Certificate Policy
for the
United States Patent and Trademark Office

August 15, 2024
Version 4.3

Prepared by:

United States Patent and Trademark Office
Public Key Infrastructure Policy Authority

Approval / Date: Tim S. Goodwin — Digitally signed by Users, Goodwin, Timothy Date: 2024.08.30 15:40:30 -04'00'

Name: Timothy Goodwin

Title: Chief Information Security Officer

REVISION HISTORY

Version	Date	Editor	Change Description
1.1-1.3	8/20/04	Darryl Clemons	Version 1.3 was the first signed version.
1.4	12/8/04	Amit Jain	Modified sections 1.4.2, 2.7.1, 3.1.4, 3.2.1, 4.2.1, 4.4.4, 4.5.1, 4.5.5, 4.6.5, 5.3.1, 6.1.5, and 6.4.1 to incorporate necessary modifications identified by FBCA/CPWG.
1.4	12/14/04	Greg McCain	Changed column title from 'Author' to 'Editor' in the Revision History table.
1.5	03/27/07	Greg McCain	Updated to reflect USPTO organizational changes related to management or operational responsibilities for: • Security Policy • Security Operations • User Account Creation and Maintenance
2.0	08/06/07	John Michie	Updated to reflect the new RFC 3647 format
2.1	01/11/10	Greg McCain and Amit Jain	Updated following review and recommendations from External Auditor.
2.1	04/16/10	Amit Jain	Updated the contact information
2.2	5/25/10	Amit Jain	Updates made based on agreements with CPWG to cross-certify at medium-hardware
2.3	6/9/10	Amit Jain	Changed CRL lifetime to 18 hours in section 4.9.7
2.4	7/9/12	Jermaine Harris and Amit Jain	Changes to implement FBCA CP change proposals: 2010-01, 2010-02, 2010-06, 2010-07, 2010-08, 2011-01, 2011-02, 2011-06 and 2011-07.
2.5	11/26/13	David Wu and Amit Jain	Changes related to requirements for FBCA CP Mapping. Modified: 3.1.5, 3.2.3.1, 3.2.3.2, 3.4, 5.4.3, 5.4.8, 5.5, 5.7.3, 6.1.1.1, 6.1.1.2, 6.2.3, 6.2.4.1, 6.2.6, 6.2.9, 6.3.2, 6.4.2, 7.1.3. Added: 6.2.4.5. Removed: 3.2.3.3. Updated outdated NIST security terms and documentation references in sections 10 and11.

Version	Date	Editor	Change Description
			Updated outdated USPTO organization names and terms in sections 1.5.3, 6.1.3, 8.1, and 9.6.6.
2.6	3/23/2016	Amit Jain and Zach Iler	Updated to bring document current and make changes based on previous audit.
2.7	10/31/2016	Ben Spainhour	Updated to reflect new OIDs for Medium Device and Medium Device Hardware. Additions to reflect recent FBCA CP changes.
2.7.1	11/8/2016	Ben Spainhour	Minor wording changes related to requirements for FBCA CP Mapping.
2.7.2	02/02/2017	Richard Arnold, Saman Farazmand and Amit Jain	Updated to reflect new OID for Basic Device. Modified: 1, 1.2, 1.4.1, 3.1.1, 4.5.1, 4.7, 4.9.12, 5.4.2, 5.4.6, 5.5.2, 6.2.1,
2.8	11/13/2017	Richard Arnold	Updated to bring document current and make changes based on previous audit
2.9	10/01/2018	Richard Arnold	Updated to bring document current and make changes based on previous audit
3.0	11/07/2019	Richard Arnold	Updated to bring document current and make changes based on previous audit
3.1	01-06-2021	Scott Cobb	Updated to align with the Bridge and Common CPs.
4.0	04-28-2021	Scott Cobb	Updated to align with the v4.0 USPTO CPS document.
4.1	06-03-2022	Scott Cobb	Remediate 2021 compliance audit findings
4.2	07-14-2023	Scott Cobb	Remediate 2022 compliance audit findings
4.3	08-15-2024	Scott Cobb	Remediate 2023 compliance audit findings

TABLE OF CONTENTS

LIST OF TABLES

1 INTRODUCTION

This Certificate Policy (CP) governs the operation of the Public Key Infrastructure (PKI) by the United States Patent and Trademark Office (USPTO) consisting of products and services that provide and manage X.509 certificates for public-key cryptography. Certificates identify the entity or organization named in the certificate, and binds that entity or organization to a particular public/private key pair.

Each policy defines an assurance level which refers to the strength of the binding between the public key and the subject of the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.

The assurance level also reflects how well the Relying Party can be certain that the entity whose subject name is cited in the certificate is controlling the use of the private key that corresponds to the public key in the certificate, and how securely the system, which was used to produce the certificate and (if appropriate) deliver the private key to the subscriber, performs its task.

A PKI provides a suite of services integral to information systems for processing sensitive information. Through digital signatures and encryption, a PKI provides authentication, data integrity, technical non-repudiation, and confidentiality. The USPTO PKI must provide the following security management services:

- Key generation/storage, escrow, recovery;
- Certificate generation, update, renewal, re-key, and distribution;
- Certificate Revocation List (CRL) generation and distribution;
- Directory management of certificate related items;
- Certificate token initialization, programming, and management; and
- System management functions (e.g., security audit, configuration management, archive, etc.)

Where a specific policy is not stated, the requirements in this CP apply equally to all policies.

In this document, the term “device” means a non-person entity, i.e., a hardware device or software application.

This CP follows the RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

1.1 Overview

1.1.1 Certificate Policy (CP)

The USPTO CP is the policy under which the USPTO establishes and operates a Certification Authority (CA). This CP applies only to CAs owned and operated by the USPTO.

Certificates issued under this policy contain one or more registered certificate policy object identifiers (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. Each certificate issued by the USPTO will assert the appropriate level of assurance in the *certificatePolicies* extension.

The USPTO will also use this policy as the basis for interoperability agreements with external PKIs such as the Federal Bridge Certification Authority (FBCA), the intellectual property offices of other nations, and international organizations.

1.1.2 Relationship between the CP and the CPS

This CP states the requirements for the issuance and management of certificates, and operating the USPTO Internal CA. The USPTO Certification Practice Statement (CPS) states how USPTO implements these requirements.

The USPTO Certification Authority that is cross-certified with the Federal Bridge CA is commonly referred to as the Internal CA.

1.1.3 Relationship between the FBCA CP and the USPTO CP

The FPKI Policy Authority maps the USPTO CP to one or more of the levels of assurance in the FBCA CP. The relationship between this CP and FBCA is asserted in CA certificates issued by the FBCA in the *policyMapping*s extension.

Since the USPTO CA is a legacy CA that is authorized to issue PIV cards, there is also a mapping to the Common Policy CP for the policies applied in the certificates that are mandated by HSPD-12 and FIPS-201.

USPTO also issues certificates with OIDs that correspond to a specific level of assurance established by Federal Common Policy Framework (FCPF) for use in Personal Identity Verification (PIV) cards; and these align with the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (COMMON CP).

1.1.4 Scope

This CP applies to certificates issued to CAs, devices, code signers, USPTO employees, contractors, and other affiliated personnel.

Note that for any certificates issued with OIDs corresponding to the Common Policy Framework (FCPF) for use in PIV cards, USPTO relies directly upon the Common Certificate Policy (CP) document.

USPTO also operates only locally trusted (OLT) CAs that issue certificates to NPE devices for only locally trusted purposes. These OLT CAs do not have a certification path to the Federal Common Policy CA.

1.1.5 Interaction with PKIs External to the Federal Government

USPTO does not have any interoperation relationships with any PKIs external to the federal government.

1.2 Document Name and Identification

This is the X.509 Certificate Policy for the United States Patent and Trademark Office.

USPTO supports Basic and Medium assurance levels. Rudimentary and High levels of assurance are not offered. Each level of assurance has an object identifier (OID), to be asserted in

certificates issued by USPTO CAs. The FBCA that is cross-certified with the USPTO Root CA may assert these OIDs in the *policyMappings* extension of certificates issued to the USPTO CA, as appropriate.

Policy	OID
csor-certpolicy OBJECT IDENTIFER	::= {2 16 840 1 101 3 2 1}
pto-policies OBJECT IDENTIFIER	::= {csor-certpolicy 2}
id-pto-basic-2003	::= {2 16 840 1 101 3 2 1 2 7}
id-pto-medium-2003	::= {2 16 840 1 101 3 2 1 2 8}
id-pto-mediumHardware	::= {2 16 840 1 101 3 2 1 2 9}
id-pto-cardAuth	::= {2 16 840 1 101 3 2 1 2 10}
id-pto-mediumDevice	::= {2 16 840 1 101 3 2 1 2 11}
id-pto-mediumDeviceHardware	::= {2 16 840 1 101 3 2 1 2 12}
id-pto-basicDevice	::= {2 16 840 1 101 3 2 1 2 13}
common-policies OBJECT IDENTIFIER	::= { csor-certpolicy 3 }
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-authentication	::= {2 16 840 1 101 3 2 1 3 13}
id-fpki-common-cardAuth	::= {2 16 840 1 101 3 2 1 3 17}
id-fpki-common-piv-contentSigning	::= {2 16 840 1 101 3 2 1 3 39}
*id-fpki-common-derived-pivAuth	::= {2 16 840 1 101 3 2 1 3 40}
*id-fpki-common-derived-pivAuth-hardware	::= {2 16 840 1 101 3 2 1 3 41}

Requirements associated with **id-pto-basicDevice** are identical to those defined for **id-pto-medium-2003**.

Requirements associated with **id-pto-mediumHardware** are identical to those defined for **id-pto-medium-2003**, except for also including the Subscriber cryptographic module requirements identified in Section 6.2.1.

Requirements associated with **id-pto-mediumDevice** are identical to those defined for **id-pto-medium-2003**, except for also including identity proofing, re-key, and activation data.

Requirements associated with **id-pto-mediumDeviceHardware** are identical to those defined for **id-pto-mediumHardware**, except for also including identity proofing, re-key, and activation data.

The use of the basicDevice, mediumDevice and mediumDeviceHardware policies are restricted to devices and systems.

Human subscriber PIV certificates must contain an appropriate policy OID, refer to the COMMON CP for policy details.

1.3 PKI PARTICIPANTS

The following are roles relevant to the administration and operation of USPTO PKI.

1.3.1 PKI Authorities

1.3.1.1 USPTO Chief Information Officer

This CP is established under the authority of the Chief Information Officer (CIO) of the USPTO.

1.3.1.2 USPTO Policy Authority (PA)

The USPTO PA governs the PKI policy. The USPTO PA consists of the Chief Information Security Officer (CISO) and the Director of Office of Infrastructure Engineering and Operations (OIEO). The PA owns PKI policy documents and represents the interests of the USPTO to external Federal PKI entities. The PA is responsible for:

- Maintenance and distribution of the USPTO CP and CPS;
- Responding to compliance audit reports;
- Ensuring continued conformance of the USPTO PKI with all applicable Federal requirements;
- Interaction with external Federal agencies;
- Directing corrective actions, or other measures that might be appropriate, such as revocation of CA certificates or changes to this CP;
- Receiving requests for modifications to USPTO CP or CPS and recommending adoption, rework, or rejections of such requests to the USPTO Chief Information Security Officer;
- Receiving requests for cross-certification from other entities and recommending adoption, rework, or rejections of such requests to the Chief Information Security Officer of the USPTO.

The USPTO PA will execute a Memorandum of Agreement (MOA) with each cross certified Entity setting forth the respective responsibilities and obligations of both parties and the mappings between the certificate levels of assurance contained in this CP and those in the Federal Bridge CP.

1.3.1.3 USPTO PKI Policy Management Authority (PMA)

The PMA is part of the Policy Authority. It is an individual or committee established by, and responsible to, the USPTO Chief Information Security Officer to hold overall responsibility for maintaining the USPTO CP and for ensuring that all USPTO PKI components are operated in compliance with the USPTO CP.

