Certificate Policy
for the
United States Patent and Trademark Office

June 03, 2022
Version 4.1

Prepared by:

United States Patent and Trademark Office
Public Key Infrastructure Policy Authority

Approved: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2022.06.21 13:45:26 -04'00' Date: _____

Don Watson
Chief Information Security Officer

This page is intentionally left blank.

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 Updated outdated NIST security terms and documentation references in sections 10 and11.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			Updated outdated USPTO organization names and terms in sections 1.5.3, 6.1.3, 8.1, and 9.6.6.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

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.

This CP addresses the requirements for the USPTO at the assurance levels of basic, basic device, medium, medium hardware, medium device, medium device hardware, and card authentication. The word "assurance" used in this CP means how well a Relying Party can be certain of the identity binding between the public key and the entity whose subject name is cited in the certificate. It 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 automated 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 shall provide the following security management services:

- Key generation, storage, and 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.)

This CP is consistent with 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 a registered certificate policy object identifier (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. 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 what level of assurance can be placed in a certificate issued by a USPTO CA. A Certification Practice Statement (CPS) specifies how that CA establishes that assurance level.

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 *policyMappings* 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.

1.1.4 Scope

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

USPTO 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 which comply with the policy stipulations herein. 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}
fbca-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}

*__Note__: As of the release of this CPS, USPTO does not use derived PIV OIDs.

The requirements associated with the mediumDevice policy are identical to those defined for the Medium Assurance policy with the exception of identity proofing, re-key, and activation data.

The requirements associated with the mediumDeviceHardware policy are identical to those defined for the mediumHardware Assurance policy with the exception of identity proofing, re-key, and activation data. In this document, the term “device” is defined as a non-person entity (NPE), i.e., a hardware device or software application. The use of the basicDevice, mediumDevice and mediumDeviceHardware policies are restricted to devices and systems.

End-Entity certificates issued to devices after October 1, 2016 shall assert policies mapped to USPTO Basic Device, Medium Device or Medium Device Hardware policies. All other policies defined in this document should be reserved for human subscribers when used in End-Entity certificates.

This document includes policies specific to FIPS 201 Personal Identity Verification (PIV) of Federal Employees and Contractors.

- Certificates issued to users supporting authentication but not digital signature, where the corresponding private key is stored on a PIV Card, may contain id-fpki-common-authentication.
- Certificates issued to users supporting authentication where the private key is stored on a PIV Card and can be used without user authentication may contain id-fpki-common-cardAuth.

- Certificates issued to users, in accordance with NIST SP 800-157, supporting authentication, but not digital signature, where the corresponding private key is not stored on a PIV Card, may contain either id-fpki-common-derived-pivAuth-hardware or id-fpki-common-derived-pivAuth as appropriate.
- The id-fpki-common-piv-contentSigning policy shall only be asserted in certificates issued to devices that sign PIV data objects in accordance with [FIPS 201] or [SP 800-157].

The requirements associated with id-fpki-common-piv-contentSigning and id-fpki-common-pivicontentSigning are identical to id-fpki-common-devicesHardware, except where specifically noted in the text.

1.3 PKI ENTITIES

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 Entity 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 PKI 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 shall 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 shall 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.

1.3.1.7 USPTO Principal Certification Authority (CA)

The Principal CA is a CA within a PKI that has been designated to cross-certify directly with the FBCA (e.g., through the exchange of cross-certificates). The Principal CA issues either end-entity certificates, or CA certificates to other Entity or external party CAs, or both. Where the Entity operates a hierarchical PKI, the Principal CA is typically the Entity Root CA. Where the Entity operates a mesh PKI, the Principal CA may be any CA designated by the Entity for cross-certification with the FBCA.

This CP may refer to CAs that are "subordinate" to the Principal CA. The use of the term "subordinate CA" shall encompass any CA under the control of the Entity that has a certificate issued to it by the Entity Principal CA or any CA subordinate to the Principal CA, whether or not the Entity employs a hierarchical or other PKI architecture.

