shared.

3.2.3.1 Authentication of Human Subscribers

Procedures used by agencies to issue identification to their own personnel and affiliates may be more stringent than that set forth below. When this is the case, the agency procedures for authentication of personnel shall apply in addition to the guidance in this section.

The RA shall ensure that the applicant's identity information is verified. Identity shall be verified no more than 30 days before initial certificate issuance. At id-fpki-common-High, the applicant shall appear at the RA in person. For all other policies, RAs may accept authentication of an applicant's identity attested to and documented by a trusted agent to support identity proofing of remote applicants, assuming agency identity badging requirements are otherwise satisfied. Authentication by a trusted agent does not relieve the RA of its responsibility to perform steps 1), 2), the verification of identifying information (e.g., by checking official records) in step 3), and the maintenance of biometrics in step 4), below.

At a minimum, authentication procedures for employees must include the following steps:

1) Verify that a request for certificate issuance to the applicant was submitted by agency management.
2) Verify Applicant's employment through use of official agency records.
3) Establish applicant's identity by in-person proofing before the registration authority, based on either of the following processes:
    a) Process #1:
        i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and
        ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and
        iii) The credential presented in step 3) a) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying a database maintained by the organization that issued the credential, but other equivalent methods may be used.
    b) Process #2:
        i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and
        ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

iii) The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The identifying information (e.g., name and address) on the credential presented in step 3) b) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid).

> Practice Note: This may be accomplished by querying a database maintained by the organization that issued the financial instrument or through use of a commercial credit database. In some instances, commercial credit card databases will validate name and address of current cardholders on-line; this validation is acceptable if the card is presented to the RA. Other methods may be accepted.

4) Record and maintain a biometric of the applicant (e.g., a photograph or fingerprint) by the RA or CA. (Handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this policy.) This establishes an audit trail for dispute resolution.

For contractors and other affiliated personnel, the authentication procedures must include the following steps:

1) Verify that a request for certificate issuance to the applicant was submitted by an authorized sponsoring agency employee (e.g., contracting officer or contracting officer's technical representative).
2) Verify sponsoring agency employee's identity and employment through either one of the following methods:
   a) A digitally signed request from the sponsoring agency employee, verified by a currently valid employee signature certificate issued by an agency CA, may be accepted as proof of both employment and identity,
   b) Authentication of the sponsoring agency employee with a valid employee PIV-authentication certificate issued by the agency may be accepted as proof of both employment and identity, or
   c) In-person identity proofing of the sponsoring agency employee may be established before the registration authority as specified in employee authentication above and employment validated through use of the official agency records.
3) Establish applicant's identity by in-person proofing before the registration authority, based on either of the following processes:
   a) Process #1:
      i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and
      ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and
      iii) The credential presented in step 3) a) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is

accomplished by querying official records maintained by the organization that issued the credential.

b) Process #2:

i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and

ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

iii) The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The identifying information (e.g., name and address) on the credential presented in step 3) b) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid).

> Practice note: This may be accomplished by querying a database maintained by the organization that issued the financial instrument or through use of a commercial credit database. In some instances, commercial credit card databases will validate name and address of current cardholders on-line; this validation is acceptable if the card is presented to the RA. Other methods may be accepted.

4) Record and maintain a biometric of the applicant (e.g., a photograph or fingerprint) by the RA or CA. (Handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this policy.) This establishes an audit trail for dispute resolution.

Additionally, the RA shall record the process that was followed for issuance of each certificate. The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the Applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury);
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The biometric of the applicant;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).

FIPS 201 imposes the strict requirement of in-person registration. The following text only applies to the issuance of non-FIPS 201 credentials:

For all certificate policies except id-fpki-common-High, where it is not possible for applicants to appear in person before the RA, a trusted agent may serve as proxy for the RA. The trusted agent forwards the information collected from the applicant directly to the RA in a secure manner. The requirement for recording a biometric of the applicant may be satisfied by providing passport-style photographs to the trusted agent. The trusted agent shall verify the photographs against the appearance of the applicant and the biometrics on the presented credentials and securely incorporate the biometric as a component in the notarized package. Packages secured in a tamper-evident manner by the trusted agent satisfy this requirement; other secure methods are also acceptable.

3.2.3.2 Authentication of Devices

Some computing and communications devices (routers, firewalls, servers, etc.) and software applications will be named as certificate subjects. In such cases, the device must have a human sponsor. The sponsor is responsible for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name) or unique software application name
- Equipment or software application public keys
- Equipment or software application authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the sponsor when required.

The identity of the sponsor shall be authenticated by:

- Verification of digitally signed messages sent from the sponsor using a certificate issued under this policy; or
- In-person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of section 3.2.3.1.

3.2.4. Non-verified Subscriber Information

Information that is not verified shall not be included in certificates.

3.2.5. Validation of Authority

Before issuing CA certificates or signature certificates that assert organizational authority, the CA shall validate the individual's authority to act in the name of the organization. For pseudonymous certificates that identify subjects by their organizational roles, the CA shall validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

Practice Note: Examples of signature certificates that assert organizational authority are code signing certificates and FIPS 201 id-PIV-content-signing certificates.

3.2.6. Criteria for Interoperation

The FPKIPA shall determine the interoperability criteria for CAs operating under this policy.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-key

CA certificate re-key shall follow the same procedures as initial certificate issuance.

For re-key of subscriber certificates issued under id-fpki-common-High, identity may be established through use of current signature key, except that identity shall be established through an in-person registration process at least once every three years from the time of initial registration.

For policies other than id-fpki-common-High, a subscriber's identity may be established through use of current signature key, except that identity shall be re-established through an in-person registration process at least once every nine years from the time of initial registration.

For device certificates, identity may be established through the use of the device's current signature key, the signature key of the device's human sponsor, except that identity shall be established through the initial registration process at least once every nine years from the time of initial registration.

3.3.2. Identification and Authentication for Re-key after Revocation

In the event of certificate revocation, issuance of a new certificate shall always require that the party go through the initial registration process per section 3.2 above.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

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

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. *CERTIFICATE APPLICATION*

The Certificate application process must provide sufficient information to:

- Establish the applicant's authorization (by the employing or sponsoring agency) to obtain a certificate. (per section 3.2.3)
- Establish and record identity of the applicant. (per section 3.2.3)
- Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required. (per section 3.2.1)
- Verify any role or authorization information requested for inclusion in the certificate.

These steps may be performed in any order that is convenient for the PKI Authorities and applicants that does not defeat security, but all must be completed before certificate issuance.

4.1.1. Who Can Submit a Certificate Application

4.1.1.1 CA Certificates

An application for a CA certificate shall be submitted by an authorized representative of the applicant CA.

4.1.1.2 User Certificates

An application for a user (subscriber) certificate shall be submitted by either the applicant or a trusted agent.

4.1.1.3 Device Certificates

An application for a device certificate shall be submitted by the human sponsor of the device.

4.1.2. Enrollment Process and Responsibilities

All communications among PKI Authorities supporting the certificate application and issuance process shall be authenticated and protected from modification; any electronic transmission of shared secrets shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used. Out-of-band communications shall protect the confidentiality and integrity of the data.

Subscribers are responsible for providing accurate information on their certificate applications.

4.2. *CERTIFICATE APPLICATION PROCESSING*

Information in certificate applications must be verified as accurate before certificates are issued. PKI Authorities shall specify procedures to verify information in certificate applications.

4.2.1. Performing Identification and Authentication Functions

The identification and authentication of the subscriber must meet the requirements specified for subscriber authentication as specified in sections 3.2 and 3.3 of this CP. The PKI Authority must identify the components of the PKI Authority (e.g., CA or RA) that are responsible for authenticating the subscriber's identity in each case.

4.2.2. Approval or Rejection of Certificate Applications

For the Common Policy Root CA, the FPKIPA may approve or reject a certificate application.

For CAs operating under this policy, approval or rejection of certificate applications is at the discretion of the Agency PMA or its designee.

4.2.3. Time to Process Certificate Applications

Certificate applications must be processed and a certificate issued within 30 days of identity verification.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions During Certificate Issuance

Upon receiving the request, the CAs/RAs will—

- Verify the identity of the requester.
- Verify the authority of the requester 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 an RA, have the CA sign the certificate).
- Make the certificate available to the subscriber after confirming that the subscriber has formally acknowledged their obligations as described in section 9.6.3.

The certificate request may already contain a certificate built by either the RA or the subscriber. This certificate will not be signed until all verifications and modifications, if any, have been completed to the CA's satisfaction.

All authorization and other attribute information received from a prospective subscriber shall be verified before inclusion in a certificate. The responsibility for verifying prospective subscriber data shall be described in a CA's CPS.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

CAs operating under this policy shall inform the subscriber (or other certificate subject) of the creation of a certificate and make the certificate available to the subscriber. For device certificates, the CA shall inform the human sponsor.

4.4. CERTIFICATE ACCEPTANCE

Before a subscriber can make effective use of its private key, a PKI Authority shall explain to the subscriber its responsibilities as defined in section 9.6.3.

4.4.1. Conduct Constituting Certificate Acceptance

For the Common Policy Root CA, failure to object to the certificate or its contents shall constitute acceptance of the certificate.

For all other CAs operating under this policy, no stipulation.

4.4.2. Publication of the Certificate by the CA

As specified in 2.1, all CA certificates shall be published in repositories.