The PMA is responsible for notifying the FPKIPA of any change to the USPTO infrastructure that may affect the FPKI operational environment. This notification must be made at least two weeks prior to the implementation; all new artifacts (CA certificates, CRL DP, AIA, and/or SIA URLs, etc.) produced as a result of the change must be provided to the FPKIPA within 24 hours following implementation.

1.3.1.4 USPTO PKI Operational Authority (OA)

The OA has operational responsibilities for the USPTO CA. Operation consists of, but are not limited to, posting newly issued certificates, Certificate Revocation Lists (CRLs) into the repository, Online Certificate Status Protocol (OCSP), maintenance of systems, remediation of

compliance audit findings and ensuring the continued availability of the repository. These items are subject to the direction of the USPTO PKI PA.

1.3.1.5 USPTO PKI Operational Authority Administrator (OAA)

The OAA is the USPTO PKI Engineering Technical Lead. This individual has primary responsibility for overseeing the operation of the CA, coordinates all engineering activities of the USPTO PKI, appoints individuals to the roles of Operational Authority officers, selects and manages the operations staff and provides management reporting. The OAA reports into to the Office of the Chief Information Officer (OCIO).

1.3.1.6 USPTO PKI Operational Authority Officers

The Operational Authority Officers are individuals within the Operational Authority who are appointed by the OAA to operate the CA, its repository and the USPTO OCSP facility. These personnel will be employees and trusted contractors who work in or for the OCIO.

The general duties of Operational Authority Officers include the installation, configuration and certain day-to-day operations of the Certification Authority. They are responsible for Certification Authority-related information maintained in the USPTO PKI repositories.

1.3.2 USPTO Certification Authority

USPTO has established the Internal Certification Authority to provide certificates to USPTO personnel, contractor employees, non-human entities, and affiliates. The CA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to Subscribers. The USPTO CA is responsible for issuing and managing certificates including:

- The certificate manufacturing process,
- Publication of certificates,
- Revocation of certificates,
- Re-key of the USPTO CA signing material, and
- 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.

CAs and related applications (e.g., OCSP, CMS) may be hosted on one or more system software layers. Operational and technical security controls including audit logging requirements specified in this CP shall apply to all system software layers, where appropriate and applicable.

1.3.2.1 Entity Cross-Certified Certification Authority (CA)

The Entity designates at least one CA within its PKI to receive a cross-certificate from the FBCA, which is referred to as the “Entity cross-certified CA”. This CP may also refer to CAs that are “subordinate” to the Entity cross-certified CA. This “subordinate CA” terminology shall encompass any CA under the control of the Entity that is subordinate to the cross-certified CA.

The USPTO Entity must ensure that no CA under its PKI shall have more than one trust path to the FBCA.

1.3.3 Card Management System (CMS)

The Card Management System is responsible for managing smart card token content. In the context of this policy, the CMS requirements are associated with the PIV policies only. The PA is responsible for ensuring that all CMSs meet the requirements described in this document.

1.3.4 Registration Authority (RA)

An RA is an entity authorized by the CA to collect, verify, and submit information provided by potential Subscribers for the purpose of issuing public key certificates. The term RA refers to hardware, software, and individuals that may collectively perform this function. Individuals performing RA functions are acting in a Trusted Role, and are considered Officers as defined in Section 5.2.1. The RA is responsible for:

- Control over the registration process
- The identification and authentication process

1.3.5 Certificate Status Servers (CSS)

The USPTO PKI provides Online Certificate Status Protocol (OCSP) responders to provide certificate revocation status for online transactions. 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. Examples include OCSP servers that are identified in the AIA extension. OCSP servers that are locally trusted, as described in RFC 6960, are not covered by this policy.

1.3.6 Key Recovery Authorities

Key Recovery policy and practices are required for CAs operating under the Federal PKIs that issue PIV key management (encryption) certificates.

- CA requirements are applied to the CA database which maintains the key recovery repository, a.k.a. the KED. USPTO does not employ a DDS
- RA requirements are applied to the Security Officer, a.k.a. the KRA. RA requirements are applied to the Probaris and IDMS systems.

USPTO issues subscriber key management certificates and operates the computer system hardware, software, staff, and procedures to escrow these private decryption keys securely and recovers them when appropriate.

For additional policy details regarding key recovery authorities, refer to the COMMON CP.

1.3.7 Subscribers

There are two types of subscribers: human end users and Non-Person Entities (NPE) such as information systems or devices. For a definition of human subscribers, refer to Section 1.3.6 of the COMMON CP for details.

NPEs are represented by a human subscriber, called the PKI Sponsor, who receives certificates for devices and other infrastructure components that require certificates in support of USPTO operations. The PKI Sponsor is responsible for managing their NPE certificates to include

requesting the certificates, guiding their usage, protecting the private key, and requesting certificate revocation when appropriate.

In the context of this CP, a CA is not considered a subscriber.

1.3.8 Affiliated Organizations

Subscriber certificates may be issued on behalf of an organization, other than USPTO, that has a relationship with the subscriber; this is termed affiliation.. The organizational affiliation will be indicated in the certificate. Affiliated Organizations are responsible for verifying the affiliation at the time of certificate application and requesting revocation of the certificate if the affiliation is no longer valid.

1.3.9 Relying Parties

A relying party is the entity that relies on the validity of the binding of the Subscriber's identity to a public key and 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's private key. A Relying Party may use information in the certificate (such as certificate policy identifiers, key usage, or extended key usage) to determine its appropriate 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 of a subscriber.

1.3.10 Other Participants

USPTO may require the services of other security, community, and application authorities, such as compliance auditors.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Subscriber certificates issued by Entity CAs may be used for authentication, key management, signature, and confidentiality requirements. The sensitivity of the information processed or protected using certificates issued by USPTO CA will vary. To provide sufficient granularity, this CP specifies security requirements at different levels of assurance: Basic, Basic Device, Medium, Medium Hardware, Medium Device, Medium Device Hardware, and Card Authentication.

Relying Parties make risk-informed decisions when certificates are used to manage the identities of systems and users by evaluating the environment, associated threats, and vulnerabilities. This evaluation is done by the relying party and is not controlled by this CP.

Certificates generated under this CP are for carrying out the business of the USPTO by providing authentication and security services.

The following table provides additional guidance for determining which policy may be most appropriate based on the sensitivity of the information processed or protected using these certificates. These descriptions are intended as guidance and are not binding.

Table 1-1: Certificate Levels of Assurance

Assurance Level	Applicability
Basic	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. These environments may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious. Basic assurance level certificates issued under the Basic Device policy are intended to be issued to internal devices to improve authentication of these devices when communicating within the USPTO.
Medium	This level is relevant to environments where risks and consequences of data compromise are moderate. These environments may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. This level of assurance includes the following certificate policies: Medium and Medium Device.
Medium Hardware	This level is relevant to environments where threats to data are high or consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk. This level of assurance includes the following: Medium Hardware and Medium Device Hardware.
Card Authentication	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include contactless smart card readers where use of an activation PIN is not practical.

Federal relying parties should review more detailed guidance governing the use of electronic signatures (which include the use of digital certificates) issued by the Office of Management and Budget, as well as more detailed subordinate guidance issued by other agencies pursuant to OMB direction (such as NIST Federal Information Processing Standards and Special Publications).

1.4.2 Prohibited Certificate Uses

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

1.5 Policy Administration

1.5.1 Organization Administering the Document

The USPTO Policy Authority (PA) is responsible for responsible for all aspects of this CP.

1.5.2 Contact Person

Questions regarding this CP may be directed to the Director of the Cybersecurity Division.

Correspondence Address:

Chief Information Security Officer
Office of Chief Information Officer
600 Dulany Street
Alexandria, VA 22314
Phone: (571) 272-0653
Email: Tomothy.Goodwin@USPTO.GOV

1.5.3 Person Determining CPS Suitability for the Policy

The Certification Practices Statement must conform to the corresponding Certificate Policy. The USPTO Director of the Cybersecurity Division must determine the suitability of the CPS for each CA that issues certificates under this policy. The Director will recommend approval to the USPTO Chief Information Security Officer if the CPS is suitable.

1.5.4 CPS Approval Procedures

The USPTO PKI Policy Authority (PA) must first determine if the CPS complies with this policy for a given level of assurance. They then submit the CPS and the results of the compliance audit to the appropriate authority identified in Section 1.5.3 for approval. USPTO is required to meet all facets of the policy.

Temporary waivers to the terms of this CP, while discouraged, may be permitted in order to meet urgent unforeseen operational requirements. Permanent waivers to the terms of this CP must not be issued. Permanent changes to the CP, arising from temporary waivers, must be reviewed by FPKIPA and may result in revocation of the cross-certificate by the FPKIPA.

In some cases, the USPTO PA may require the additional approval of an external authorized agency such as the FPKIPA. The USPTO PA must determine if this approval is required based on the nature of the system function, the type of communications, or the operating environment.

In each case, the determination of suitability must 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

The USPTO EDS Active Directory serves as the internal online directory of all electronically-based Certification Authority-related information.

USPTO also operates a publicly accessible repository, http://ipki.uspto.gov

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

USPTO CA certificates must contain valid Uniform Resource Identifiers (URIs) that are publicly accessible, for the purposes of certification path building and for revocation checking.

All CA certificates and CRLs issued by the USPTO must be published to an online repository that is available to subscribers and Relying Parties.

The USPTO CA must implement mechanisms and procedures designed to ensure CA certificates and CRLs are available for retrieval 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually. Availability targets exclude network outages.

USPTO must publish all CA certificates it issues into a file available via a publicly accessible HTTP URI. This URI must be asserted in the Subject Information Access (SIA) extension in all valid certificates issued to the CA. The file must be a certs-only Cryptographic Message Syntax file that has an extension of .p7c.

With the exception of self-signed certificates, all CA certificates must be published by the Subject CA in a file available via a publicly accessible HTTP URI. This URI must be asserted in the Authority Information Access (AIA) extension in all valid certificates issued by the Subject CA. The file must be:

- a certs-only Cryptographic Message Syntax file that has an extension of .p7c, or
- a single DER encoded certificate that has an extension of .cer

The certs-only Cryptographic Message Syntax format is preferred as it allows flexibility for inclusion of multiple certificates.

CAs must publish the latest CRL covering all unexpired certificates via a publicly accessible HTTP URI until such time as all issued certificates have expired. This URI must be asserted in the CRL distribution point extension of all certificates issued by that CA, except for OCSP responder certificates that include the id-pkix-ocsp-nocheck extension.

A CSS provides status information about certificates on behalf of a CA through on-line transactions.

CAs must include a CSS in the form of a delegated Online Certificate Status Protocol (OCSP) service, as described in [RFC 6960], to provide on-line status information for Subscriber certificates via a publicly accessible HTTP URI in the AIA extension. The operations of the OCSP service are within the scope of this CP.

Pre-generated OCSP responses may be created by the CSS and distributed to OCSP servers. OCSP responses, like CRLs, are publicly distributable data. OCSP servers that lack OCSP response signing capability have the same security requirements as a repository hosting CRLs.

OCSP services that are locally trusted, as described in [RFC 6960], are not covered by this policy.

2.2.2 Publication of CA Information

The USPTO CP and CPS documents must be publicly available to subscribers and Relying Parties on a USPTO internet facing website.

2.3 Time or Frequency of Publication

This CP document is reviewed, updated, and published on an annual basis, or as needed, and provided to the USPTO Policy Authority for approval. It will be made publicly available within 30 days of approval.

2.4 Access Controls on Repositories

CA certificates, CRLs, and pre-generated OCSP responses in the repository must be publicly available. Information not intended for public dissemination or modification must be protected.

Posted certificates, CRLs, and pre-generated OCSP responses may be replicated in additional repositories for performance enhancement.

The USPTO General Counsel, under applicable Federal Laws, and Departmental and USPTO regulations must determine access to other information in the CA repositories. The CPS must define what information in the repository must be exempt from automatic availability to USPTO staff or external parties and to whom, and under what conditions, the restricted information may be made available.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

This CP establishes requirements for both subject distinguished names and subject alternative names.