The Entity shall ensure that no CA under its PKI shall have more than one trust path to the FBCA (regardless of path validation results).

1.3.2 USPTO Certificate Authority

USPTO has established the Internal Certification Authority to provide certificates to USPTO personnel, contractor employees, non-human entities, and affiliates. This CPS distinguishes the term "Certification Authority" to mean the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to Subscribers.

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 that collects and verifies each subscriber's identity and information that is to be entered into the subscriber's public key certificates, and authorizes the CA to issue certificates to verified subscribers. The RA must perform its functions in accordance with a CPS approved by the PA.

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 authority information access (AIA) extension. OCSP servers that are locally trusted, as described in RFC 6960, are not covered by this policy.

1.3.6 Key Recovery

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

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.

1.3.7 Subscribers

There are two types of subscribers: human end users and Non-Person Entities (NPE) such as information systems or devices.

A human subscriber is the user to whom a certificate is issued (typically packaged in a smartcard or token).The human subscriber is the person whose name appears as the subject of the certificate and who asserts that they use the assigned key and certificate in accordance with the CP asserted in the certificate. Human subscribers to the USPTO PKI include, but are not limited to, USPTO employees, contractor employees, and other personnel requiring authenticated access to USPTO sensitive information or services. Other personnel for which PKI authentication may be required are foreign government and organization personnel and their contractors and agents who are part of the intellectual property community.

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

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.

1.3.8 Affiliated Organizations

Subscriber certificates may be issued in conjunction with an organization that has a relationship with the subscriber; this is termed an 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. A Relying Party uses a Subscriber's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the Subscriber. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

This CP makes no assumptions or limitations regarding the identity of Relying Parties. While Relying Parties are generally Subscribers, Relying Parties are not required to have an established relationship with the FBCA or an Entity CA.

1.3.10 Other Participants

USPTO may require the services of other security, community, and application authorities. If required, the FBCA or Entity CPS shall identify the parties, define the services, and designate the mechanisms used to support these services.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The sensitivity of the information processed or protected using certificates issued by USPTO CA will vary. Relying Parties must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Relying Party for its application and is not controlled by this CP. To provide sufficient granularity, this CP specifies security requirements at varying qualitative levels of assurance: Basic, Basic Device, Medium, Medium Hardware, Medium Device, Medium Device Hardware, and Card Authentication.

Certificates generated under this CP are for carrying out the business of the USPTO by providing authentication and security services. Transactions within and between the USPTO, USPTO external customers and international partners such as the Trilateral Offices of the European Patent Office, the Japan Patent Office, and the World Intellectual Property Organization are authorized.

The following table provides a brief description of the appropriate uses for certificates at each level of assurance defined in this CP. 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.

Assurance Level	Applicability
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 provides the level of assurance for use in FIPS 201 Personal Identity Verification (PIV) card certificates where the private key can be used without cardholder activation of the PIV card with a PIN. It is used in conjunction with Medium Hardware to provide the set of policies required for PIV card implementation.

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

No stipulation.

1.5 Policy Administration

1.5.1 Specification Administration Organization

The USPTO Policy Authority (PA) is responsible for the definition, revision and promulgation of this policy.

1.5.2 Contact Person

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

Correspondence Address:

Director of Cybersecurity Division
Office of Chief Information Officer
P.O. Box 1450
Alexandria, VA 22313-1450
Phone: (571) 272-8233
Electronic Mail: Don.Watson@USPTO.GOV

Location Address:

Director of Cybersecurity Division
Office of Chief Information Officer
600 Dulany Street

MDW 05D01
Alexandria, VA 22314

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 shall 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) shall determine if the CPS complies with this policy for a given level of assurance. 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 shall not be issued. Permanent changes to the CP, arising from temporary waivers, shall be reviewed by FPKIPA and may result in revocation of the cross-certificate by the FPKIPA.

In some cases, the PA may require the additional approval of an external authorized agency such as the FPKIPA. The PA shall 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 shall be based on an independent compliance auditor's results and recommendations. See section 8 for further details.