This policy makes no stipulation regarding publication of subscriber certificates, except as noted in section 9.4.3.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

The Federal PKI Policy Authority must be notified whenever a CA operating under this policy issues a CA certificate.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and Certificate Usage

The intended scope of usage for a private key is specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

4.5.2. Relying Party Public key and Certificate Usage

Common Policy-issued certificates specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. All CAs operating under this policy shall issue CRLs specifying the current status of all unexpired certificates (except for OCSP responder certificates that include the id-pkix-ocsp-nocheck extension). It is recommended that relying parties process and comply with this information whenever using Common Policy certificates in a transaction.

4.6. CERTIFICATE RENEWAL

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.6.1. Circumstance for Certificate Renewal

Subscriber certificates issued under this policy shall not be renewed, except during recovery from CA key compromise (see 5.7.3). In such cases, the renewed certificate shall expire as specified in the original subscriber certificate.

CA Certificates and OCSP responder certificates may be renewed so long as the aggregated lifetime of the public key does not exceed the certificate lifetime specified in section 6.3.2.

The CA may automatically renew certificates during recovery from key compromise.

4.6.2. Who May Request Renewal

For all CAs and OCSP responders operating under this policy, the corresponding operating authority may request renewal of its own certificate. For the Common Policy Root CA, the FPKI MA may also request renewal of CA certificates.

4.6.3. Processing Certificate Renewal Requests

For the Common Policy Root CA, CA certificate renewal for reasons other than re-key of the Common Policy Root CA shall be approved by the FPKIPA.

For all other renewal requests, no stipulation.

4.6.4. Notification of New Certificate Issuance to Subscriber

The CA shall inform the subscriber of the renewal of his or her certificate and the contents of the certificate.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

For certificates issued by the Common Policy Root CA, failure to object to the renewal of the certificate or its contents constitutes acceptance of the certificate.

For all other CAs operating under this policy, no stipulation.

4.6.6. Publication of the Renewal Certificate by the CA

As specified in Section 2.1, all CA certificates shall be published in repositories.

This policy makes no stipulation regarding publication of subscriber certificates, except as noted in section 9.4.3.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7. CERTIFICATE RE-KEY

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. Re-key of a certificate does not require a change to the subjectName and does not violate the requirement for name uniqueness. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

Subscribers shall identify themselves for the purpose of re-keying as required in section 3.3.

4.7.1. Circumstance for Certificate Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a subscriber periodically obtain new keys. (Section 6.3.2 establishes usage periods for private keys for both CAs and subscribers.) Examples of circumstances requiring certificate re-key include: expiration, loss or compromise, issuance of a new hardware token, and hardware token failure.

4.7.2. Who May Request Certification of a New Public Key

Requests for certification of a new public key shall be considered as follows:

Subscribers with a currently valid certificate may request certification of a new public key. CAs and RAs may request certification of a new public key on behalf of a subscriber. For device certificates, the human sponsor of the device may request certification of a new public key.

4.7.3. Processing Certificate Re-keying Requests

Digital signatures on subscriber re-key requests shall be validated before electronic re-key requests are processed. Alternatively, subscriber re-key requests may be processed using the same process used for initial certificate issuance.

4.7.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

For certificates issued by the Common Policy Root CA, failure to object to the certificate or its contents constitutes acceptance of the certificate.

For all other CAs operating under this policy, no stipulation.

4.7.6. Publication of the Re-keyed Certificate by the CA

All CA certificates must be published as specified in section 2.1.

This policy makes no stipulation regarding publication of subscriber certificates, except as noted in section 9.4.3.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8. CERTIFICATE MODIFICATION

Modifying a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.8.1. Circumstance for Certificate Modification

A CA operating under this policy may modify a CA or OCSP responder certificate whose characteristics have changed (e.g. assert new policy OID). The new certificate may have the same or a different subject public key.

A CA may perform certificate modification for a subscriber whose characteristics have changed (e.g., name change due to marriage). The new certificate shall have a different subject public key.

4.8.2. Who May Request Certificate Modification

Requests for certification of a new public key shall be considered as follows:

Subscribers with a currently valid certificate may request certificate modification. CAs and RAs may request certificate modification on behalf of a subscriber. For device certificates, the human sponsor of the device may request certificate modification.

4.8.3. Processing Certificate Modification Requests

If an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or other designated agent in order for a certificate with the new name to be issued. If an individual's authorizations or privileges change, the RA will verify those authorizations. If authorizations have reduced, the old certificate must be revoked.

Proof of all subject information changes must be provided to the RA or other designated agent and verified before the modified certificate is issued.

4.8.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

For certificates issued by the Common Policy Root CA, failure to object to the certificate or its contents constitutes acceptance of the certificate.

For all other CAs operating under this policy, no stipulation

4.8.6. Publication of the Modified Certificate by the CA

All CA certificates must be published as specified in section 2.1.

This policy makes no stipulation regarding publication of subscriber certificates, except as noted in section 9.4.3.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

CAs operating under this policy shall issue CRLs covering all unexpired certificates issued under this policy except for OCSP responder certificates that include the id-pkix-ocsp-nocheck extension.

CAs operating under this policy 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.

Revocation requests must be authenticated. 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**.**

Certificate suspension for CA certificates is not allowed by this policy. However, the use of certificate suspension for end entity certificates is allowed.

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 the 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 becomes 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.
- There is reason to believe the private key has been compromised.
- The subscriber or other authorized party (as defined in the 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. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

4.9.2. Who Can Request Revocation

Within the PKI, a CA may summarily revoke certificates within its domain. A written notice and brief explanation for the revocation shall subsequently be provided to the subscriber. The RA can request the revocation of a subscriber's certificate on behalf of any authorized party as specified in the CPS. A subscriber may request that its own certificate be revoked. The human sponsor of a device can request the revocation of the device's certificate. Other authorized agency officials may request revocation as described in the CPS.

4.9.3. Procedure for Revocation Request

A request to revoke a certificate 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). The steps involved in the process of requesting a certification revocation are detailed in the CPS.

Where subscribers use hardware tokens, revocation is optional if all the following conditions are met:

- the revocation request was not for key compromise;
- the hardware token does not permit the user to export the signature private key;
- the subscriber surrendered the token to the PKI;
- the token was zeroized or destroyed promptly upon surrender;
- the token has been protected from malicious use between surrender and zeroization or destruction.

In all other cases, revocation of the certificates is mandatory. Even where all the above conditions have been met, revocation of the associated certificates is recommended.

4.9.4. Revocation Request Grace Period

There is no grace period for revocation under this policy.

4.9.5. Time within which CA must Process the Revocation Request

CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published, excepting those requests received within two hours of CRL issuance. Revocation requests received within two hours of CRL issuance shall be processed before the following CRL is published.

4.9.6. Revocation Checking Requirements for Relying Parties

No stipulation.

> Practice note: Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the relying party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.9.7. CRL Issuance Frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below.

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote (laptop) operation.

CAs operating as part of the Shared Service Providers program that only issue certificates to CAs and that operate off-line must issue CRLs at least once every 24 hours, and the *nextUpdate* time in the CRL may be no later than 48 hours after issuance time (i.e., the *thisUpdate* time). For legacy Federal PKIs only, CAs that only issue certificates to CAs and that operate off-line must issue CRLs at least once every 31 days, and the *nextUpdate* time in the CRL may be no later than 32 days after issuance time (i.e., the *thisUpdate* time).

CAs that issue certificates to subscribers or operate on-line must issue CRLs at least once every 18 hours, and the *nextUpdate* time in the CRL may be no later than 48 hours after issuance time (i.e., the *thisUpdate* time). For legacy Federal PKIs only, the *nextUpdate* time in the CRL may be no later than 180 hours after issuance time (i.e., the *thisUpdate* time).

> Practice Note: Since many applications only check for a new CRL at nextUpdate, a longer nextUpdate time may result in applications continuing to rely on older CRLs even when a newer CRL is available. A longer nextUpdate time also increases the potential of a replay attack to validate a newly revoked certificate. Where the CRL nextUpdate exceeds 48 hours, relying parties should consider these risks and take appropriate measures to mitigate the risk. For high-risk, sensitive Relying Party applications suggested measures include configuring a preference for OCSP by applications, pre-fetching CRLs at least every 18 hours, and use of other compensating controls.

Circumstances related to emergency CRL issuance are specified in section 4.9.12.

4.9.8. Maximum Latency for CRLs

CRLs shall be published within 4 hours of generation. Furthermore, each CRL shall be published no later than the time specified in the *nextUpdate* field of the previously issued CRL for same scope.

4.9.9. On-line Revocation/Status Checking Availability

CAs shall support on-line status checking via OCSP [RFC 2560] for end entity certificates issued under id-fpki-common-authentication and id-fpki-common-cardAuth.

Where on-line status checking is supported, status information must be updated and available to relying parties within 18 hours of certificate revocation.

Where on-line status checking is supported and a certificate issued under id-fpki-common-High is revoked for key compromise, the status information must be updated and available to relying parties within 6 hours.

Since some relying parties cannot accommodate on-line communications, all CAs will be required to support CRLs.

4.9.10. On-line Revocation Checking Requirements

Relying party client software may optionally support on-line status checking. Client software using on-line status checking need not obtain or process CRLs.

4.9.11. Other Forms of Revocation Advertisements Available

A CA may also 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 CA's approved CPS;
- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.
- The alternative method must meet the 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

When a CA certificate is revoked a CRL must be issued within 18 hours of notification.