CA certificates must contain a non-null subject Distinguished Name (DN). All RA certificates must include a non-NULL subject DN. This CP does not restrict the types of names that can be used.

The table below specifies the naming requirements that apply to each level of assurance

Table 3-1: USPTO Assurance Level Naming Requirements

Assurance Level	Naming Requirements
Basic (all policies)	Non-null Subject Name, and optional Subject Alternative Name if marked non-critical
Medium (all policies)	Non-null Subject Name and optional Subject Alternative Name if marked non-critical
Card Authentication	Non-null Subject Alternative Name that is of the FASC-N name type, and Subject Name

3.1.1.1 Subject Names

Device Subscriber distinguished names must be a unique name for the device and must not take the form of a Human.

Device Subscriber names must take the following form:

- Base DN, CN=device name

where device name is a descriptive name for the device.

For policy details regarding human subscriber subject names, refer to the COMMON CP.

3.1.1.2 Subject Alternative Names

For human subscriber certificates issued under id-fpki-common-authentication or id-fpki-common-cardAuth, refer to the COMMON CP for SAN details.

3.1.2 Need for Names to be Meaningful

Names used in certificates issued by the USPTO CA must identify the Subscriber or object to which they are assigned in a clear, meaningful way.

For policy details regarding the need for human subscriber names to be meaningful, refer to the COMMON CP.

When DNs are used, the common name must respect name space uniqueness requirements and must not be misleading. This does not preclude the use of pseudonymous certificates as defined in Section 3.1.3.

The subject name in CA certificates must match the issuer name in certificates issued by the CA, as required by RFC 5280.

3.1.3 Anonymity or Pseudonymity of Subscribers

The USPTO CAs must not issue anonymous certificates. CAs may issue pseudonymous certificates to support internal operations. CA certificates issued by the CA must not contain anonymous or pseudonymous identities.

DNs in device subscriber certificates (e.g. NPE) issued by USPTO CA may contain a pseudonym (such as a large number) as long as name space uniqueness requirements are met.

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

Name uniqueness across the USPTO PKI must be enforced by the CA.

The Policy Authority along with CA and RA must enforce name uniqueness within the X.500 namespace that they have been authorized to use (e.g., an electronic mail address or Domain Name System (DNS) name). When name forms other than a Distinguished Name are used, they too must be allocated such that name uniqueness across the USPTO and the Federal PKI is ensured. Name uniqueness is not violated when multiple certificates are issued to the same entity.

3.1.6 Recognition, Authentication, and Role of Trademarks

The USPTO PA resolves any name collisions or disputes regarding USPTO-issued certificates brought to its attention. The USPTO will not knowingly use trademarks in names unless the subject has the rights to use that name.

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 must prove possession of the private key, which corresponds to the public key in the certificate request.

Practice Note: For signature keys, this may be done by the entity using its private key to sign a value and providing that value to the CA or RA, who will then validate the signature using the party's public key. The Policy Authority may allow other mechanisms that are at least as secure as those cited here.

Proof of possession is not required when a key is generated by the CA or RA and written directly to the applicant's hardware or software token or in a key generator that benignly transfers the key to the applicant's token.

3.2.2 Authentication of Organization Identity

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

USPTO does not issue subscriber certificates on behalf of an affiliated organization.

3.2.3 Authentication of Individual Identity

For each certificate issued, the CA must authenticate the identity of the individual requester.

In addition to the processes described below, Subscriber certificates may be issued on the basis of an electronically authenticated request, using a valid signature or authentication certificate and associated private key, with the following restrictions:

- The assurance level of the new certificate must be the same or lower than the assurance level of the certificate used to authenticate the request;
- Identity information in the new certificate must match the identity information from the signature or authentication certificate;
- The expiration date of the new certificate must not exceed the next required initial identity authentication date associated with the certificate used to authenticate the request.
- The next required initial identity authentication date remains unchanged in the event of a new certificate issuance based on electronic authentication.

3.2.3.1 Authentication of Human Subscribers

For policy details regarding human subscriber authentication, refer to the COMMON CP.

3.2.3.2 Authentication of Human Subscribers for Role-based Certificates

USPTO does not issue role-based certificates.

3.2.3.3 Authentication of Human Subscribers for Group Certificates

USPTO does not issue group certificates.

3.2.3.4 Authentication of Devices

Some computing and communications devices (e.g., servers, routers, firewalls) will be named as certificate subjects. In such cases, the devices must have a human PKI Sponsor. The PKI 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 PKI Sponsor

In the case a PKI sponsor is changed, the new sponsor must review the status of each device under his/her sponsorship to ensure it is still authorized to receive certificates. The CPS must describe procedures to ensure that certificate accountability is maintained.

The registration information must be verified to an assurance level commensurate with the certificate assurance level being requested. For example, certificates issued with mediumDevice and/or mediumDeviceHardware policies, registration information must be verified commensurate with the Medium assurance level. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

1. Verification of digitally signed messages sent from Sponsor (using certificates of equivalent or greater assurance than that being requested); or
2. In person, or supervised remote registration by the Sponsor, with the identity of the PKI 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 must not be included in certificates.

3.2.5 Validation of Authority

Before issuing CA certificates or signature certificates that assert organization authority, the CA must validate the individual's authority to act in the name of the organization.

3.2.6 Criteria for Interoperation

The USPTO Policy Authority must determine the criteria for cross-certification in accordance to the Federal PKI cross certification requirements.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

In the event that a routine re-key of the USPTO CA is required, a new cross certificate will be requested from the FBCA. The identification and authentication process is defined in the FBCA CP and the governing MOA will be followed.

For certificates asserting policies mapped to mediumDevice and mediumDeviceHardware, identity may be established through the use of the device's current signature key or the signature key of the device's human PKI sponsor.

For policy details regarding identification and authentication of human subscribers, refer to the COMMON CP.

3.3.2 Identification and Authentication for Re-key after Revocation

For policy details regarding identification and authentication for re-key after revocation, refer to the COMMON CP.

3.4 Identification and Authentication for Revocation Requests

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 private key has been compromised.

3.5 Identification and Authentication for Key Recovery Requests

The Security Officer executes the KRA responsibilities and must authenticate to the Entrust CA database by using their credentials which were issued by the USPTO PKI. The assurance level of these credentials must be the same as or greater than that of the certificate whose corresponding private key is being recovered and must meet the requirements of an RA credential.

The Operational Authority must verify the identity and authorization of the Requestor prior to initiating the key recovery request. A Requestor is the person that requests the recovery of a Subscriber's private decryption key. Any individual who can demonstrate a verifiable authority and a need to obtain a recovered key may be considered a Requestor.

3.5.1 Third-Party Requestor Authentication

A Third-Party Requestor is someone other than the Subscriber. Identity authentication must be commensurate with the assurance level of the certificate associated with the key being recovered. Identity must be established using one of the following methods:

- An Internal Third-Party Requestor will use their USPTO PIV card for authentication.
- An External Third-Party Requestor will use certificate-based authentication (e.g., digitally signed e-mail or client-authenticated TLS) that can be verified using current, valid (i.e., un-revoked) public key certificates at the requested certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose corresponding private key is being recovered).

3.5.2 Subscriber Requestor Authentication

The Subscriber identity must be established as specified in Section 3.3.1. Alternatively, if the authentication cannot be verified using the public key certificates issued by the USPTO CA and for at least the given certificate policy assurance level, then the identity validation can use the steps outlined in Section 3.2.3.1.

3.5.3 KRA Authentication

The Security Officer executes the KRA responsibilities. Refer to the COMMON CP for KRA authentication details.

3.5.4 KRO Authentication

USPTO does not employ KROs

3.5.5 Data Decryption Server Authentication

USPTO does not employ a DDS.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

To cross-certify with the FBCA, USPTO must fulfill the application requirements as specified in the U.S. Government Public Key Infrastructure Cross-Certification Criteria and Methodology. The FPKIPA acts on the application and, upon making a determination to issue a certificate establishes an MOA with the Entity.

For policy details regarding steps an RA must perform for prospective subscribers, refer to the COMMON CP.

4.1.1 Who Can Submit a Certificate Application

Type of Certificate	Who can submit an application
CA and Delegated OCSP Responder Certificates	Authorized representative of the CA
Human Subscriber Certificate	Authorized agency official or the Applicant
Device Certificate	PKI Sponsor of the device

4.1.2 Enrollment Process and Responsibilities

For policy details regarding enrollment process and responsibilities, refer to the COMMON CP.

4.2 Certificate Application Processing

Information in certificate applications must be verified as accurate before certificates are issued. PKI Authorities must 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. This CP must identify the components of the RA that are responsible for authenticating the Subscriber's identity in each case.

4.2.2 Approval or Rejection of Certificate Applications

For the USPTO Root CA, the USPTO Policy Authority 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 USPTO Operational Authority Officers or their designees.

4.2.3 Time to Process Certificate Applications

Certificate applications must be processed and a certificate issued within 90 days of identity verification.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Upon receiving the request, the CA or RA (as applicable to their functions) will:

- Verify the identity of the requestor;
- Verify the authority of the requestor and the integrity of the information in the certificate request;
- Build and sign a certificate, if all certificate requirements have been met (in the case of 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 attribute information received from a prospective Subscriber must be verified before inclusion in a certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

CAs operating under this policy must 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 must inform the PKI Sponsor.

4.4 Certificate Acceptance

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

4.4.1 Conduct Constituting Certificate Acceptance

For all CAs operating under this policy, failure to object to the certificate or its contents constitutes acceptance of the certificate.

For certificates issued to Subscribers, a signed Subscriber Agreement or auditable record of acceptance constitutes acceptance of the certificates.

4.4.2 Publication of the Certificate by the CA

As specified in 2.2, all CA certificates must be published in a repository accessible over the Internet.

Certificates that contain the FASC-N and/or UUID in the subject alternative name extension, such as PIV authentication certificates, must not be distributed via public repositories.

This policy makes no other stipulation regarding publication of subscriber certificates.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

Whenever a CA operating under this policy issues a CA certificate, the FPKIPA must be notified at least two weeks prior to issuance. In addition, all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the event must be provided to the FPKIPA within 24 hours following issuance.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers must protect their private keys from access by other parties.

Restrictions in the intended scope of usage for a private key are 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

USPTO-issued certificates specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. All CAs operating under this policy must issue CRLs specifying the current status of all unexpired certificates. Relying parties should process certificate and status information as specified in [X.509] when relying on certificates.

4.6 Certificate Renewal

Renewing a certificate means creating a new certificate with a new serial number where all certificate subject information, including the subject public key and subject key identifier, remain unchanged.

The new certificate may have an extended validity period and may include new issuer information (e.g., different CRL distribution point, AIA and/or be signed with a different issuer key).

Once renewed, the old certificate may or may not be revoked, but must not be reused for requesting further renewals, re-keys, or modifications.

4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged. In addition, the validity period of the certificate must meet the requirements specified in Section 6.3.2.

Delegated OCSP responder certificates may be renewed so long as the aggregated lifetime of the private key does not exceed the requirements specified in Section 6.3.2.

4.6.2 Who May Request Renewal

The Operational Authority is responsible for monitoring the OCSP 120 day lifecycle, and taking action to renew the certificates.

4.6.3 Processing Certificate Renewal Requests

When a CA re-keys, it may renew the certificates it has issued.

When certificates are renewed as a result of CA key compromise, as described in Section 4.6.1, the CA or RA must verify all certificates issued since the date of compromise were issued appropriately. If the certificate cannot be verified, then it must not be renewed.

4.6.4 Notification of New Certificate Issuance to Subscriber

As specified in 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As specified in 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

The OCSP certificates are not published.

As specified in 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

As specified in Section 4.4.3.

4.7 Certificate Re-key

Re-key is identical to renewal except the new certificate must have a different subject public key and serial number.

Subscribers must identify themselves for the purpose of re-keying as required in Section 3.3.1.