1.6 Definitions and Acronyms

See Sections 11 and 12.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

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

2.1.1 USPTO Repository Obligations

The USPTO CA may use a variety of mechanisms for posting information into a repository as required by this CP. These mechanisms at a minimum shall include:

- Encryption certificates that assert one or more of the policy OIDs;
- Current CRLs and CARLs;
- Cross-certificates where appropriate;
- CA's certificate for all certificate signing keys, including link certificates.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

USPTO CA certificates shall only contain valid Uniform Resource Identifiers (URIs) accessible by Relying Parties.

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

The USPTO CA shall 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.

2.2.2 Publication of CA Information

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

The CPS for the USPTO CA is considered sensitive information and shall not be publicly published. Contact the USPTO Cybersecurity Division Director for access.

2.2.3 Interoperability

Standards-based schemas for directory objects and attributes shall be used when certificates and CRLs are published in directories.

2.3 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.

2.4 Access Controls on Repositories

USPTO CAs shall protect any repository information not intended for public dissemination or modification. CA certificates, CRLs and CARLs in the repository shall be publicly available.

The USPTO General Counsel, under applicable Federal Laws, and Departmental and USPTO regulations shall determine access to other information in the CA repositories. The CPS shall define what information in the repository shall 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

The USPTO Certificate Authorities shall only generate and sign certificates that contain a Non-Null X.500 Distinguished Name (DN); the X.500 DN may also contain domain component elements or alternative name forms.

Certificates issued to CAs and RAs shall use the Distinguished Name form, and have an assurance level equal to, or greater than, the highest level of assurance of the certificates the CA issues to subscribers or other CAs. Subscriber DNs shall be assigned in accordance with section 3.1. Certificates may additionally assert an alternate name form subject to requirements set forth below intended to ensure name uniqueness.

The table below summarizes the naming requirements that apply to each level of assurance in use at USPTO.

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

The USPTO CA must assign Distinguished Names to all Subscriber certificates. These distinguished names are comprised of a base distinguished name (Base DN) and additional relative distinguished names (RDNs).

The distinguished name form of the federal employee subscribers:

- *cn=lastname, firstname, cn=Users, dc=USPTO, dc=gov*

The distinguished name form of the federal contractors:

- *cn=lastname, firstname (affiliate), cn=Users, dc=USPTO, dc=gov*

PIV Content Signing certificates shall clearly indicate the organization administering the CMS.

For PIV Card Authentication subscriber certificates, use of the subscriber common name is prohibited. These certificates shall include a pivFASC-N name type, where the value is the FASC-N of the subject's PIV card.

When id-fpki-common-cardAuth is asserted, the certificate's subject distinguished name must take the following form:

- *serialNumber=FASC-N, ou=U.S. Patent and Trademark Office, dc=USPTO, dc=gov*

Certificates issued under id-fpki-common-authentication or id-fpki-common-cardAuth must include a subject alternative name extension. The subject alternative name extension must include both:

- the pivFASC-N name type [FIPS 201], the value of which must be the FASC-N [PACS] of the subject's PIV credential; and
- a UUID encoded as a URI as specified in Section 3 of [RFC 4122].

Certificates issued under id-fpki-common-cardAuth must not include any other name in the subject alternative name extension.

3.1.2 Need for Names to be Meaningful

Names used in certificates issued by the USPTO PKI shall identify the subscriber to which they are assigned in a clear, consistent manner understood by Relying Parties.

The directory information tree shall accurately reflect organizational structures.

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.

User Principal Names (UPN) shall be unique and accurately reflect organizational structures.

3.1.3 Anonymity or Pseudonymity of Subscribers

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

DNs in certificates (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.

The Policy Authority along with Certificate Authorities and Registration Authorities shall enforce name uniqueness within the X.500 name space 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 shall resolve 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 shall be required to prove possession of the private key, which corresponds to the public key in the certificate request.

For signature keys, this may be done by the entity using its private key to sign a value 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 certificates in the name of an affiliated organization shall include the organization name, address and documentation of the existence of the organization.

USPTO does not issue organizational certificates.