When a CA certificate issued under id-fpki-common-High is revoked or subscriber certificate issued under id-fpki-common-High is revoked because of compromise, or suspected compromise, of a private key, a CRL must be issued within 6 hours of notification.

4.9.13. Circumstances for Suspension

For CA certificates, suspension is not permitted.

For end entity certificates, no stipulation.

4.9.14. Who Can Request Suspension

No stipulation for end entity certificates.

4.9.15. Procedure for Suspension Request

No stipulation for end entity certificates.

4.9.16. Limits on Suspension Period

No stipulation for end entity certificates.

4.10. CERTIFICATE STATUS SERVICES

No stipulation.

4.10.1. Operational Characteristics

No stipulation.

4.10.2. Service Availability

No stipulation.

4.10.3. Optional Features

No stipulation.

4.11. END OF SUBSCRIPTION

No stipulation.

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key Escrow and Recovery Policy and Practices

CA private keys are never escrowed.

Subscriber key management keys may be escrowed to provide key recovery. CAs that support private key escrow for key management keys shall identify the document describing the practices in the applicable CPS. Escrowed keys shall be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber.

Under no circumstances shall a subscriber signature key be held in trust by a third party.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

CAs that support session key encapsulation and recovery shall identify the document describing the practices in the applicable CPS.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. PHYSICAL CONTROLS

CA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The CA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. CA cryptographic tokens shall be protected against theft, loss, and unauthorized use.

All the physical control requirements specified below apply equally to the Common Policy Root CA and subordinate CAs, and any remote workstations used to administer the CAs except where specifically noted.

5.1.1. Site Location and Construction

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

5.1.2. Physical Access

5.1.2.1 Physical Access for CA Equipment

At a minimum, the physical access controls for CA equipment, as well as remote workstations used to administer the CAs, shall—

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

When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA equipment shall be placed in secure containers. Activation data shall be either 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 or removable hardware associated with remote workstations used to administer the CA.

A security check of the facility housing the CA equipment or remote workstations used to administer the CAs shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when "open," and secured when "closed," and for the CA, that all equipment other than the repository is shut down).
- Any security containers are properly secured.
- Physical security systems (e.g., door locks, vent covers) are functioning properly.
- The area is secured against unauthorized access.

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

5.1.2.2 Physical Access for RA Equipment

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. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

5.1.2.3 Physical Access for CSS Equipment

Physical access control requirements for CSS equipment (if implemented), shall meet the CA physical access requirements specified in 5.1.2.1.

5.1.3. Power and Air Conditioning

The CA shall have backup capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown. The repositories (containing CA certificates and CRLs) shall be provided with uninterrupted power sufficient for a minimum of 6 hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4. Water Exposures

CA equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).

Potential water damage from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5. Fire Prevention and Protection

No stipulation.

5.1.6. Media Storage

Media shall be stored so as to protect them from accidental damage (e.g., water, fire, or electromagnetic) and unauthorized physical access.

5.1.7. Waste Disposal

Sensitive media and documentation that are no longer needed for operations shall be destroyed in a secure manner. For example, sensitive paper documentation shall be shredded, burned, or otherwise rendered unrecoverable.

5.1.8. Off-Site Backup

Full system backups sufficient to recover from system failure shall be made on a periodic schedule, and described in a CA's CPS. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an off-site location (separate from CA equipment). Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA.

For legacy Federal PKIs operating an offline CA, the full system backup shall be performed each time the system is turned on or once a week, whichever is less frequent.

Requirements for CA private key backup are specified in section 6.2.4.1.

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 extraordinarily responsible, or the integrity of the CA will be weakened. The functions performed in these roles form the basis of trust for the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The primary trusted roles defined in this policy are Administrator, Officer, Auditor, and Operator. Individual personnel shall be specifically designated to the four roles defined below. These four roles are employed at the CA, RA, and CSS locations as appropriate.

5.2.1.1 Administrator

The administrator role shall be responsible for:

- Installation, configuration, and maintenance of the CA and CSS (where applicable);
- Establishing and maintaining CA and CSS system accounts;
- Configuring certificate profiles or templates;
- Configuring CA, RA, and CSS audit parameters;
- Configuring CSS response profiles; and
- Generating and backing up CA and CSS keys.

Administrators do not issue certificates to subscribers.

5.2.1.2 Officer

The officer role shall be responsible for issuing certificates, that is:

- Registering new subscribers and requesting the issuance of certificates;
- Verifying the identity of subscribers and accuracy of information included in certificates;
- Approving and executing the issuance of certificates; and
- Requesting, approving and executing the revocation of certificates.

5.2.1.3 Auditor

The auditor role shall be responsible for:

- Reviewing, maintaining, and archiving audit logs; and
- Performing or overseeing internal compliance audits to ensure that the CA, associated RAs, and CSS (where applicable) are operating in accordance with its CPS.

5.2.1.4 Operator

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

5.2.2. Number of Persons Required per Task

Two or more persons are required for the following tasks:

- CA key generation;
- CA signing key activation;
- CA private key backup.

Where multiparty control is required, at least one of the participants shall be an Administrator. All participants must serve in a trusted role as defined in section 5.2.1. Multiparty control shall not be achieved using personnel that serve in the Auditor trusted role.

5.2.3. Identification and Authentication for Each Role

An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.2.4. Roles Requiring Separation of Duties

Individuals may only assume one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both the Administrator and Officer roles, assume both the Administrator and Auditor roles, or assume both the Auditor and Officer roles. For CAs that issue at id-fpki-common-High, the Auditor may not assume any other role. No individual shall have more than one identity.

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, Experience, and Clearance Requirements

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

5.3.2. Background Check Procedures

CA personnel shall, at a minimum, pass a background investigation covering the following areas:

- Employment;
- Education;
- Place of residence;
- Law Enforcement; and
- References.

The period of investigation must cover at least the last five years for each area, excepting the residence check which must cover at least the last three years. Regardless of the date of award, the highest educational degree shall be verified.

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

5.3.3. Training Requirements

All personnel performing duties with respect to the operation of the CA or RA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA (or RA) security principles and mechanisms;
- All PKI software versions in use on the CA (or RA) system;
- All PKI duties they are expected to perform;
- Disaster recovery and business continuity procedures; and
- Stipulations of this policy.

5.3.4. Retraining Frequency and Requirements

All individuals responsible for PKI roles shall be made aware of changes in the CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

The CA shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the CA or its RAs that are not authorized in this CP, CPSs, or other published procedures.

5.3.7. Independent Contractor Requirements

Contractors fulfilling trusted roles are subject to all personnel requirements stipulated in this policy.

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

5.3.8. Documentation Supplied to Personnel

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

5.4. AUDIT LOGGING PROCEDURES

Audit log files shall be generated for all events relating to the security of the CA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

5.4.1. Types of Events Recorded

All security auditing capabilities of CA operating system and CA applications shall be enabled during installation. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event;
- The date and time the event occurred;
- A success or failure indicator when executing the CA's signing process;
- A success or failure indicator when performing certificate revocation; and
- The identity of the entity and/or operator that caused the event.

A message from any source requesting an action by the CA is an auditable event; the corresponding audit record must also include message date and time, source, destination, and contents.

The CA shall record the events identified in the list below. Where these events cannot be electronically logged, the CA shall supplement electronic audit logs with physical logs as necessary.

- SECURITY AUDIT:
  - Any changes to the Audit parameters, e.g., audit frequency, type of event audited
  - Any attempt to delete or modify the Audit logs
  - Obtaining a third-party time-stamp
- IDENTIFICATION AND AUTHENTICATION:
  - Successful and unsuccessful attempts to assume a role
  - The value of maximum authentication attempts is changed
  - Maximum authentication attempts unsuccessful authentication attempts occur during user login
  - An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
  - An Administrator changes the type of authenticator, e.g., from password to biometrics
- LOCAL DATA ENTRY:
  - All security-relevant data that is entered in the system
- REMOTE DATA ENTRY:
  - All security-relevant messages that are received by the system
- DATA EXPORT AND OUTPUT:
  - All successful and unsuccessful requests for confidential and security-relevant information
- KEY GENERATION:
  - Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)
- PRIVATE KEY LOAD AND STORAGE:
  - The loading of Component private keys
  - All access to certificate subject private keys retained within the CA for key recovery purposes
- TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE:
  - All changes to the trusted public keys, including additions and deletions
- SECRET KEY STORAGE:
  - The manual entry of secret keys used for authentication
- PRIVATE AND SECRET KEY EXPORT:
  - The export of private and secret keys (keys used for a single session or message are excluded)
- CERTIFICATE REGISTRATION:

    - All certificate requests
- CERTIFICATE REVOCATION:
    - All certificate revocation requests
- CERTIFICATE STATUS CHANGE APPROVAL:
    - The approval or rejection of a certificate status change request
- CA CONFIGURATION:
    - Any security-relevant changes to the configuration of the CA
- ACCOUNT ADMINISTRATION:
    - Roles and users are added or deleted
    - The access control privileges of a user account or a role are modified
- CERTIFICATE PROFILE MANAGEMENT:
    - All changes to the certificate profile
- REVOCATION PROFILE MANAGEMENT:
    - All changes to the revocation profile
- CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT:
    - All changes to the certificate revocation list profile
- MISCELLANEOUS:
    - Appointment of an individual to a trusted role
    - Designation of personnel for multiparty control
    - Installation of the operating system
    - Installation of the CA
    - Installing hardware cryptographic modules
    - Removing hardware cryptographic modules
    - Destruction of cryptographic modules
    - System startup
    - Logon attempts to CA applications
    - Receipt of hardware / software
    - Attempts to set passwords
    - Attempts to modify passwords
    - Backing up CA internal database
    - Restoring CA internal database
    - File manipulation (e.g., creation, renaming, moving)

- Posting of any material to a repository
- Access to CA internal database
- All certificate compromise notification requests
- Loading tokens with certificates
- Shipment of tokens
- Zeroizing tokens
- Re-key of the CA
- Configuration changes to the CA server involving:
  - Hardware
  - Software
  - Operating system
  - Patches
  - Security profiles

- PHYSICAL ACCESS / SITE SECURITY:
  - Personnel access to room housing CA
  - Access to the CA server
  - Known or suspected violations of physical security
- ANOMALIES:
  - Software error conditions
  - Software check integrity failures
  - Receipt of improper messages
  - Misrouted messages
  - Network attacks (suspected or confirmed)
  - Equipment failure
  - Electrical power outages
  - Uninterruptible power supply (UPS) failure
  - Obvious and significant network service or access failures
  - Violations of certificate policy
  - Violations of certification practice statement
  - Resetting operating system clock

5.4.2. Frequency of Processing Log

For CAs that issue certificates under id-fpki-common-High, review of the audit log shall be required at least once every month. For CAs that do not issue certificates under id-fpki-common-High, review of the audit log shall be required at least once every two months.