Once re-keyed, the old certificate may or may not be revoked, but must not be reused for requesting further re-keys, renewals, or modifications.

4.7.1 Circumstance for Certificate Re-key

Circumstances requiring certificate re-key include nearing the maximum usage period of a private key, certificate expiration, loss or compromise, issuance of a new hardware token, and hardware token failure.

Sections 5.6 and 6.3.2 establish usage periods for private keys for both CAs and subscribers.

4.7.2 Who May Request Certification of a New Public Key

For CA certificates and OCSP responder certificates, the Operational Authority may request re-key of its own certificate.

Subscribers with a currently valid certificate may request re-key of the certificate. CAs and RAs may request certification of a new public key on behalf of a subscriber. The PKI sponsor of a device may request re-key of the device certificate.

4.7.3 Processing Certificate Re-keying Requests

Before performing re-key, subscribers must be identified by performing the identification processes defined in Section 3.2 or Section 3.3.

Digitally signed Subscriber re-key requests must be validated before the re-key requests are processed.

4.7.4 Notification of New Certificate Issuance to Subscriber

As specified in Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

As specified in Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

As specified in Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As specified in Section 4.4.3.

4.8 Certificate Modification

Modifying a certificate means creating a new certificate that has the same or a different key, a different serial number, and differs in one or more other fields from the old certificate. Once modified, the old certificate may or may not be revoked, but must not be reused for requesting further renewals, re-keys, or modifications.

4.8.1 Circumstance for Certificate Modification

CA certificates and Delegated OCSP responder certificates whose characteristics have changed (e.g. assert new policy OID) may be modified. The new certificate may have the same or a different subject public key.

A certificate associated with a Subscriber whose characteristics have changed (e.g., name change due to marriage) may be modified. The new certificate must have a different subject public key.

4.8.2 Who May Request Certificate Modification

For CA certificates and Delegated OCSP responder certificates, the Operational Authority may request modification.

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

4.8.3 Processing Certificate Modification Requests

Proof of all subject information changes (e.g. name changes due to marriage) must be provided to the RA or other designated agent.

The CA or RA must verify the information provided prior to issuing the new certificate as specified in Section 4.3.

If an individual's authorizations or privileges change, such that the modified certificate indicates a reduction in privileges and authorizations, the old certificate must be revoked.

If the modified certificate is issued with a new (different) public key, the additional requirements specified in Section 4.7.3 must also apply.

4.8.4 Notification of New Certificate Issuance to Subscriber

As specified in Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

As specified in Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

As specified in 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

As specified in Section 4.4.3.

4.9 Certificate Revocation and Suspension

Certificate suspension is not allowed by this policy.

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.

CAs operating under this policy must issue CRLs covering all unexpired certificates issued under this policy.

USPTO must notify the FPKIPA at least two weeks prior to the revocation of a CA certificate, whenever possible. For emergency revocation, CAs must follow the notification procedures in Section 5.7.

4.9.1 Circumstances for Revocation

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

- The subject's employment, contract or other relationship with the USPTO ends;
- Identifying information or affiliation components of any names in the certificate become invalid;

- Privilege attributes asserted in the subscriber's certificate are reduced;
- The subscriber can be shown to have violated the stipulations of its Subscriber Agreement;
- There is reason to believe the private key has been compromised
- The subscriber or other authorized party (as defined in the CPS) asks that the subscriber's certificate be revoked;
- The failure of a CA to adequately adhere to the requirements of this CP or the approved CPS.

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

4.9.2 Who can Request a Revocation

A CA may summarily revoke certificates within its domain. A written notice and brief explanation for the revocation may subsequently be provided to the subscriber.

The RA can request the revocation of a subscriber's certificate on behalf of any authorized party, such as a PKI Sponsor, as specified in the CPS.

Subscribers may request revocation of their own certificates, and PKI Sponsors may request revocation of certificates they sponsor.

The CA must provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected private key compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to certificates. The CA must publicly disclose the instructions through a readily accessible online means.

4.9.3 Procedure for Revocation Request

A request to revoke a certificate must 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 certificate revocation must be detailed in the CPS.

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

- Revocation request was not for key compromise;
- Hardware token does not permit the user to export the signature private key;
- Subscriber surrendered the token to the PKI;
- Token was zeroized or destroyed promptly upon surrender;

- 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.

Information about a revoked certificate must remain in the status information until the certificate expires.

4.9.4 Revocation Grace Period

There is no grace period for revocation under this policy.

4.9.5 Time within which CA must Process the Revocation Request

CA certificates are revoked once all necessary notification periods have elapsed.

CAs will revoke Subscriber certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests must 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 must be processed before the following CRL is published.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying parties are expected to verify the validity of certificates as specified in RFC 5280.

Practice Note: Use of revoked certificates could have damaging or catastrophic consequences. It is the responsibility of the Relying Party to determine how often new revocation data should be obtained, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.9.7 CRL Issuance Frequency

CRLs must be issued periodically, even if there are no changes to be made, to ensure timeliness of information. CRLs may be issued more frequently than required.

Certificate status information must be published not later than the next scheduled update. This publishing will facilitate the local caching of certificate status information for offline or remote operation.

USPTO CAs that issue certificates to subscribers or operate online 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).

If the CA is operated in an offline manner, the interval between routine CRL issuance must never exceed 35 days.

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

4.9.8 Maximum Latency for CRLs

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

4.9.9 Online Revocation / Status Checking Availability

CAs must support online status checking. Because not all operational environments can accommodate online communications, all CAs must support CRLs. Client software using online status checking need not obtain or process CRLs.

OCSP services must be designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually, with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

USPTO CAs that issue certificate status online or via delegated certificate status responders, must meet or exceed the requirements for CRL issuance stated in 4.9.7 for distribution of certificate status information.

4.9.10 Online Revocation Checking Requirements

Relying Party client software may optionally support online status checking. Client software using online status checking need not obtain or process CRLs.

4.9.11 Other Forms of Revocation Advertisements Available

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

- The alternative method must be described in the 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

In the event of a CA private key compromise or loss, the FPKIMA must revoke the cross-certificate, publish an emergency CRL as soon as feasible, and notify the FPKIPA and all cross-certified entities.

If the USPTO CA certificate is revoked or subscriber certificate is revoked because of compromise, or suspected compromise, of a private key, an emergency CRL must be published within 18 hours of notification.

4.9.13 Circumstances for Suspension

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

4.9.14 Who Can Request Suspension

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

4.9.15 Procedure for Suspension Request

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

4.9.16 Limits on Suspension Period

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

4.10 Certificate Status Services

Refer to Section 4.9.9 for OCSP.

4.10.1 Operational Characteristics

Where applicable, this must be described in the CPS.

4.10.2 Service Availability

Where applicable, this must be described in the CPS.

4.10.3 Optional Features

Where applicable, this must be described in the CPS.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

USPTO only provides key escrow and recovery capabilities for Key Management Keys issued to subscribers on PIV credentials. As a result, USPTO maintains the requirements for subscriber private decryption key escrow and recovery as outlined in the COMMON CP.

- The Security Officer executes the KRA responsibilities.
- The USPTO implementation of the Key Escrow Database entity is established within the Entrust CA database.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 FACILITY, MANAGEMENT & OPERATIONAL CONTROLS

5.1 Physical Controls

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

All the physical control requirements specified below apply equally to all CAs, and any remote workstations used to administer the CAs except where specifically noted.

Practice Note: The phrase "remote workstations used to administer the CAs" refers to dedicated systems solely used for accessing either the system hosting the CA or the CA itself through external networks for maintenance and administration. It does not refer to administration workstations or consoles within the CA's security perimeter or to Registration Authority workstations used by RAs to support certificate management and Subscribers.

5.1.1 Site Location and Construction

The location and construction of the facility housing CA equipment, as well as sites housing remote workstations used to administer the CAs, must 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, must provide robust protection against unauthorized access to the CA equipment and records.

All CAs operated under this CP must be instantiated in the geographic boundaries of the United States of America.

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

The CA equipment must always be protected from unauthorized access, especially while the cryptographic module is installed and activated. Remote workstations running administrative software like Security Manager Administration that are used to administer the CAs must be protected at all times. The security mechanisms must be commensurate with the level of threat in the equipment environment.

The physical security requirements for basic assurance certificates are:

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

In addition to those requirements, the following requirements must apply to medium assurance certificates:

- Ensure manual or electronic monitoring for unauthorized intrusion at all times;
- Ensure an access log is maintained and inspected periodically;
- Require two-person physical access control to both cryptographic module and computer systems.

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

A security check of the facility housing the CA equipment must occur if the facility is to be left unattended. At a minimum, the check must 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 not "closed");
- 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 must 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 must be maintained. If the facility is not continuously attended, the last person to depart must 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 must be protected from unauthorized access while the cryptographic module is installed and activated. The RA must implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms must 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 Validation Authority, must meet the CA physical access requirements specified in 5.1.2.1. The responders will be placed in the USPTO DMZ, so they can respond to requests from outside of USPTO. Communication between the responders and Validation Authorities will be controlled by the USPTO firewalls.

5.1.2.4 Physical Access for CMS Equipment

Physical access control requirements for CMS equipment containing a PIV Content Signing key must meet the CA physical access requirements specified in 5.1.2.1.

5.1.3 Power and Air Conditioning

The CA must have sufficient alternative power supply in the event of a primary power source failure to either maintain CA operations or, at a minimum, prevent loss of data. The repositories (containing CA certificates, CRLs, and re-generated OCSP responses) must 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 must 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

The CA must comply with local commercial building codes for fire prevention and protection.

5.1.6 Media Storage

CA media must be stored so as to protect it from accidental damage (water, fire, electromagnetic) and unauthorized physical access.

5.1.7 Waste Disposal

Sensitive media and documentation that are no longer needed for operations must be sanitized when disposed. For example, sensitive paper documentation must be shredded, burned, or otherwise rendered unrecoverable.

5.1.8 Off-site Backup

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

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 is weakened. The functions performed in these roles form the basis of trust in the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first approach is to ensure that the person fill the role is trustworthy and properly trained. The second is to distribute

the functions of the role among several people, so that any malicious activity would require collusion. An auditable record must be created identifying when personnel are added or removed from a trusted role, as well as who added or removed them from the role. The individual who authorized the role assignment, or any series of role assignments over a given period of time, must also be traceable via audit and archive records.

5.2.1.1 Certification Authority Trusted Roles

The requirements of this policy are defined in terms of four roles, implementing organizations may define additional roles provided the following separation of duties are enforced.

1. *Administrator* – authorized to install, configure, and maintain the CA; establish and maintain system accounts; configure audit parameters; and generate component keys.
2. *Officer* – authorized to request or approve certificate issuance and revocations.
3. *Auditor* – authorized to review, maintain, and archive audit logs.
4. *Operator* – authorized to install, configure, maintain the baseline Operating System and perform system backup and recovery.

Administrators do not issue certificates to subscribers.

The roles required for each level of assurance are identified in Section 5.2.4. Separation of duties must comply with 5.2.4, and requirements for two-person control with 5.2.2, regardless of the titles and numbers of Trusted Roles.

5.2.1.2 Registration Authority Trusted Roles

The Operational Authority Administrator appoints individuals to serve as officers in the Registration Authority Trusted Role. These officials are responsible for implementing PIV card processes (sponsorship, identity proofing/registration, adjudication, issuance) in manner which complies with the requirements of this CP.

5.2.2 Number of Persons Required per Task

USPTO operates a medium assurance CA. Performing any task which requires access to the CA, requires at least two trusted role holders; at least one must be an Administrator. Multi-person control for logical access must not be achieved using a person serving in a USPTO Auditor Trusted Role. A Trusted Role Operator will also need to be present to log on to the system console.

Two or more persons are required for the following tasks

- CA key generation
- CA signing key activation
- CA private key backup
- Generating private keys on the HSM
- Recovering Subscriber private decryption keys from escrow

5.2.3 Identification and Authentication for Each Role

At all assurance levels, an individual must 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 must be specifically designated to assume only one trusted role; Administrator, Security Officer, Registration Authority, Auditor, or Operator.