Such reviews involve verifying that the log has not been tampered with and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. A statistically significant portion of the security audit data generated by the CA since the last review shall be examined. This amount will be described in the CPS.

All significant events shall be explained in an audit log summary. Actions taken as a result of these reviews shall be documented.

5.4.3. Retention Period for Audit Log

Audit logs shall be retained on-site for at least 2 months in addition to being archived as described in section 5.5. The individual who removes audit logs from the CA system shall be an official different from the individuals who, in combination, command the CA signature key.

5.4.4. Protection of Audit Log

The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing. CA system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data. Procedures must be implemented to protect archived data from deletion or destruction before 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 location where the data was generated.

5.4.5. Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least monthly. A copy of the audit log shall be sent off-site on a monthly basis.

5.4.6. Audit Collection System (Internal vs. External)

The audit log collection system may or may not be external to the CA system. Automated audit processes shall be invoked at system or application startup, and cease only at system or application shutdown. Audit collection systems shall be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files). Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, operations shall be suspended until the problem has been remedied.

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 CA will perform routine self-assessments of security controls.

> Practice Note: The security audit data should 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 should check for continuity of the security audit data.

5.5. RECORDS ARCHIVAL

The Common Policy CA must follow either the General Records Schedules established by the National Archives and Records Administration or an agency-specific schedule as applicable.

5.5.1. Types of Events Archived

CA archive records shall be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data shall be recorded for archive:

- CA accreditation (if applicable)
- Certificate policy
- Certification practice statement
- Contractual obligations
- and other agreements concerning operations of the CA
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- All certificates issued and/or published
- Record of re-key
- Revocation requests
- Subscriber identity authentication data as per section 3.2.3
- Documentation of receipt and acceptance of certificates (if applicable)
- Subscriber agreements
- Documentation of receipt of tokens
- All CRLs issued and/or published
- Other data or applications to verify archive contents
- Compliance Auditor reports

- Any changes to the Audit parameters, e.g. audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- Whenever the CA generates a key (Not mandatory for single session or one-time use symmetric keys)
- All access to certificate subject private keys retained within the CA for key recovery purposes
- All changes to the trusted public keys, including additions and deletions
- The export of private and secret keys (keys used for a single session or message are excluded)
- The approval or rejection of a certificate status change request
- Appointment of an individual to a Trusted Role
- Destruction of cryptographic modules
- All certificate compromise notifications
- Remedial action taken as a result of violations of physical security
- Violations of Certificate Policy
- Violations of Certification Practice Statement

5.5.2. Retention Period for Archive

For CAs that issue certificates under id-fpki-common-High, archive records must be kept for a minimum of 20 years and 6 months without any loss of data.

For CAs that do not issue certificates under id-fpki-common-High, archive records must be kept for a minimum of 10 years and 6 months without any loss of data.

5.5.3. Protection of Archive

No unauthorized user shall be permitted to write to, modify, or delete the archive. For the CA, archived records may be moved to another medium. The contents of the archive shall not be released except in accordance with sections 9.3 and 9.4. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the CA.

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.

Alternatively, a CA operating under this policy may retain data using whatever procedures have been approved by NARA for that category of documents. Applications required to process the archive data shall be maintained for a period that equals or exceeds the archive requirements for the data.

Prior to the end of the archive retention period, the FPKI Management Authority shall provide archived data and the applications necessary to read the archives to a Federal PKI Policy Authority approved archival facility, which shall retain the applications necessary to read this archived data.

5.5.4. Archive Backup Procedures

No stipulation.

5.5.5. Requirements for Time-Stamping of Records

CA 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 or 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, verify, package, transmit, and store the CA archive information, shall be published in the CPS.

5.6. KEY CHANGEOVER

To minimize risk from compromise of a CA's private signing key, that key may be changed often. From that time on, only the new key will be used to sign CA and subscriber certificates. If the old private key is used to sign OCSP responder certificates or CRLs that cover certificates signed with that key, the old key must be retained and protected.

The CA's signing key shall have a validity period as described in section 6.3.2.

When a CA updates its private signature key and thus generates a new public key, the CA shall notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed. When a CA that distributes self-signed certificates updates its private signature key, the CA shall generate key rollover certificates, where the new public key is signed by the old private key, and vice versa. This permits acceptance of newly issued certificates and CRLs without distribution of the new self-signed certificate to current users. Key rollover certificates are optional for CAs that do not distribute self-signed certificates. SSPs and Federal Legacy PKIs CAs cross certified with the Common Policy Root CA must be able to continue to interoperate with the Common Policy Root CA after the Common Policy Root CA performs a key rollover, whether or not the DN of the Common Policy Root CA is changed.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

The Federal PKI Policy Authority shall be notified if any CAs operating under this policy experience the following:

- suspected or detected compromise of the CA systems;
- suspected or detected compromise of a certificate status server (CSS) if (1) the CSS certificate has a lifetime of more than 72 hours and (2) the CSS certificate cannot be revoked (e.g., an OCSP responder certificate with the id-pkix-ocsp-nocheck extension);
- physical or electronic penetration of CA systems;
- successful denial of service attacks on CA components; or
- any incident preventing the CA from issuing a CRL within 48 hours of the issuance of the previous CRL.

The Federal PKI Policy Authority will take appropriate steps to protect the integrity of the Federal PKI.

The CA's Management Authority shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the CA's CPS.

5.7.2. Computing Resources, Software, and/or Data Are Corrupted

When computing resources, software, and/or data are corrupted, CAs operating under this policy shall respond as follows:

- Before returning to operation, ensure that the system's integrity has been restored.
- If the CA signature keys are not destroyed**,** CA operation shall be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in section 4.9.7.
- If the CA signature keys are destroyed**,** CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

The Agency PMA shall be notified as soon as possible.

5.7.3. Entity (CA) Private Key Compromise Procedures

In the event of a CA private key compromise, the following operations must be performed.

- The FPKIPA shall be immediately informed, as well as any superior or cross-certified CAs and any entities known to be distributing the CA certificate (e.g., in a root store).
- The CA must generate new keys in accordance with section 6.1.1.1.

If the CA distributed the private key in a Trusted Certificate, the CA shall perform the following operations:

- Generate a new Trusted Certificate.
- Securely distribute the new Trusted Certificate as specified in section 6.1.4.
- Initiate procedures to notify subscribers of the compromise.

Subscriber certificates may be renewed automatically by the CA under the new key pair (see section 4.6), or the CA may require subscribers to repeat the initial certificate application process.

5.7.4. Business Continuity Capabilities after a Disaster

For the Common Policy Root CA, recovery procedures shall be in place to reconstitute the CA within six (6) hours of failure.

All other CAs operating under this policy shall have recovery procedures in place to reconstitute the CA within 72 hours of failure.

In the case of a disaster whereby the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the FPKIPA shall be notified at the earliest feasible time, and the FPKIPA shall take whatever action it deems appropriate.

Relying parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of CA operation with new certificates.

5.8. CA OR RA TERMINATION

When a CA operating under this policy terminates operations before all certificates have expired, the CA signing keys shall be surrendered to the Federal PKI Policy Authority.

> Practice Note: This section does not apply to CAs that have ceased issuing new certificates but are continuing to issue CRLs until all certificates have expired. Such CAs are required to continue to conform with all relevant aspects of this policy (e.g., audit logging and archives).

Prior to CA termination, the CA shall provide archived data to an archive facility as specified in the CPS. As soon as possible, the CA will advise all other organizations to which it has issued certificates of its termination, using an agreed-upon method of communication specified in the CPS.

6. TECHNICAL SECURITY CONTROLS

6.1. *KEY PAIR GENERATION AND INSTALLATION*

6.1.1. Key Pair Generation

6.1.1.1 CA Key Pair Generation

Cryptographic keying material used by CAs to sign certificates, CRLs or status information shall be generated in FIPS 140 validated cryptographic modules. For CAs that issue certificates under id-fpki-common-High, the module(s) shall meet or exceed FIPS 140 Level 3. For CAs that do not issue certificates under id-fpki-common-High, the module(s) shall meet or exceed FIPS 140 Level 2. Multiparty control is required for CA key pair generation, as specified in section 6.2.2.

CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. An independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

> Practice Note: If the audit trail identifies and documents any failures or anomalies in the key generation process, along with the corrective action taken, the key generation process need not be restarted but may continue.

6.1.1.2 Subscriber Key Pair Generation

Subscriber key pair generation may be performed by the subscriber, CA, or RA. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in section 6.1.2 must also be met.

Validated software or hardware cryptographic modules shall be used to generate all subscriber key pairs, as well as pseudo-random numbers and parameters used in key pair generation. For the id-fpki-common-hardware, id-fpki-common-High, id-fpki-common-authentication, and id-fpki-common-cardauth policies, subscriber key pairs shall be generated in FIPS 140 Level 2 hardware cryptographic modules. Any pseudo-random numbers used for key generation material shall be generated by a FIPS-approved method. Symmetric keys may be generated by means of either software or hardware mechanisms.

> Practice Note: If the audit trail identifies and documents any failures or anomalies in the key generation process, along with the corrective action taken, the key generation process need not be restarted but may continue.

6.1.1.3 CSS Key Pair Generation

Cryptographic keying material used by CSSes to sign status information shall be generated in FIPS 140 validated cryptographic modules. For CSSes that provide status under id-fpki-common-High, the module(s) shall meet or exceed FIPS 140 Level 3. For CSSes that do not

provide status under id-fpki-common-High, the module(s) shall meet or exceed FIPS 140 Level 2.

6.1.2. Private Key Delivery to Subscriber

If subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

When CAs or RAs generate keys on behalf of the subscriber, then the private key must be delivered securely to the subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met:

- Anyone who generates a private signing key for a subscriber shall not retain any copy of the key after delivery of the private key to the subscriber.
- The private key(s) must be protected from activation, compromise, or modification during the delivery process.
- The subscriber shall acknowledge receipt of the private key(s).
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subscribers.
    - For hardware modules, accountability for the location and state of the module must be maintained until the subscriber accepts possession of it.
    - For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.

The CA must maintain a record of the subscriber acknowledgment of receipt of the token.

6.1.3. Public Key Delivery to Certificate Issuer

Where key pairs are generated by the subscriber or RA, the public key and the subscriber's identity must be delivered securely to the CA for certificate issuance. The delivery mechanism shall bind the subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate.

6.1.4. CA Public Key Delivery to Relying Parties

When a CA updates its signature key pair, the CA shall distribute the new public key in a secure fashion. The new public key may be distributed in a self-signed certificate, in a key rollover certificate, or in cross-certificates.

Self-signed certificates shall be conveyed to relying parties in a secure fashion to preclude substitution attacks. Acceptable methods for self-signed certificate delivery are:

- Loading a self-signed certificate onto tokens delivered to relying parties via secure mechanisms; such as

- The Trusted Certificate is loaded onto the token during the subscriber's appearance at the RA.
- The Trusted Certificate is loaded onto the token when the RA generates the subscriber's key pair and loads the private key onto the token, which is then delivered to the subscriber in accordance with section 6.1.2.

- Secure distribution of self-signed certificates through secure out-of-band mechanisms;
- Comparison of the hash of the self-signed certificate against a hash value made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and
- Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.

> Practice Note: Other methods that preclude substitution attacks may be considered acceptable.

Key rollover certificates are signed with the CA's current private key, so secure distribution is not required.

> Practice Note: To ensure the availability of the new public key, the key rollover certificates must be distributed using repositories.

6.1.5. Key Sizes

This CP requires use of RSA PKCS #1, RSASSA-PSS, or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy shall contain RSA or elliptic curve public keys.

> Practice Note: Future versions of this policy may specify additional FIPS-approved signature algorithms.

Trusted Certificates that expire before January 1, 2031 shall contain subject public keys of 2048 or 3072 bits for RSA or 256 or 384 bits for elliptic curve, and be signed with the corresponding private key. Trusted Certificates that expire on or after January 1, 2031 shall contain subject public keys of 3072 bits for RSA or 256 or 384 bits for elliptic curve, and be signed with the corresponding private key.

CAs that generate certificates and CRLs under this policy shall use signature keys of 1024, 2048, or 3072 bits for RSA and 256 or 384 bits for elliptic curve algorithms. Certificates that expire on or after December 31, 2010 shall be generated with 2048 or 3072 bit keys for RSA and 256 or 384 bit keys for elliptic curve algorithms. Certificates that expire after December 31, 2030 shall be generated with 3072 bit keys for RSA and 256 or 384 bit keys for elliptic curve algorithms.

Practice Note: Where certificates are issued to satisfy FIPS 201 requirements, CAs shall use signature keys of 2048 or 3072 bits for RSA and 256 or 384 bits for elliptic curve algorithms to sign certificates issued on or after January 1, 2008. CAs may continue to use 1024 bit RSA keys to sign CRLs that only cover certificates that were signed using 1024 bit RSA keys. CAs may also use 1024 bit RSA keys to sign OCSP responder certificates that expire before December 31, 2010.

CAs that generate certificates and CRLs under this policy shall use the SHA-1, SHA-256, or SHA-384 hash algorithm when generating digital signatures. RSA signatures on certificates and CRLs that are issued after December 31, 2010 shall be generated using SHA-256, however, RSA signatures on CRLs that are issued before January 1, 2012, and that include status information for certificates that were generated using SHA-1 may be generated using SHA-1. RSA signatures on CRLs that are issued on or after January 1, 2012, but before January 1, 2014 that only provide status information for certificates that were generated using SHA-1 may continue to be generated using SHA-1. ECDSA signatures on certificates and CRLs shall be generated using SHA-256 or SHA-384, as appropriate for the key length.

RSA signatures on certificates that are issued after December 31, 2010 and before January 1, 2014, to CAs that issued certificates prior to December 31, 2010 may be generated using SHA-1 provided that CA issues no additional end entity certificates. Additionally, certificates issued to OCSP responders that include SHA-1 certificates may be signed using SHA-1 until December 31, 2013. CAs that issue certificates signed with SHA-224 or SHA-256 after December 31, 2010 must not issue certificates signed with SHA-1.

Where implemented, CSSs shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs. After December 31, 2010, OCSP responders that generate signatures on OCSP responses using SHA-1 shall only provide signed responses that are pre-produced (i.e., any signed response that is provided to an OCSP client shall have been signed before the OCSP responder received the request from the client).

End entity certificates issued under id-fpki-common-devices that expire before December 31, 2010 shall contain RSA public keys that are 1024, 2048, or 3072 bits in length or elliptic curve keys that are 256 or 384 bits. End entity certificates issued under id-fpki-common-devices and id-fpki-common-devicesHardware that expire on or after December 31, 2010 shall contain RSA public keys that are 2048 or 3072 bits or elliptic curve keys that are 256 or 384 bits. End entity certificates issued under id-fpki-common-devices and id-fpki-common-devicesHardware that expire after December 31, 2030 shall contain RSA public keys that are 3072 bits or elliptic curve keys that are 256 or 384 bits.

End entity certificates issued under id-fpki-common-authentication or id-fpki-common-cardAuth that expire before January 1, 2014 shall contain RSA public keys that are 1024 or 2048 bits in length or elliptic curve keys that are 256 bits. End entity certificates issued under id-fpki-common-authentication or id-fpki-common-cardAuth that expire on or after January 1, 2014 shall contain RSA public keys that are 2048 bits in length or elliptic curve keys that are 256 bits.

End entity certificates issued under id-fpki-common-policy, id-fpki-common-hardware, and id-fpki-common-High shall contain RSA public keys that are 2048 or 3072 bits or elliptic curve keys that are 256 or 384 bits.

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require (1) triple-DES or AES for the symmetric key through December 31, 2010 and AES for the symmetric key after December 31, 2010 and (2) at least 1024 bit RSA or 163 bit elliptic curve keys through December 31, 2008, at least 2048 bit RSA or 224 bit elliptic curve keys after December 31, 2008, and 3072 bit RSA or at least 256 bit elliptic curve keys after December 31, 2030.

6.1.6. Public Key Parameters Generation and Quality Checking

Elliptic Curve public key parameters shall always be selected from the set specified in section 7.1.3.

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

The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates shall include a critical key usage extension.

Public keys that are bound into subscriber user certificates shall be used only for signing or encrypting, but not both. User certificates that assert id-fpki-common-authentication or id-fpki-common-cardAuth shall only assert the *digitalSignature* bit. Other user certificates to be used for digital signatures shall assert both the *digitalSignature* and *nonRepudiation* bits. User certificates that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit. User certificates that contain elliptic curve public keys that are to be used for key agreement shall assert the *keyAgreement* bit.

Public keys that are bound into CA certificates shall be used only for signing certificates and status information (e.g., CRLs). CA certificates whose subject public key is to be used to verify other certificates shall assert the *keyCertSign* bit. CA certificates whose subject public key is to be used to verify CRLs shall assert the *cRLSign* bit. CA certificates whose subject public key is to be used to verify Online Certificate Status Protocol (OCSP) responses shall assert the *digitalSignature* and/or *nonRepudiation* bits.

Public keys that are bound into device certificates may be used for digital signature (including authentication), key management, or both. Device certificates to be used for digital signatures shall assert the *digitalSignature* bit. Device certificates that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit. Device certificates that contain elliptic curve public keys that are to be used for key agreement shall assert the *keyAgreement* bit. Device certificates to be used for both digital signatures and key management shall assert the *digitalSignature* bit and either the *keyEncipherment* (for RSA) or *keyAgreement* (for elliptic curve) bit. Device certificates shall not assert the *nonRepudiation* bit.