The CA, RA, and CMS system applications must identify and authenticate its users, and must ensure that no user identity can assume multiple roles.

No individual may have more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

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

5.3.2 Background Check Procedures

CA personnel must receive a favorable adjudication after undergoing 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, except for the residence check, which must cover at least the last three years. Regardless of the date of award, the highest educational degree must be verified.

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

If a formal clearance or other check is the basis for background check, the background refresh must be in accordance with the corresponding formal clearance or other check. Otherwise, the background check must be refreshed every ten years.

Practice Note for federal agencies: A successfully adjudicated National Agency Check with Written Inquires (NACI) or National Agency Check with Law Enforcement Check (NACLC) on record is deemed to have met the minimum standards specified above.

5.3.3 Training Requirements

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

- CA or RA security principles and mechanisms;

- Key Recovery System 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.

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

5.3.4 Retraining Frequency and Requirements

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

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

5.3.5 Job Rotation Frequency and Sequence

Job rotation must not violate role separation. All access rights associated with a previous role must be terminated.

All job rotations must be documented. Individuals assuming an auditor role must not audit their own work from a previous role.

5.3.6 Sanctions for Unauthorized Actions

A CA must take appropriate administrative and disciplinary actions against personnel who have performed actions that are not authorized in this CP, the CPS, or other published procedures published by the Operational Authority.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to operate any part of the CA must be subject to the same criteria as USPTO employees and any additional requirements as defined in the CPS.

5.3.8 Documentation Supplied to Personnel

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

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

5.4 Audit Logging Procedures

The objective of audit log processing is to review all actions to ensure they are made by authorized parties and for legitimate reasons.

At a minimum, audit records must be generated for all applicable events identified in Section 5.4.1 of this policy and must be available during audit reviews and third-party audits. For CAs and related applications (e.g., OCSP, CMS) which may be hosted on one or more system software layers operated in a virtual environment, audit records must be generated for all applicable events on the application software and all system software layers.

Where possible, the security audit logs must be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism must be used. All security audit logs, both electronic and non-electronic, must be retained and made available during compliance audits. Implementation and documentation of automated tools must describe how relevant events and anomalies are recorded.

Audit record reviews should be performed using an automated process, and must include verification that the logs have not been tampered with, an inspection of log entries, and a root cause analysis for any alerts or irregularities.

A record of the review, all significant events, and any actions taken as a result of these reviews must be explained in an audit log summary. This review summary must be retained as part of the long-term archive.

For key escrow and recovery, all audit records of unsuccessful key recoveries must be analyzed to determine the cause and to ensure that the key recovery systems are operating correctly and securely, and is not vulnerable to unauthorized use.

Real-time alerts are neither required nor prohibited by this policy.

5.4.1 Types of Events Recorded

All security auditing capabilities of the underlying CA operating system and the PKI CA applications must be enabled. At a minimum, each audit record must include the following:

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

- What type of event occurred;
- Date and time when the event occurred;
- Where the event occurred (e.g., on what systems or in what physical locations);
- Source of the event;
- Outcome of the event to include success or failure; and
- Identity of any individuals, subjects, or objects/entities associated with the event.

Any request or action requiring the use of a private key controlled by the CA is an auditable event.

If out-of-band processes are used for authorization of certificate issuance, external artifacts from the process (e.g., forms, emails, etc.) must be recorded.

The CA must record the events identified in the table below, where applicable to the application, environment, or both. Where these events cannot be electronically logged, electronic audit logs must be supplemented 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

IDENTIFICATION AND AUTHENTICATION

- Platform or CA application level authentication attempts
- The value of maximum authentication attempts is changed
- The number of unsuccessful authentication attempts exceeds the maximum authentication attempts 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 smart card login to password

DATA ENTRY AND OUTPUT

- Any additional event that is relevant to the security of the CA (such as remote or local data entry or data export); must be documented

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 CA, RA, CSS, CMS, or other keys used by the CA in the lifecycle management of certificates
- All access to certificate subject private keys retained within the CA for key recovery purposes

TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE

- Any changes to public keys used by components of the CA to authenticate other components or authorize certificate lifecycle requests (e.g., RA or CMS trust stores)

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 records related to certificate request authorization, approval and signature, whether generated directly on the CA or generated by a related external system or process

CERTIFICATE REVOCATION

- All records related to certificate revocation request authorization, approval and execution, whether generated directly on the CA or generated by a related external system or process

CERTIFICATE STATUS CHANGE APPROVAL

- All records related to certificate status change request authorization, approval and execution, whether generated directly on the CA or generated by a related external system or process

CA CONFIGURATION

- Any security-relevant changes to the configuration of the CA. The specific configuration items relevant to the environment in which the CA operates must be identified and documented

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

CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT

- All changes to the certificate revocation list profile

MISCELLANEOUS

- Appointment of an individual to a designated Trusted Role
- 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
- Records of manipulation of critical files (e.g., creation, renaming, moving), critical files will vary between installation, and must be identified in the relevant documentation
- The date and time any CA artifact are posted to a public repository
- Access to CA internal database
- All certificate compromise notification requests
- Loading tokens with certificates
- Shipment and receipt of tokens containing key material, or tokens that allow access to key material (e.g., HSM operator cards)

- Zeroizing tokens
- Re-key of the CA

CONFIGURATION CHANGES TO THE CA SERVER:

- 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
- Equipment failure
- Electrical power outages
- Uninterruptible Power Supply (UPS) failure
- Network service or access failures that could affect certificate trust
- Violations of Certificate Policy
- Violations of Certification Practice Statement
- Resetting Operating System clock

5.4.2 Frequency of Processing Audit Log

Audit records must be reviewed at least once every month for CAs issuing certificates at Basic or above. CSS, CMS, IDMS audit log processing frequency must align with the CA audit log processing frequency.

5.4.3 Retention Period for Audit Logs

Audit records must be accessible until reviewed, in addition to specific records being archived as described in Section 5.5.

5.4.4 Protection of Audit Logs

System configuration and operational procedures must be implemented together to ensure that only authorized individuals may move or archive audit records and that audit records are not modified.

Collection of the audit records from the CA system must be performed by, witnessed by or under the control of trusted roles who are different from the individuals who, in combination, command the CA signature key.

For RA systems, the individual authorized to move or archive records may not hold an RA Trusted Role.

Procedures must be implemented to protect audit records from deletion or destruction before they are reviewed. as described in Section 5.4.2. To protect the integrity of audit records, they must be transferred to a backup environment distinct from the environment where the audit records are generated.

5.4.5 Audit Log Backup Procedures

Audit records and audit summaries must be backed up at least monthly.

If audit records are stored locally in the system where the events occur, they must be transferred to a backup environment and protected as described in Section 5.4.4. The backup procedure may be automated or manual, but must occur no less frequently than the audit log review described in Section 5.4.2.

The process for transferring the audit records to the backup environment must be documented.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system may or may not be external to the CA system. Security audit processes must be invoked at system or application startup, and cease only at shutdown.

Audit collection systems must be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files). If 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 must 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

CAs must perform routine vulnerability assessments of the security controls described in the applicable policy.

The self-assessment of controls and control effectiveness (e.g., FISMA) must be performed in accordance with the frequency determined by the risk rating of the CA.

Automated vulnerability scans, if executed, should be run no less frequently than required by the risk rating of the component.

The methodology, tools and frequency of the vulnerability assessment must be documented.

5.5 Records Archival

CAs must comply with their respective record retention policies in accordance with whatever laws apply to those entities.

The primary objective of the CA archive is to prove the validity of any certificate (including those revoked or expired) issued by the CA in the event of dispute regarding the use of the certificate.

The primary objective of the private decryption key archive is to enable reconstruction of key recovery activities, in case of dispute. Examples of disputes may include:

- Validation of key recovery requests
- Validation of the identity of the recipient of an escrowed key;
- Verification of authorization to obtain the escrowed key copy;
- Verification of transfer of custody of escrowed keys to an authorized Requestor;
- Establishment of the circumstances under which a copy of the escrowed key was provided.

5.5.1 Types of Events Archived

At a minimum, the following data must be recorded for archive for all assurance levels:

- Certificate policy
- Certification Practice Statement
- Contractual obligations
- Other agreements concerning operations of the CA
- System and equipment configuration
- Modifications and updates to system or configuration
- All records related to certificate request authorization, approval and signature, whether generated directly on the CA or generated as part of a related external system or process
- All records related to certificate status changes (e.g. revocation, suspension, or restoration) whether generated directly on the CA or generated as part of a related external system or process
- Subscriber identity Authentication data as per Section 3.2.3
- Documentation of receipt and acceptance of certificates
- Subscriber agreements
- Documentation of receipt of tokens
- All certificates issued or published
- Record of CA Re-key
- Other data or applications to verify archive contents
- Audit summary reports generated by internal reviews and documentation generated during third party audits
- 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 for key recovery purposes
- Changes to trusted public keys used or published by the CA including certificates used for trust between the CA and other components such as CMS, RA, etc.

- 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
- Record of an individual being added or removed from a trusted role, and who added or removed them from the 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 Certificate Practice Statement
- Auditor Training

5.5.2 Retention Period for Archive

Archive retention periods begin at the key generation event for any CA. For CAs that leverage key-rollover procedures, a new retention period begins for each subsequent key generation event.

CAs will maintain all archived records related to that CA, in an accessible fashion, for 3 years after CA expiration or CA termination.

Individual RA records associated with certificate request authorization, certificate revocation, subscriber authentication, or subscriber certificate acceptance must be maintained for a minimum of 3 years after the subject certificate expiration date. Issuance of new certificates with extended validity periods (i.e., renewal, rekey or modification) supported by existing subscriber authentication records (i.e., authentication using an existing valid certificate) will result in a new retention period for those initial records, based on the new certificate expiration date.

NARA General Records Schedules (NARA GRS) 5.6 Item 120, defines required enrollment chain-of-trust records, and archive retention periods related to credentials issued in support of HSPD-12.

RA system operations audit records, that include any IT resources that facilitate RA functions, must maintain relevant archives for a minimum of 3 years after RA system replacement or termination.

5.5.3 Protection of Archive

As described in Section 5.2, only Auditors or other personnel specifically authorized by the CA, are permitted to add or delete records from the archive. Deletion of records identified in Section 5.5.1 before the end of the retention period is not permitted under any circumstances. The contents of the archive must not be released except in accordance with Sections 9.3 and 9.4.

Archive media must be stored in a safe, secure storage facility geographically separate from the CA in accordance with its records retention policies. The transfer process between the backup environment and archive location must be documented.

In order to ensure that records in the archive may be referenced when required, the CA must do one of the following:

- Maintain the hardware or software required to process or read the archive records, or

- Define a process to transfer records to a new format or medium when the old format or medium becomes obsolete and verify the integrity of the records after transfer

5.5.4 Archive Backup Procedures

USPTO will not backup its archival records at the current time.

5.5.5 Requirements for Time Stamping of Records

CA archive records must have accurate time stamps when they are added to the archive .

The time precision must be such that the sequence of events can be determined.

The CPS must describe how system clocks used for time stamping are maintained in synchrony with an authoritative time source.

5.5.6 Archive Collection System (Internal vs. External)

Archive data may be collected in any expedient manner, but must be documented in the associated CPS.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures detailing how to create, verify, package, transmit, and store archive information must be included in the CPS.

Records of individual transactions may be released upon request of any subscribers who were involved in the transaction, or their legally recognized agents.

5.6 Certification Authority Key Changeover

The CA's signing key must have a validity period as described in Section 6.3.2.

To minimize risk to the PKI through compromise of a CA's private signing key, the private signing key may be changed often. Prior to the end of a CA's signing key validity period, a new CA must be established or a re-key on the existing CA must be performed. From that time on, only the new key will be used to sign CA and Subscriber certificates. The older valid certificate will be available to verify old signatures until all of the subscriber certificates signed under it have also expired. If the old private key is used to sign OCSP responder certificates or CRLs that cover certificates signed with that key, then the old key must be retained and protected.

After a CA performs a Key Changeover, the CA may continue to issue CRLs with the old key until all certificates signed with that key have expired. As an alternative, after all certificates signed with that old key have been revoked, the CA may issue a final long-term CRL using the old key, with a nextUpdate time past the validity period of all issued certificates. This final CRL must be available for all Relying Parties until the validity period of all issued certificates has passed. Once the last CRL has been issued, the old private signing key of the CA may be destroyed.

When a CA updates its private signature key and thus generates a new public key, the CA must notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed.

CAs that distribute self-signed certificates must 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.

Lastly, if a Domain Name is changed at the same time as a key, new cross certificates must be established with the Federal Common Policy CA.

5.7 Compromise and Disaster Recovery

The CA and repository must be deployed to provide availability 24 hours a day, 365 days a year, with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually.

The CA must have an incident handling process, which documents any security incidents. Security incidents may include violation or threat of violation to the system, improper usage, malicious or anomalous activity and violations of the CPS or CP.

The CA must have recovery procedures in place to reconstitute the CA within 72 hours in the event of a catastrophic failure, as described in the following subsections.

5.7.1 Incident and Compromise Handling Procedures

The USPTO PKI Policy Authority must be notified if any CAs operating under this policy experience the incidents listed below. In turn, the USPTO PKI PA must then notify the Federal PKI PA within 24 hours. The notification must include preliminary remediation analysis.

- Suspected or detected compromise of the CA systems
- Physical or electronic penetration of CA systems
- Successful denial of service attacks on CA components
- Any incident preventing the CA from issuing a CRL prior to the nextUpdate time of the previous CRL
- Suspected or detected compromise of a CSS
- Suspected or detected compromise of an RA

Once the incident has been resolved, the organization operating the CA must provide notification directly to the FPKIPA which includes detailed measures taken to remediate the incident. The notice must include the following:

1. Which CA components were affected by the incident
2. The CA's interpretation of the incident
3. Who is impacted by the incident
4. When the incident was discovered
5. A complete list of all certificates that may have been issued erroneously or are not compliant with the CP/CPS as a result of the incident
6. A statement that the incident has been fully remediated

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

If Certification Authority equipment, software, and/or data are corrupted, is damaged or rendered inoperative, CAs operating under this policy must 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 must be reestablished as quickly as possible, 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 must be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

The USPTO PKI Operational Authority Officers and Policy Management Authority must be notified as soon as possible.

In the event of an incident as described above, a notice must be posted on the web page identifying the incident and provide notification to the FPKIPA. See Section 5.7.1 for contents of the notice.

5.7.3 Certification Authority Signature Keys are Compromised

If the CA signature key is compromised or lost (such that compromise is possible) the following operations must be performed:

- The USPTO PKI Policy Authority must be immediately and securely notified.
- The USPTO PKI PA must notify the FPKIPA, as well as any cross-certified CAs and any entities known to be distributing the CA certificate (e.g., in a root store).
- The CA must request revocation of any certificates issued to the compromised CA.
- 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 must 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 issued prior to compromise of the CA private key 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.

The organization operating the CA must post a notice on its web page describing the compromise. See Section 5.7.1 for contents of the notice.

5.7.4 Business Continuity Capabilities after a Disaster

Recovery procedures must be place to reconstitute the CA after a 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 USPTO Policy Authority must take action to

notify the Federal PKI PA at the earliest feasible time, and the FPKIPA must take whatever action it deems appropriate.

The CA installation must then be completely rebuilt, by reestablishing the CA equipment, generating new private and public keys, being re-certified, and re-issuing all cross certificates.

5.8 CA or RA Termination

If possible, the FPKIPA must be notified at least two weeks prior to the termination of any Entity CA. For emergency termination, CAs must follow the notification procedures in Section 5.7

In the event the decision is made to terminate CA operations, the following must be accomplished prior to termination:

- Notify all cross-certified CAs.
- Transfer all archive data to an archive facility that has been approved by the Policy Authority.
- Revoke any issued certificates that have not expired.
- Generate and publish a final long term CRL with a nextUpdate time past the validity period of all issued certificates. This final CRL must be available for all relying parties until the validity period of all issued certificates has passed.
- Once the last CRL has been issued, destroy the private signing key(s) of the USPTO CA.

When an organizational RA function operating under this policy terminates operations, the RA must archive all audit logs and other records prior to termination and destroy its private keys upon termination.

.

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 must be generated in FIPS 140 validated cryptographic modules, as specified in Section 6.2.1. Multiparty control is required for CA key pair generation, as specified in Section 6.2.2. A private key must not appear outside of the module in which it was generated unless it is encrypted for local transmission or for processing or storage by a key recovery mechanism.

CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. For all levels of assurance, the documentation of the procedure must be detailed enough to show that appropriate role separation was used.

For High, Medium Hardware, and Medium Assurance, an independent third party must 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.

6.1.1.2 Subscriber Key Pair Generation

For policy details regarding subscriber key pair generation, refer to the COMMON CP.

6.1.1.3 CSS Key Pair Generation

Cryptographic keying material used by CSSs to sign status information must be generated in FIPS 140 validated cryptographic modules as specified in Section 6.2.1.

6.1.1.4 PIV Content Signing Key Pair Generation

Cryptographic keying material used by PIV issuing systems or devices for Common PIV Content Signing must be generated in FIPS 140 validated cryptographic modules as specified in Section 6.2.1

6.1.2 Private Key Delivery to Subscriber

For policy details regarding private key delivery to subscribers, refer to the COMMON CP.

6.1.3 Public Key Delivery to Certificate Issuer

For CAs issuing certificates that assert policies other than rudimentary, the following requirements apply:

- Where the Subscriber or RA generates a key pair, the public key and the Subscriber's identity must be delivered securely to the CA for certificate issuance.

- The delivery mechanism must 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

Self-signed root CA certificates must be conveyed to Relying Parties in a secure fashion to preclude substitution attacks. Acceptable methods include:

- Secure distribution of trusted certificates through secure out-of-band mechanisms;
- Download the certificate from a Federal Government operated web site secured with a currently valid certificate and subsequent comparison of the hash of the self-signed certificate against a hash value made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism);

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 must contain 2048-bit, 3072-bit, 4096-bit RSA keys, or 256-bit or 384-bit elliptic curve keys.

	CA certs expiring on or before 12-31-2030	CA certs expiring after 12-31-2030
Minimum Key Size	RSA: 2048 Elliptic Curve: 256	RSA: 3072 Elliptic Curve: 256
Hash Algorithm	SHA-256, SHA-384, or SHA-512	SHA-256, SHA-384, or SHA-512

	Subscriber certs expiring on or before 12-31-2030	Subscriber certs expiring after 12-31-2030
Minimum Key Size	RSA: 2048 Elliptic Curve: 256	RSA: 3072 Elliptic Curve: 256
Hash Algorithm	SHA-256, SHA-384, or SHA-512	SHA-256, SHA-384, or SHA-512

Reference NIST Special Publication 800-78 for algorithms and key sizes for certificates stored on PIV or Derived PIV credentials.

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP must require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 2048-bit RSA or equivalent for the asymmetric keys.

After December 31, 2030, use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP must require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 3072-bit RSA or equivalent for the asymmetric keys.

The Entrust CA database keys must be equal to or stronger than the subscriber private decryption keys which are being held in escrow.

6.1.6 Public Key Parameters Generation

Public key parameter generation and quality checking must be conducted in accordance with SP 800-89. Key validity must be confirmed in accordance with SP 800-56A.

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

For policy details regarding human subscriber key usage, refer to the COMMON CP.

Keys associated with CA certificates must be used only for signing certificates and CRLs.

Keys associated with Device Subscriber certificates may be used for digital signature (including authentication), encryption, or both. Except for OCSP Responder certificates, device certificates must not assert the nonRepudiation bit.

Where the subject signs OCSP responses, the certificate may also set the *digitalSignature* and/or *nonRepudiation* bits.

Certificates that assert id-fpki-common-piv-contentSigning must include a critical Extended Key Usage extension that asserts only id-PIV-content-signing {2.16.840.1.101.3.6.7}.

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* (current version of FIPS 140). Cryptographic modules must be validated to the FIPS 140 level identified in this section.

The table below summarizes the minimum requirements for cryptographic modules.

Table 6-1: Minimum FIPS 140 Requirements for Cryptographic Modules

Assurance Level	CA,	CMS, CSS	Subscriber	RA
Basic	Level 2	Level 2	Level 1	Level 1
Medium	Level 3 (Hardware)	Level 2 (Hardware)	Level 1	Level 2 (Hardware)
Card Authentication	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

CAs that do not issue certificates under id-fpki-common-High must use a FIPS 140 Level 2 or higher validated hardware cryptographic module.

RAs must use a FIPS 140 Level 2 or higher validated hardware cryptographic module when authenticating to systems to fulfill their duties.

PIV Cards must only be issued using card stock that has been tested and approved by the FIPS 201 Evaluation Program and listed on the GSA Approved Products List (APL). Card stock that has been removed from the APL may continue to be issued for no more than one year after GSA approved replacement card stock is available. PIV cards issued using the deprecated card stock may continue to be used until the current subscriber certificates expire, unless otherwise notified by USPTO.

6.2.1.1 Custodial Subscriber Key Stores

USPTO does not use custodial subscriber key stores.

6.2.2 Private Key Multi-Person Control

A single person must not be permitted to activate the CA signature key or access any cryptographic module containing the complete CA private signing key. For the Medium, Medium Hardware or High levels of assurance, CA signing key activation requires multiparty control as specific in Section 5.2.2.

Access to CA signing keys backed up for disaster recovery must be under the same multi-person control as the original CA signing key. The names of the parties used for two-person control must be maintained on a list that must be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

6.2.3.1 Escrow of CA Private Signature Key

CA private keys must never be escrowed.

Subscriber key management keys may be escrowed to provide key recovery as described in section 4.12.1.

6.2.4 Private Key Backup

All backups of CA, CSS, and PIV Content Signing private signature keys must be accounted for and protected under the same multi-person control as the original signature key. At least one copy of the CA private signature key must be stored off site.

For all other keys, backup, when permitted, must provide security controls consistent with the protection provided by the original cryptographic module. Backed up private signature key(s) must not be exported or stored in plaintext form outside the cryptographic module.

Private Key	**Backup**
CA • all applicable policies	Required
CSS • all applicable policies	Optional
PIV Content Signing • id-fpki-common-piv-contentSigning	Optional
Hardware Signature and Authentication • id-fpki-common-authentication • id-fpki-common-derived-pivAuth-hardware • id-fpki-common-cardAuth • id-fpki-common-hardware	Not Permitted
Hardware Subscriber Key Management	Required

Private Key	Backup
• id-fpki-common-hardware	
Software Signature and Authentication • id-fpki-common-derived-pivAuth	Optional (Software Subscriber private signature keys may be backed up or copied, but must be held in the Subscriber's control)
Software Device • id-fpki-common-devices	Optional

6.2.5 Private Key Archival

CA private signature keys and Subscriber private signature keys must not be archived.

Escrowed Subscriber private key management keys may be archived for business continuity purposes, and must be protected in accordance with Sections 4.12, 5.1, 5.2, and 6.2.1.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The CA private key must not exist in plaintext outside the cryptographic module.

The CA, CSS, and PIV Content Signing private keys may be exported from the cryptographic module only to perform backup procedures as described in section 6.2.4.

If any private key is transported from one cryptographic module to another, the private key must be protected using a FIPS approved algorithm and at a bit strength commensurate with the key being transported. 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 Keys

Cryptographic modules must be protected from unauthorized access.

For mediumDevice and mediumDeviceHardware, user activation of the private key is not required.

For policy details regarding method of activating subscriber private keys, refer to the COMMON CP.

6.2.9 Method of Deactivating Private Keys

After use, cryptographic modules must be deactivated, e.g. via a manual logout procedure, or automatically after a period of inactivity as defined in the CPS. CA cryptographic modules must be removed and stored in a secure container as outlined in Section 5.1.2, when not in use.