The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits shall not be asserted in certificates issued under this policy.

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 *Security Requirements for Cryptographic Modules* [FIPS 140-2]. Cryptographic modules shall be validated to a FIPS 140 level identified in this section.

CAs that issue certificates under id-fpki-common-High shall use a FIPS 140 Level 3 or higher validated hardware cryptographic module. CAs that do not issue certificates under id-fpki-common-High shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module. RAs shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module. Subscribers shall use a FIPS 140 Level 1 or higher validated cryptographic module for all cryptographic operations. Subscribers issued certificates under the hardware users policy (id-fpki-common-hardware or id-fpki-common-devicesHardware), one of the authentication policies (id-fpki-common-authentication or id-fpki-common-cardAuth), or common High policy (id-fpki-common-High) shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module for all private key operations.

CSSes that provide status information for certificates issued under id-fpki-common-High shall use a FIPS 140 Level 3 or higher validated hardware cryptographic module. CSSes that do not provide status information for certificates issued under id-fpki-common-High shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module.

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

A single person shall not be permitted to activate or access any cryptographic module that contains the complete CA private signing key. CA signature keys may be backed up only under two-person control. Access to CA signing keys backed up for disaster recovery shall be under at least two-person control. 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.

6.2.3. Private Key Escrow

CA private keys are never escrowed.

Subscriber key management keys may be escrowed to provide key recovery as described in section 4.12.1. If a device has a separate key management key certificate, the key management private key may be escrowed.

6.2.4. Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

The CA private signature keys shall be backed up under the same multiperson control as the original signature key. At least one copy of the private signature key shall be stored off-site. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original. Backup procedures shall be included in the CA's CPS.

6.2.4.2 Backup of Subscriber Private Signature Key

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the id-fpki-common-authentication, id-fpki-common-cardAuth, or id-fpki-common-High policy shall not be backed up or copied.

Subscriber private signature keys whose corresponding public key is contained in a certificate that does not assert id-fpki-common-authentication, id-fpki-common-cardAuth, or id-fpki-common-High may be backed up or copied, but must be held in the subscriber's control. Backed up subscriber private signature keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

6.2.4.3 Backup of Subscriber Private Key Management Key

Backed up subscriber private key management keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

6.2.4.4 Backup of CSS Private Key

CSS private keys may be backed up. If backed up, all copies shall be accounted for and protected in the same manner as the original.

6.2.4.5 Backup of Device Private Keys

Device private keys may be backed up or copied, but must be held under the control of the device's human sponsor or other authorized administrator. Backed up device private keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the device's cryptographic module.

6.2.5. Private Key Archival

CA private signature keys and subscriber private signatures keys shall not be archived. CAs that retain subscriber private encryption keys for business continuity purposes shall archive such subscriber private keys, in accordance with section 5.5.

6.2.6. Private Key Transfer into or from a Cryptographic Module

CA private keys may be exported from the cryptographic module only to perform CA key backup procedures as described in section 6.2.4.1. At no time shall the CA private key exist in plaintext outside the cryptographic module.

All other keys shall 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.

6.2.7. Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS 140.

6.2.8. Method of Activating Private Key

For certificates issued under id-fpki-common-authentication, id-fpki-common-policy, id-fpki-common-hardware, and id-fpki-common-High, the subscriber must be authenticated to the cryptographic token before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to passphrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

For certificates issued under id-fpki-common-devices and id-fpki-common-devicesHardware, the device may be configured to activate its private key without requiring its human sponsor or authorized administrator to authenticate to the cryptographic token, provided that appropriate physical and logical access controls are implemented for the device and its cryptographic token. The strength of the security controls shall be commensurate with the level of threat in the device's environment, and shall protect the device's hardware, software, and the cryptographic token and its activation data from compromise.

For certificates issued under id-fpki-common-cardAuth, subscriber authentication is not required to use the associated private key.

6.2.9. Method of Deactivating Private Key

Cryptographic modules that have been activated shall not be available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure or automatically after a period of inactivity as defined in the applicable CPS. CA cryptographic modules shall be removed and stored in a secure container when not in use.

6.2.10. Method of Destroying Private Key

Individuals in trusted roles shall destroy CA, RA, and CSS (e.g., OCSP server) private signature keys when they are no longer needed. Subscribers shall either surrender their cryptographic module to CA/RA personnel for destruction or destroy their private signature keys, when they are no longer needed or when the certificates to which they correspond expire or are revoked. Physical destruction of hardware is not required.

Practice Note: Destruction will likely be performed by executing a "zeroize" command.

To ensure future access to encrypted data, subscriber private key management keys should be secured in long-term backups or archived.

6.2.11. Cryptographic Module Rating

See 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 Usage Periods

The usage period for the Common Policy Root CA key pair is a maximum of 20 years.

For all other CAs operating under this policy, the usage period for a CA key pair is a maximum of ten years. The CA private key may be used to sign certificates for at most four years, but may be used to sign CRLs and OCSP responder certificates for the entire usage period. All certificates signed by a specific CA key pair must expire before the end of that key pair's usage period.

Subscriber public keys in certificates that assert the id-PIV-content-signing OID in the extended key usage extension have a maximum usage period of eight years. The private keys corresponding to the public keys in these certificates have a maximum usage period of three years.

For OCSP responders operating under this policy and all other subscriber public keys, the maximum usage period is three years. Subscriber signature private keys have the same usage period as their corresponding public key. The usage period for subscriber key management private keys is not restricted.

6.4. ACTIVATION DATA

6.4.1. Activation Data Generation and Installation

CA activation data may be user-selected (by each of the multiple parties holding that activation data). If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

RA and subscriber activation data may be user-selected. The strength of the activation data shall meet or exceed the requirements for authentication mechanisms stipulated for Level 2 in FIPS 140-2. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2. Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data shall be:

- memorized;
- biometric in nature; or
- recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module.

Practice Note: Level 2 in FIPS 140-2 requires that the protection mechanism includes a facility to protect against repeated guessing attacks.

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Specific Computer Security Technical Requirements

Computer security controls are required to ensure CA/RA operations are performed as specified in this policy. The following computer security functions pertaining to the Common Policy Root CA may be provided by the operating system, or through a combination of operating system, software, and physical safeguards**:**

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

For other CAs operating under this policy, the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA and its ancillary parts shall include the following functionality:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see section 5.4)
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

For certificate status servers operating under this policy, the computer security functions listed below are required:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

For remote workstations used to administer the CAs, the computer security functions listed below are required:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see section 5.4)
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

All communications between any PKI trusted role and the CA shall be authenticated and protected from modification.

6.5.2. Computer Security Rating

No Stipulation.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

The system development controls for the CA and RA are as follows:

- The CA shall use software that has been designed and developed under a formal, documented development methodology.
- Hardware and software procured to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the vendor cannot identify the PKI component that will be installed on a particular device).
- Hardware and software developed specifically for the CA shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- 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 that are not parts of the CA operation. Where the CA operation supports multiple CAs, the hardware platform may support multiple CAs.

- Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. All applications required to perform the operation of the CA shall be obtained from documented sources. RA 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 shall be installed by trusted and trained personnel in a defined manner.

6.6.2. Security Management Controls

The configuration of the CA system, in addition to any modifications and upgrades, shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the software or configuration. The CA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. The CA shall periodically verify the integrity of the software as specified in the CPS.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. NETWORK SECURITY CONTROLS

A network guard, firewall, or filtering router must protect network access to CA equipment. The network guard, firewall, or filtering router shall limit services allowed to and from the CA equipment to those required to perform CA functions.

Protection of CA equipment shall be provided against known network attacks. All unused network ports and services shall be turned off. Any network software present on the CA equipment shall be necessary to the functioning of the CA application.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment.

Repositories, certificate status servers, and remote workstations used to administer the CAs shall employ appropriate network security controls. Networking equipment shall turn off unused network ports and services. Any network software present shall be necessary to the functioning of the equipment.

The CA shall establish connection with a remote workstation used to administer the CA only after successful authentication of the remote workstation at a level of assurance commensurate with that of the CA.

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

7.1. CERTIFICATE PROFILE

Certificates issued by a CA under this policy shall conform to the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program [CCP-PROF].

7.1.1. Version Number(s)

The CA shall issue X.509 v3 certificates (populate version field with integer "2").

7.1.2. Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in [CCP-PROF].

7.1.3. Algorithm Object Identifiers

Certificates issued under this CP 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}
RSA with PSS padding	id-RSASSA-PSS ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}
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}

The PSS padding scheme OID is independent of the hash algorithm; the hash algorithm is specified as a parameter (for details, see [PKCS#1]). Certificates issued under this CP must use the SHA-256 hash algorithm when generating RSASSA-PSS signatures. The following OID shall be used to specify the hash in an RSASSA-PSS digital signature:

SHA-256	id-sha256 ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1}

Certificates issued under this CP shall use the following OIDs to identify the algorithm associated with the subject key:

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) id-publicKeyType(2) 1}

Where the certificate contains an elliptic curve public key, the parameters shall be specified as one of the following named 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 }

7.1.4. Name Forms

The subject field in certificates issued under id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-High, id-fpki-common-devices, and id-fpki-common-devicesHardware shall be populated with an X.500 distinguished name as specified in section 3.1.1.