6.2.10 Method of Destroying Private Keys

Individuals in trusted roles must destroy CA, RA, and CSS (e.g., OCSP server) private signature keys when they are no longer needed. Subscribers must 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. For software cryptographic modules, this can be done by overwriting the data. For hardware cryptographic modules, this will likely be executing a "zeroize" command. Physical destruction of hardware is not required.

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 administrative records of the CA.

6.3.2 Certificate Operational Periods and Key Usage Periods

CA private key 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.

Key Type	Private Key	Certificate
Intermediate/Signing CA certificate	10 years	10 years
Cross Certificate	3 years	3 years
Subscriber Authentication	3 years	3 years
Subscriber Signature	3 years	3 years
Subscriber Encryption	Unrestricted	3 years
PIV Card Auth	3 years	3 years
Content Signing	3 years	8 years
Code Signing	3 years	8 years
OCSP Responder	3 years	120 days
Device	2 years	2 years

6.4 Activation Data

6.4.1 Activation Data Generation & Installation

CA activation data may be user selected. The activation data used to unlock CA or subscriber private keys, in conjunction with any other access control, must have an appropriate level of strength for the keys or data to be protected. If the activation data must be transmitted, it must be via an appropriately protected channel, and distinct in time and place from the associated

cryptographic module. Where a USPTO CA uses passwords as activation data for the CA signing key, at a minimum the activation data must be changed upon CA re-key.

For Medium Assurance and above, RA and Subscriber activation data may be user-selected. The strength of the activation data must meet or exceed the requirements for authentication mechanisms stipulated for Level 2 in [FIPS 140]. If the activation data must be transmitted, it must 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 must be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data must be:

- Memorized;
- Biometric in nature; or
- Recorded and secured at the level of assurance associated with the activation of the cryptographic module, and must not be stored with the cryptographic module.

The protection mechanism must include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the CPS.

6.4.3 Other Aspects of Activation Data

A CA operating under this policy must define any other aspects of Activation Data in its CPS.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions are required and may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The USPTO CA and its ancillary parts must 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;
- require use of cryptography for session communication and database security;
- require self-test security-related CA services;
- require a trusted path for identification of all users;
- provide residual information protection; and
- require recovery from key or system failure.

For CSS, the computer security functions listed below are required (these functions pertain to all system software layers, where applicable, e.g. virtual machines):

- 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;
- provide residual information protection; and
- require recovery from key or system failure.

For remote workstations used to administer the CA, 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;
- provide residual information protection; and
- require recovery from system failure.

All communications between any PKI trusted role and the CA must 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:

- For commercial off-the-shelf software, the software must be designed and developed under a formal, documented development methodology.
- Where open source software has been utilized, the applicant must demonstrate that security requirements were achieved through software verification & validation and structured development/life-cycle management.
- Hardware and software procured to operate the CA must be purchased and shipped in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- Custom hardware and software must be developed in a controlled environment, and the development process must be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- The CA hardware and software, including all system software layers, must be dedicated to operating and supporting the CA (i.e., the systems and services dedicated to the issuance and management of certificates). There must be no other applications; hardware devices, network connections, or component software installed which are not part of the CA operation, administration, monitoring and security compliance of the system. CA

hardware and system software layers of the CA may support multiple CAs and their supporting systems, provided all systems have comparable security controls and are dedicated to the support of the CA in compliance of the same CP.

- Proper care must be taken to prevent malicious software from being loaded onto the CA equipment. All applications required to perform the operation of the CA must be obtained from documented sources. Except for Offline CAs, CA and RA hardware and software must be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates must be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

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

USPTO's formal Life Cycle Management processes and procedures will be followed to control, document and manage implementation, modifications, upgrades and retirement of the USPTO PKI systems.

6.6.3 Life-Cycle Security Ratings

USPTO CAs must identify any life cycle security control requirements in this CP..

6.7 Network Security Controls

Network security controls (e.g. firewalls) must be employed to protect network access to the USPTO CA and its repositories. These security appliances will limit services to and from the CA equipment so that only the required services to perform CA and key recovery functions are allowed.

CA equipment must be protected against known network attacks. All unused network ports and services must be turned off. Any network software residing on the CA must be necessary to the functioning of the CA applications.

Any boundary control devices used to protect the USPTO CA repositories and local area network on which PKI equipment is hosted must deny all but the necessary services to the PKI equipment.

RAs, CMSs, repositories, CSSs, directories, and remote workstations used to administer the CAs, and certificate status servers must be located on internal networks behind boundary/perimeter network defenses and afforded protections consistent with commercial electronic commerce practices for network security controls. Networking equipment must turn off unused network ports and services. Any network software present must be necessary to the function of the equipment.

Any remote workstation used to administer the CA must use a Virtual Private Network (VPN) to access the CA. The VPN must be configured for mutual authentication, encryption, and integrity. If mutual authentication is shared secret based, the shared secret must be changed at least annually, must be randomly generated, and must have entropy commensurate with the cryptographic strength of certificates issued by the PKI being administered.

The CA may permit remote administration only after successful multi-factor authentication of the Trusted Role at a level of assurance commensurate with that of the CA.

6.8 Time-Stamping

Asserted times must 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

PIV certificates must conform to the Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles [CCP-PROF]

All other certificates must be compatible with X.509 Certificate and CRL Extensions Profile [FBCA-PROF].

7.1.1 Version Numbers

The CA must issue X.509 Version 3 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 profiles. These profiles are written to prescribe an appropriate amount of control over an infrastructure, yet be flexible enough to meet the needs of the various CAs and communities. CAs issuing certificates under this CP must comply with both the RFC 5280 and the Federal certificate and CRL profile guidelines.

CA certificates must not include critical private extensions.

7.1.3 Algorithm Object Identifiers

Certificates under this Policy must use one of the following OIDs for signatures.

Signature Algorithm	Object Identifier
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
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}
ecdsa-with-Sha512	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4}

The PSS padding scheme OID is independent of the hash algorithm; the hash algorithm is specified as a parameter. The following OIDs must be used to specify the hash in an RSASSA-PSS digital signature:

Hash	Object Identifier
id-sha256	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1}
id-sha384	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 2}
id-sha512	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3}

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

Public Key Algorithm	Object Identifier
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 non-CA certificates contains an elliptic curve public key, the parameters must be specified as one of the following named curves:

Curve	Object Identifier
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

Where required as set forth in Section 3.1.1, the subject and issuer fields of the base certificate must be populated with an X.500 Distinguished Name, with standard attribute types such as those defined in RFC 5280.

7.1.5 Name Constraints

CAs must assert name constraints in CA certificates as required.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this policy must assert at least one certificate policy OID in the certificate policies extension, as specified in Section 1.2.

Certificates issued for PIV card authentication or PIV content signing must not express any other policy OIDs.

Delegated OCSP Responder certificates must assert all policy OIDs for which they are authoritative.

7.1.7 Usage of Policy Constraints Extension

CAs may assert policy constraints in CA certificates. When this extension appears, at least one of *requireExplicitPolicy* or *inhibitPolicyMapping* must be present. When present, this extension may be marked critical.

For Subordinate CA certificates *inhibitPolicyMappings*, skip certs will be set to 0. For cross-certificates *inhibitPolicyMappings*, skip certs will be set to 1, or 2 for the Federal Bridge CA. When *requireExplicitPolicy* is included, skip certs must be set to 0.

Practice Note: *inhibitPolicyMapping*, skip certs is usually set to 1 in a cross-certificate issued to a Bridge so it can do another cross-certificate mapping to its CA members. A skip certs value of 2 may be required to allow transitive trust if that Bridge issues a cross-certificate to a CA that also allows mapping, e.g., the Federal Common Policy CA also issues cross-certificates with policy mapping. If transitive trust is not the desired behavior other constraints such as name constraints may be required to control appropriate results

7.1.8 Policy Qualifiers Syntax and Semantics

USPTO CAs must avoid issuing certificates containing policy qualifiers. If a requirement for a USPTO CA is identified that requires the issuance of certificates containing policy qualifiers, they must be identified in the applicable CPS and are constrained to the policy qualifiers identified in RFC 5280.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Certificates issued under this CP must contain a non-critical certificate policies extension.

7.1.10 Inhibit Any Policy Extension

CAs may assert *InhibitAnyPolicy* in CA certificates. When present, this extension may be marked critical. Skip Certs must be set to 0.

7.2 CRL Profile

CRLs issued by a CA under this CP must conform to the CRL profile specified in [FPKI-PROF].

7.2.1 Version Numbers

CAs must issue X.509 Version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

Detailed CRL profiles addressing the use of each extension must conform to the Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile.

7.3 OCSP Profile

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

All CSSs must accept and return SHA-1 hashes in the CertID and responderID fields. CSS may accept and return additional hash algorithms within the CertID fields. CSSs must not return any response containing a hash algorithm in the CertID that differs from the CertID in the request

7.3.1 Version Numbers

CSSs must use OCSP version 1.

7.3.2 OCSP Extensions

Critical OCSP extensions must not be used.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

All USPTO CAs are subject to an annual review by the FPKIPA to ensure policies and operations remain consistent with the policy mappings in the certificate issued to the Entity by the FBCA.

The USPTO Policy Authority will ensure that each CA operating under this CP must have a compliance audit mechanism in place to ensure that requirements of this CP and the CPS are being implemented and enforced.

The USPTO Policy Authority is responsible for ensuring annual audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated.

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

8.1 Frequency of Audit or Assessments

The USPTO PKI must be subject to an annual PKI compliance audit in accordance with the *FPKI Annual Review Requirements* document. The audit must include all CAs, CSS, CMS, RAs, and supporting repositories. Where a status server is specified in certificates issued by a CA, the status server must be subject to the same compliance audit requirements as the corresponding CA.

The USPTO PKI Policy Authority has the right to require periodic and aperiodic compliance audits or inspections of any or all CA or RA operations to validate that the entities are operating in accordance with the security practices and procedures described in the applicable CPS.

The FPKI Policy Authority has the right to require aperiodic compliance audits of Entity PKIs (and, when needed, their subordinate CAs) that interoperate with the FBCA under this CP. The FPKIPA must state the reason for any aperiodic compliance audit.

On an annual basis, for each PCI configuration used (as defined by the FIPS 201 Evaluation Program), one populated, representative PIV card must be submitted to the FIPS 201 Evaluation Program for testing.

8.2 Identity/Qualifications of Assessor

The auditor must demonstrate competence in the field of compliance audits and be thoroughly familiar with the requirements which the USPTO CA imposes on the issuance and management of their certificates. The compliance auditor must perform such compliance audits as a regular ongoing business activity.

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor either must be a private firm, that is independent from the entities being audited, or it must 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 ensure 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 Policy Authority must determine whether a compliance auditor meets this requirement.

8.4 Topics Covered by Compliance Audit

The purpose of a compliance audit must be to verify that the CA and its RAs comply with all the requirements of this CP, the USPTO CPS, FBCA CP, FCPCA CP as well as any MOA's between USPTO CA's and any other PKI. All aspects of the CA and RA operation must be subject to compliance and inspection.

If the auditor uses statistical sampling, all PKI components, PKI component managers and operators must be considered in the sample. The samples must vary on an annual basis.

A full compliance audit covers all aspects within the scope identified above.

8.5 Actions Taken as a Result of Deficiency

When the compliance auditor finds a discrepancy between how the USPTO CA and RA is designed or is being operated or maintained, and the requirements of this CP, the MOAs, or the applicable CPS, the following actions must be performed:

- The compliance auditor must document the discrepancy and provide a copy to the USPTO Operational Authority;
- The compliance auditor must notify the responsible party promptly;
- The USPTO Operational Authority will provide a copy of the discrepancy documentation to the USPTO PKI Policy Authority;
- The USPTO Operational Authority will report findings and corrective action to the USPTO PKI Policy Authority;
- The USPTO PKI Policy Authority must determine what further notifications or actions are necessary to meet the requirements of this CP, MOAs, MOU, and /or other entities with which the USPTO has contractual agreements and then make such notifications and take such actions without delay;
- Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the Policy Authority may direct the Operational Authority to take additional actions as appropriate, including temporarily halting operation of the CA and RA.