The issuer field of certificates issued under the policies in this document shall be populated with a non-empty X.500 Distinguished Name as specified in section 3.1.1.

The subject alternative name extension shall be present and include the pivFASC-N name type in certificates issued under id-fpki-common-authentication and id-fpki-common-cardAuth.

7.1.5. Name Constraints

The CAs may assert name constraints in CA certificates.

7.1.6. Certificate Policy Object Identifier

Certificates issued under this CP shall assert at least one of the following OIDs in the certificate policies extension, as appropriate:

id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}

id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}

id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}

id-fpki-common-devicesHardware ::= {2 16 840 1 101 3 2 1 3 36}

id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13}

id-fpki-common-High ::= {2 16 840 1 101 3 2 1 3 16}

id-fpki-common-cardAuth ::= {2 16 840 1 101 3 2 1 3 17}

Certificates generated with SHA-1 after December 31, 2010 shall assert at least one of the following OIDs in the certificate policies extension, as appropriate:

id-fpki-SHA1-policy ::= {2 16 840 1 101 3 2 1 3 23}

id-fpki-SHA1-hardware ::= {2 16 840 1 101 3 2 1 3 24}

id-fpki-SHA1-devices ::= {2 16 840 1 101 3 2 1 3 25}

id-fpki-SHA1-authentication ::= {2 16 840 1 101 3 2 1 3 26}

id-fpki-SHA1-cardAuth ::= {2 16 840 1 101 3 2 1 3 27}

7.1.7. Usage of Policy Constraints Extension

The CAs may assert policy constraints in CA certificates.

7.1.8. Policy Qualifiers Syntax and Semantics

Certificates issued under this CP shall not contain policy qualifiers.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

Certificates issued under this policy shall not contain a critical certificate policies extension.

7.2. CRL PROFILE

CRLs issued by a CA under the id-fpki-SHA1-authentication, id-fpki-SHA1-cardAuth, or id-fpki-SHA1-hardware policy shall conform to the CRL profile specified in [CCP-PROF] except that SHA-1WithRSAEncryption may be used as the signature algorithm in CRLs that are issued before January 1, 2014.

7.2.1. Version Number(s)

The CAs shall issue X.509 Version two (2) CRLs.

7.2.2. CRL and CRL Entry Extensions

Detailed CRL profiles addressing the use of each extension are specified in [CCP-PROF].

7.3. OCSP PROFILE

Certificate status servers (CSSs) operated under this policy shall sign responses using algorithms designated for CRL signing.

CSSs shall be able to process SHA-1 hashes when included in the CertID field and the keyHash in the responderID field.

7.3.1. Version Number(s)

CSSs operated under this policy shall use OCSP version 1.

7.3.2. OCSP Extensions

Critical OCSP extensions shall not be used.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

CAs operating under this policy shall have a compliance audit mechanism in place to ensure that the requirements of their CPS are being implemented and enforced.

For the Common Policy Root CA, the FPKI Management Authority shall have a compliance audit mechanism in place to ensure that the requirements of this CP are being implemented and enforced by its CPS.

This specification does not impose a requirement for any particular assessment methodology.

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

CAs and RAs operating under this policy shall be subject to a periodic compliance audit at least once per year. As an alternative to a full annual compliance audit against the entire CPS, the compliance audit of CAs and RAs may be carried out in accordance with the requirements as specified in the Triennial Audit Guidance document located at http://www.idmanagement.gov/fpkipa/.

Further, the Federal PKI Policy Authority has the right to require aperiodic compliance audits of CAs operating under this policy. The Federal PKI Policy Authority shall state the reason for any aperiodic compliance audit.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CA's CPS and this CP. The compliance auditor must perform such compliance audits as a regular ongoing business activity. In addition to the previous requirements, the auditor must be a certified information system auditor (CISA) or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor either shall be a private firm that is independent from the entities (CA and RAs) being audited, or it shall be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. An example of the latter situation may be an Agency inspector general. To insure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's CA Facility or certificate practices statement. The FPKIPA shall determine whether a compliance auditor meets this requirement.

The Agency PMA is responsible for identifying and engaging a qualified auditor of agency operations implementing aspects of this CP.

8.4. TOPICS COVERED BY ASSESSMENT

The purpose of a compliance audit shall be to verify that a CA and its recognized RAs comply with all the requirements of the current versions of this CP and the CA's CPS. All aspects of the CA/RA operation shall be subject to compliance audit inspections.

8.5. ***ACTIONS TAKEN AS A RESULT OF DEFICIENCY***

When the compliance auditor finds a discrepancy between the requirements of this CP or the stipulations in the CPS and the design, operation, or maintenance of the PKI Authorities, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the parties identified in section 8.6 of the discrepancy; and
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the FPKIPA and appropriate Agency PMA.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the FPKIPA may decide to temporarily halt operation of the CA or RA, to revoke a certificate issued to the CA or RA, or take other actions it deems appropriate. The FPKIPA will develop procedures for making and implementing such determinations.

8.6. ***COMMUNICATION OF RESULTS***

An Audit Compliance Report shall be provided to the entity responsible for CA operations. The Audit Compliance Report and identification of corrective measures shall be provided to both the FPKIPA and (where applicable) the Agency PMA within 30 days of completion. 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

No stipulation.

9.1.2. Certificate Access Fees

Section 2 of this policy requires that CA certificates be publicly available. CAs operating under this policy must not charge additional fees for access to this information.

9.1.3. Revocation or Status Information Access Fees

CAs operating under this policy must not charge additional fees for access to CRLs and OCSP status information.

9.1.4. Fees for other Services

No stipulation.

9.1.5. Refund Policy

No stipulation.

9.2. *FINANCIAL RESPONSIBILITY*

This CP contains no limits on the use of certificates issued by CAs under this policy. Rather, entities, acting as relying parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

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.

9.3. *CONFIDENTIALITY OF BUSINESS INFORMATION*

CA information not requiring protection shall be made publicly available. Public access to organizational information shall be determined by the respective organization.

9.3.1. Scope of Confidential Information

No stipulation.

9.3.2. Information not within the Scope of Confidential Information

No stipulation.

9.3.3. Responsibility to Protect Confidential Information

No stipulation.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

The FPKI Management Authority or Agency PMA shall conduct a Privacy Impact Assessment. If deemed necessary, the FPKI Management Authority or Agency PMA shall have a Privacy Plan to protect personally identifying information from unauthorized disclosure. For the Common Policy Root CA, the Federal PKI Policy Authority shall approve the Privacy Plan. Privacy plans will be implemented in accordance with the requirements of the Privacy Act of 1974, as amended.

9.4.2. Information Treated as Private

Federal entities acquiring services under this policy shall protect all subscriber personally identifying information from unauthorized disclosure. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. The contents of the archives maintained by CAs operating under this policy shall not be released except as required by law.

9.4.3. Information not Deemed Private

Information included in certificates is not subject to protections outlined in section 9.4.2. However, certificates that contain the FASC-N in the subject alternative name extension, such as PIV Authentication Certificates, shall not be distributed via public repositories (e.g., via LDAP or HTTP).

9.4.4. Responsibility to Protect Private Information

Sensitive information must be stored securely, and may be released only in accordance with other stipulations in section 9.4.

9.4.5. Notice and Consent to Use Private Information

The FPKI Management Authority or Agency PMA is not required to provide any notice or obtain the consent of the subscriber or Authorized Agency Personnel in order to release private information in accordance with other stipulations of section 9.4.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

The FPKI Management Authority or Agency PMA shall not disclose private information to any third party unless authorized by this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. Any request for release of information shall be processed according to 41 CFR 105-60.605.

9.4.7. Other Information Disclosure Circumstances

None.

9.5. INTELLECTUAL PROPERTY RIGHTS

The FPKI Management Authority will not knowingly violate intellectual property rights held by others.

9.6. REPRESENTATIONS AND WARRANTIES

The obligations described below pertain to the FPKI Management Authority and Agency PMAs.

The Federal PKI Policy Authority shall—

- Approve the CPS for each CA that issues certificates under this policy;
- Review periodic compliance audits to ensure that CAs are operating in compliance with their approved CPSs;
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under this CP;
- Revise this CP to maintain the level of assurance and operational practicality;
- Publicly distribute this CP; and
- Coordinate modifications to this CP to ensure continued compliance by CAs operating under approved CPSs.

The Agency Policy Management Authorities shall—

- Review periodic compliance audits to ensure that RAs and other components operated by the agency are operating in compliance with their approved CPSs; and
- Review name space control procedures to ensure that distinguished names are uniquely assigned within their agency.

9.6.1. CA Representations and Warranties

CAs operating under this policy shall warrant that their procedures are implemented in accordance with this CP, and that any certificates issued that assert the policy OIDs identified in this CP were issued in accordance with the stipulations of this policy.

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

- Providing to the FPKIPA a CPS, as well as any subsequent changes, for conformance assessment.
- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Ensuring that registration information is accepted only from approved RAs operating under an approved CPS.

- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates.
- Revoking the certificates of subscribers found to have acted in a manner counter to their obligations in accordance with section 9.6.3.
- Operating or providing for the services of an on-line repository, and informing the repository service provider of their obligations if applicable.

9.6.2. RA Representations and Warranties

An RA that performs registration functions as described in this policy shall comply with the stipulations of this policy, and comply with a CPS approved by the FPKIPA 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. An RA supporting this policy shall conform to the stipulations of this document, including—

- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the 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.