8.6 Communication of Results

On an annual basis, USPTO must submit an audit compliance annual review package to the FPKIPA. This package must be prepared in accordance with the *FPKI Annual Review Requirements* document and includes an assertion from the USPTO PMA that all PKI components have been audited - including any components that may be separately managed and operated. The package must identify the versions of the CP and CPS used in the assessment. Additionally, where necessary, the results must be communicated as set forth in Section 8.5 above.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

The USPTO PKI Policy Authority reserves the right to charge a fee for any or all services provided.

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 limits the use of certificates issued by CAs under this policy to USPTO applications and other applications that have been explicitly approved. Relying Parties must determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction, and must include this information in their agreement to rely on certificates issued under this CP.

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 identified in Section 2 not requiring protection must be made publicly available.

USPTO operates a publicly accessible repository, http://ipki.uspto.gov

9.3.1 Scope of Confidential Information

The following information must also be considered confidential and may not be disclosed except as detailed in section 9.3.3:

- Information concerning the events leading up to and the investigation of a revocation.

9.3.2 Information not within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

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

The USPTO PKI is responsible for maintaining the confidentiality of information clearly marked or labeled as confidential that is shared with it. This information must be treated with the same degree of care and security as it treats its own confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

A Privacy Threshold Assessment is conducted periodically to determine the necessity of a Privacy Impact Assessment. A Privacy Program Plan is created to describe the mission and strategy for safeguarding personal privacy in accordance with the Privacy Act of 1974.

9.4.2 Information Treated as Private

The CA must protect all subscribers' personally identifying information (PII) from unauthorized disclosure. The contents of the archives maintained by the USPTO Operational Authority must not be released except as required by law.

Collection of PII must be limited to the minimum necessary to validate the identity of the subscriber. This may include attributes that correlate identity evidence to authoritative sources. The RA must provide explicit notice to the subscriber regarding the purpose for collecting and maintaining a record of the PII necessary for identity proofing and the consequences for not providing the information. PII collected for identity proofing purposes must not be used for any other purpose.

9.4.3 Information not Deemed Private

Information included in certificates is not subject to protections outlined in section 9.4.2, but may not be sold to a third party.

Certificates that contain the FASC-N in the subject alternative name extension, such as PIV Authentication Certificates, must 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.

All information collected as part of the identity proofing process must be protected to ensure confidentiality and integrity. In the event the Entity terminates PKI activities, it must be responsible for disposing of or destroying sensitive information, including PII, in a secure manner, and maintaining its protection from unauthorized access until destruction.

9.4.5 Notice and Consent to Use Private Information

The USPTO PKI Operational Authority is not required to provide any notice or obtain the consent of the subscriber or authorized USPTO 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 CAs and RAs will not disclose certificate or certificate-related information to any third party unless authorized by this Policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. Any third-party request or court order for release of information must be immediately directed to the USPTO General Counsel. Any request for release of information must be processed according to 41 CFR 105-60.605.

9.4.7 Other Information Disclosure Circumstances

No stipulation

9.5 Intellectual Property Rights

Any patent or copyright covering products or processes derived from this CP or compliant CPS must be licensed to users on a reasonable and nondiscriminatory royalty basis.

9.6 Representations and Warranties

The obligations described below pertain to all USPTO CAs.

9.6.1 CA Representations and Warranties

CAs operating under this policy must 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.

The CA database provides the key escrow repository and fulfills the requirements necessary to provide key recovery services.

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

- Provide a CPS to the Policy, as well as notice of 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 who comply with this policy and the associated CPS;
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating that information contained in the certificates;
- Revoking the certificates of subscribers found to have acted in a manner counter to subscriber obligations in accordance with section 9.6.3;
- Operating or providing for the services of an online repository that satisfies the obligations, and informing the repository service provider of those obligations if applicable.

9.6.2 RA Representations and Warranties

An RA who performs registration functions as described in this policy must comply with the stipulations of this policy and comply with a CPS approved by the Policy Authority 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 must conform to the stipulations of this document, including:

- Maintaining its operations in conformance to the general 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 informing subscribers of the consequences of not complying with those obligations.

9.6.3 Subscriber Representations and Warranties

A subscriber must be required to sign a document containing the requirements the subscriber must meet respecting protection of the private key and use of the certificate before being issued the certificate. Wherever possible, subscriber documents must be digitally signed.

Subscribers must:

- Accurately represent themselves in all communications with the PKI authorities and other subscribers;
- Protect their private keys at all times, in accordance with this policy, as stipulated in their subscriber agreements, certificate acceptance agreements and local procedures;
- Promptly notify the CA upon suspicion of loss or compromise of their private keys. Such notification must be made directly or indirectly through mechanisms consistent with the CPS;
- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates;
- Subscribers must provide accurate identification and authentication information during key recovery request.

- PKI Sponsors assume the obligations of subscribers for the certificates associated with their devices.

9.6.4 Relying Party 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..

9.6.5 Representations and Warranties of Affiliated Organizations

Affiliated Organizations must authorize the affiliation of subscribers with the organization, and must inform the USPTO CA of any severance of affiliation with any current subscriber.

9.6.6 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 must not be liable to any party, except as determined pursuant to the Federal Tort Claims Act, 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 USPTO PKI Policy Authority. This CP has no specified term.

9.10.2 Termination

Termination of this CP is at the discretion of the USPTO 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 & Communications with Participants

Any planned change to the infrastructure that has the potential to affect the FPKI operational environment must be communicated to the FPKIPA at least two weeks prior to implementation,

and all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change must be provided to the FPKIPA within 24 hours following implementation.

For all other communications, no stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

The Policy Authority must review this policy at least once every year. Corrections, updates, or suggested changes to this CP must be publicly available. 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 must be distributed electronically to USPTO PKI Policy Authority 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 USPTO PKI Policy Authority determines that a change in the CP reduces the level of assurance provided.

9.13 Dispute Resolution Provisions

The USPTO PKI PA is the final authority to resolve disputes arising with respect to this policy or certificates issued under this policy.

9.14 Governing Law

United States Federal law (statute, case law, or regulation) must govern the construction, validity, performance and effect of certificates issued under this CP for all purposes.

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 must remain in effect until the CP is updated. The process for updating this CP is described in section 9.12.1.

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

Number	Title	Revision	Date
AUDIT	FPKI Annual Review Requirements	V 1.2	May 6, 2022
FCPCA CP	X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework	V 2.7	February 2, 2024
FBCA CP	X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)	V 3.4	February 2, 2024
FIPS 140-3	Security Requirements for Cryptographic Modules https://csrc.nist.gov/		03-22-2019
FIPS 186-5	Digital Signature Standard (DSS) https://csrc.nist.gov/pubs/fips/186-5/final		February 3, 2023
FIPS 201-3	Personal Identity Verification (PIV) of Federal Employees and Contractors https://csrc.nist.gov/pubs/fips/201-3/final		January 2022
RFC 3447	Public Key Cryptographic Standard (PKCS) #1 v2.1: RSA Cryptography Standard		February 2003
RFC 7292	PKCS #12: Personal Information Exchange Syntax	1.1	July 2014
RFC 4210	Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)		September 2005
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile		May 2008
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework		November 2003
SP 800-63-3	Digital Identity Guidelines	3	June 2017
SP 800-78-4	Cryptographic Algorithms and Key Sizes for Personal Identity Verification		May 2015
SP 800-76-2	Biometric Specifications for Personal Identity Verification		July 2013

11 ACRONYMS AND ABBREVIATIONS

Acronym	Defintion
CA	Certification Authority
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Objects Registry
CSS	Certificate Status Service
DN	Distinguished Name
ECDSA	Elliptic Curve Digital Signature Algorithm
FBCA	Federal Bridge Certification Authority
FIPS PUB	(US) Federal Information Processing Standards Publication
FPKI	Federal Public Key Infrastructure
FPKI OA	Federal Public Key Infrastructure Operational Authority
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
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
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

Acronym	Defintion
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
USPTO	United States Patent and Trademark Office
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
VME	Virtual Machine Environment
WWW	World Wide Web

12 GLOSSARY

Term	Definition
access	Ability to make use of any information system 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]
applicant	The subscriber is sometimes also called an "applicant" after applying to a CA for a certificate, but before the certificate issuance procedure is completed.
archive	Long-term, physically separate storage.
audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
audit data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
binding	Process of associating two related elements of information. [NS4009]
biometric	A physical or behavioral characteristic of a person.
Certification Authority (CA)	An authority trusted by one or more users to create and assign certificates. [ISO9594-8]
CA facility	The collection of equipment, personnel, procedures and structures that are used by a CA to perform certificate issuance and revocation.

Term	Definition
Certificate	A digital representation of information which at least (1) identifies the CA 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 CA issuing it. [ABADSG]
certificate-related information	Information, such as a subscriber's postal address, that is not included in a certificate, but that may be used by a CA in certificate management.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [Federal Information Processing Standard 140]
Custodial Subscriber Key Stores	Custodial Subscriber Key Stores hold keys for a number of Subscriber certificates in one location.
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 or decrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. The process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate is sometimes referred to as key management.
firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
Hypervisor	Computer software, firmware or hardware that creates and runs virtual machines. A hypervisor uses native execution to share and manage hardware, allowing for multiple environments which are isolated from one another, yet exist on the same physical machine. Also known as an isolation kernel or virtual machine monitor.

Term	Definition
inside threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
integrity	Protection against unauthorized modification or destruction of information. [NS4009]
intellectual property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
key escrow	The retention of the private component of the key pair associated with a subscriber's encryption certificate to support key recovery.
key exchange	The process of exchanging public keys (and other information) in order to establish secure communication.
key generation material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
naming authority	An organizational entity responsible for assigning distinguished names and for assuring that each distinguished name is meaningful and unique within its domain.
non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009]
outside threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
PKI Sponsor	Fills the role of a subscriber for non-human system components or organizations that are named as public key certificate subjects, and is responsible for meeting the obligations of subscribers as defined throughout this document.
privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	Entity responsible for verification of subscriber identity and generation and issuance of subscriber certificates.

Term	Definition
Root Certification Authority	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application.
Relying Party	A person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them. [ABADSG]
renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates. [ABADSG]
risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
risk tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
server	A system entity that provides a service in response to requests from clients.
signature certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate. [ABADSG].
superior Certification Authority	In a hierarchical PKI, a CA who has certified the certificate signing key of another CA, and who constrains the activities of that CA. (see subordinate Certification Authority)
Supervised Remote Identity Proofing	A real-time identity proofing event where the RA/Trusted Agent is not in the same physical location as the applicant/subscriber. The RA/Trusted Agent controls a device which is utilized by the applicant/subscriber in order to ensure the remote identity proofing process employs physical, technical and procedural measures to provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person identity proofing process. Supervised Remote Identity Proofing must meet the criteria specified in NIST SP 800-63A Section 5.3.3; and must have the capacity to capture an approved biometric when utilized for PIV-I credential issuance.

Term	Definition
system equipment configuration	A comprehensive accounting of all system hardware and software types and settings.
technical non-repudiation	The contribution public key mechanisms make to the provision of technical evidence supporting a non-repudiation security service.
threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
trust list	Collection of Trusted Certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of a CA in confirming Subscriber identification during the registration process. Trusted agents do not have automated interfaces with certification authorities. ***Note***: At the time of publication, USPTO does not use Trusted Agents in the Identify Proofing process. This entity is commonly used in SSP business models.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure, authenticated delivery. The public keys included in Trusted Certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
two-person control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. [NS4009]
update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Virtual Machine Environment	An emulation of a computer system (in this case, a CA) that provides the functionality of a physical machine in a platform-independent environment. They provide functionality needed to execute entire operating systems.
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. [Federal Information Processing Standard 140]