9.6.3. Subscriber Representations and Warranties

A subscriber (or human sponsor for device certificates) shall be required to sign a document containing the requirements the subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate.

Subscribers shall—

- Accurately represent themselves in all communications with the PKI authorities.
- Protect their private key(s) at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures.
- Promptly notify the appropriate CA upon suspicion of loss or compromise of their private key(s). Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS.
- Abide by all the terms, conditions, and restrictions levied on the use of their private key(s) and certificate(s).

9.6.4. Relying Parties Representations and Warranties

This CP does not specify the steps a relying party should take to determine whether to rely upon a certificate. The relying party decides, pursuant to its own policies, what steps to take. The CA

merely provides the tools (i.e., certificates and CRLs) needed to perform the trust path creation, validation, and CP mappings that the relying party may wish to employ in its determination.

9.6.5. Representations and Warranties of Other Participants

None.

9.7. DISCLAIMERS OF WARRANTIES

CAs operating under this policy may not disclaim any responsibilities described in this CP.

9.8. LIMITATIONS OF LIABILITY

The U.S. Government shall not be liable to any party, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.

9.9. INDEMNITIES

No stipulation.

9.10. TERM AND TERMINATION

9.10.1. Term

This CP becomes effective when approved by the Federal PKI Policy Authority. This CP has no specified term.

9.10.2. Termination

Termination of this CP is at the discretion of the Federal PKI Policy Authority.

9.10.3. Effect of Termination and Survival

The requirements of this CP remain in effect through the end of the archive period for the last certificate issued.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

The FPKIPA shall establish appropriate procedures for communications with CAs operating under this policy via contracts or memoranda of agreement as applicable.

For all other communications, no stipulation.

9.12. AMENDMENTS

9.12.1. Procedure for Amendment

The FPKIPA shall review this CP at least once every year. Corrections, updates, or changes to this CP shall be publicly available. Suggested changes to this CP 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.

9.12.2. Notification Mechanism and Period

Proposed changes to this CP shall be distributed electronically to FPKIPA members and observers in accordance with the Charter and By-laws.

9.12.3. Circumstances under which OID must be Changed

OIDs will be changed if the FPKIPA determines that a change in the CP reduces the level of assurance provided.

9.13. DISPUTE RESOLUTION PROVISIONS

The FPKIPA shall facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this policy. When the dispute is between Federal agencies, and the FPKIPA is unable to facilitate resolution, dispute resolution may be escalated to OMB or U.S. Department of Justice, Office of Legal Counsel as necessary.

For CAs operating as Shared Service Providers, disputes as to operational or policy issues shall use the procedure set forth in the *Shared Service Provider Roadmap*.

.

9.14. GOVERNING LAW

The construction, validity, performance and effect of certificates issued under this CP for all purposes shall be governed by United States Federal law (statute, case law, or regulation).

9.15. COMPLIANCE WITH APPLICABLE LAW

All CAs operating under this policy are required to comply with applicable law.

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 CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 9.12.

9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5. **Force Majeure**

No stipulation.

9.17. ***OTHER PROVISIONS***

No stipulation.

10. BIBLIOGRAPHY

The following documents were used in part to develop this CP:

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

CCP-PROF — X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program. http://www.idmanagement.gov/fpkipa/documents/CertCRLprofileForCP.pdf

CIMC — Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001. http://csrc.nist.gov/pki/documents/CIMC_PP_20011031.pdf

E-Auth — E-Authentication Guidance for Federal Agencies, M-04-04, December 16, 2003. http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

FIPS 140-2 — Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

FIPS 186-2 — Digital Signature Standard (DSS), FIPS 186-2, January 27, 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

FIPS 201-1 — Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201-1, March 2006. http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

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

ISO9594-8 — ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

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

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

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

NS4005	NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.
NS4009	NSTISSI 4009, National Information Systems Security Glossary, January 1999.
PACS	*Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.2, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, July 30, 2004. http://www.idmanagement.gov/smartcard/information/TIG_SCEPACS_v2.2.pdf
PKCS#1	Jakob Jonsson and Burt Kaliski, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, RFC 3447, February 2003. http://www.ietf.org/rfc/rfc3447.txt
PKCS#12	PKCS 12 v1.0: Personal Information Exchange Syntax-June 24, 1999. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf
RFC 2510	Certificate Management Protocol, Adams and Farrell, March 1999. http://www.ietf.org/rfc/rfc2510.txt
RFC 2560	X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP, Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams, June 1999. http://www.ietf.org/rfc/rfc2560.txt
RFC 2822	Internet Message Format, Peter W. Resnick, April 2001. http://www.ietf.org/rfc/rfc2822.txt
RFC 3647	Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003. http://www.ietf.org/rfc/rfc3647.txt
RFC 4122	A Universally Unique IDentifier (UUID) URN Namespace, Paul J. Leach, Michael Mealling, and Rich Salz, July 2005. http://www.ietf.org/rfc/rfc4122.txt
SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems, NIST Special Publication 800-37, May 2004. http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf
SP 800-73-3(1)	Interfaces for Personal Identity Verification – Part 1: End-Point PIV Card Application Namespace, Data Model and Representation, NIST Special Publication 800-73-3, February 2010. http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART1_piv-

card-applic-namespace-date-model-rep.pdf

11. ACRONYMS AND ABBREVIATIONS

CA	Certification Authority
C&A	Certification and Accreditation
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Objects Registry
DN	Distinguished Name
ECDSA	Elliptic Curve Digital Signature Algorithm
FPKI MA	Federal Public Key Infrastructure Management Authority
FIPS PUB	(US) Federal Information Processing Standards Publication
FPKI	Federal Public Key Infrastructure
FPKIA	Federal PKI Architecture
FPKIPA	Federal PKI Policy Authority
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector

NARA	U.S. National Archives and Records Administration
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PSS	Probabilistic Signature Scheme
RA	Registration Authority
RDN	Relative Distinguished Name
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
RSASSA	RSA Signature Scheme with Appendix
SHA	Secure Hash Algorithm
S/MIME	Secure/Multipurpose Internet Mail Extensions
SP	Special Publication
SSL	Secure Sockets Layer
SSP-REP	Shared Service Provider Repository Service Requirements
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator

U.S.C.	United States Code
UUID	Universal Unique Identifier
WWW	World Wide Web

12. GLOSSARY

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

Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term "certificate" refers to X.509 certificates that expressly reference the OID of this CP in the certificatePolicies extension.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a certification authority to perform certificate issuance and revocation.
Certification Authority Software	Key management and cryptographic software used to manage certificates issued to subscribers.
Certificate Policy (CP)	A certificate policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A certificate policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List	A list maintained by a certification authority of the certificates that it

(CRL)	has issued that are revoked prior to their stated expiration date.
Certificate Status Server (CSS)	A trusted entity that provides on-line verification to a relying party of a subject certificate's revocation status, and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cross-Certificate	A certificate used to establish a trust relationship between two certification authorities.
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. [FIPS 140-2]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer’s digital certificate; and (2) whether the message has been altered since the transformation was made.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.

End Entity Certificate	A certificate in which the subject is not a CA.
FPKI Management Authority (FPKI MA)	The Federal Public Key Infrastructure Management Authority is the organization responsible for operating the Common Policy Root Certification Authority.
Federal Public Key Infrastructure Policy Authority (FPKIPA)	The FPKIPA is a Federal Government body responsible for setting, implementing, and administering policy decisions regarding the Federal PKI Architecture.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Information Systems Security Officer (ISSO)	Person responsible to the Designated Approving Authority for ensuring the security of an information system throughout its life-cycle, from design through disposal. [NS4009]
Inside Threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish secure

	communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one (public) key can be used to encrypt a message that can only be decrypted using the other (private) key, and (2) even knowing the public key, it is computationally infeasible to discover the private key.
Legacy Federal PKI	A PKI Implementation owned and managed by a Federal Agency and cross-certified with the Federal Bridge prior to 12/31/2005.
Modification (of 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.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a relying party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In

	the Federal PKI, OIDS are used to uniquely identify certificate policies and cryptographic algorithms.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring on-line).
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.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI Sponsor	Fills the role of a subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of subscribers as defined throughout this CP.
Policy Management Authority (PMA)	Body established to oversee the creation and update of certificate policies, review certification practice statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
Privacy	Restricting access to subscriber or relying party information in accordance with Federal law.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is normally made publicly available in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public/private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a registration authority is delegated certain tasks on behalf of an authorized CA).

Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate that contains the new public key.
Relying Party	A person or entity who has received information that includes 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.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
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.
Structural Container	An organizational unit attribute included in a distinguished name solely to support local directory requirements, such as differentiation between human subscribers and devices.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not

	limited to, an individual, an application or network device.
Superior CA	In a hierarchical PKI, a CA that has certified the certificate signature key of another CA, and that constrains the activities of that CA. (See subordinate CA).
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
System High	The highest security level supported by an information system. [NS4009]
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Trust List	Collection of Trusted Certificates used by relying parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of a CA in confirming subscriber identification during the registration process. Trusted agents do not have automated interfaces with certification authorities.
Trusted Certificate	A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Trustworthy System	Computer hardware, software, and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. [NS4009]
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS 140-2]

13. ACKNOWLEDGMENTS

The Certificate Policy Working Group developed this CP based on RFC 3647 and the original U.S. Federal PKI Common Policy Framework Certificate Policy.