3.2.3 Authentication of Individual Identity

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

3.2.3.1 Authentication of Human Subscribers

For Subscribers, the RA shall ensure that the applicant's identity information is verified in accordance with this CP and the applicable CPS. Process information depends upon the certificate level of assurance and must be addressed in the CPS.

The CAs RAs must record the information set forth below for issuance of each certificate.

- The identity of the person performing the identification; use one of the following;
  - An auditable record linking the authentication of the person performing the identification to their verification of each Applicant; or

- A signed declaration by that person that he or she verified the identity of the applicant as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

- If in-person or supervised remote[1] identity proofing is done, a unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The date and time of the verification; and either;
  - An auditable record indicating the applicant accepted the certificate; or
  - A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at (declaration under penalty of perjury) or comparable procedure under local law.

Practice Note: In those cases, in which the individual is in possession of a valid digital signature credential of equal or higher level of assurance or the signature certificate is generated immediately upon authentication of the applicant's identity, the applicant may sign the declaration of identity and certificate of acceptance using the digital credential. In the latter case, if the applicant fails to sign the declaration of identity, then the certificate must be revoked.

For All Levels except PIV: If an applicant is unable to perform face-to-face, either in-person or supervised remote, registration (e.g., a network device), the applicant may be represented by a trusted person already issued a digital certificate by the Entity. The trusted person will present information sufficient for registration at the level of the certificate being requested, for both himself/herself and the applicant whom the trusted person is representing.

For Basic and Medium Assurance Levels: An entity certified by a State or Federal Entity as being authorized to confirm identities may perform in-person authentication on behalf of the RA. The certified entity forwards the information collected from the applicant directly to the RA in a secure manner. Packages secured in a tamper-evident manner by the certified entity satisfy this requirement; other secure methods are also acceptable. Such authentication does not relieve the RA of its responsibility to verify the presented data.

For PIV Certificates: For certificates issued under id-fpki-common-authentication and id-fpki-common-cardAuth, identity must be verified in accordance with the requirements specified for issuing PIV in Section 2.7 of [FIPS 201].

At id-fpki-common-authentication, the Applicant must appear at the RA in person or via supervised remote identity proofing.

For id-fpki-common-hardware, RAs may accept authentication of an Applicant's identity attested to and documented by a trusted agent, assuming agency identity requirements are

[1] The minimum requirements associated with supervised remote identity proofing are described in NIST SP 800-63A, Digital Identity Guidelines: Enrollment and Identity Proofing, Section 5.3.3.

otherwise satisfied. Authentication by a trusted agent does not relieve the RA of its responsibility to verify required procedures were followed as described above.

For certificates issued under id-fpki-common-derived-pivAuth-hardware and id-fpki-common-derived-pivAuth, identity must be verified in accordance with the requirements specified for issuing derived credentials in [SP 800-157]. At id-fpki-common-derived-pivAuth-hardware, the Applicant must appear at the RA in person or via supervised remote.

The RA or CA must:

1) Verify that the request for certificate issuance to the Applicant was submitted by an authorized agency employee;
2) Use the PKI-AUTH authentication mechanism from Section 6 of [FIPS 201] to verify that the PIV Authentication certificate on the Applicant's PIV credential is valid and that the Applicant is in possession of the corresponding private key;
3) Maintain a copy of the Applicant's PIV Authentication certificate.

Seven days after issuing the derived credential, the CA should recheck the revocation status of the PIV Authentication certificate. This step can detect use of a compromised PIV credential to obtain a derived credential.

For certificates issued under id-fpki-common-derived-pivAuth-hardware, the Applicant must appear in person or via supervised remote to present the PIV credential and perform the PKI-AUTH authentication mechanism. The RA must perform a one-to-one comparison of the Applicant against biometric data stored on the PIV credential, in accordance with [SP 800-76], and must record and maintain the biometric sample used to validate the Applicant.

In cases where a 1:1 biometric match against the biometrics available on the PIV credential or in the chain-of-trust, as defined in [FIPS 201] is not possible:

1) The Applicant must present a government-issued form of identification (e.g., a passport or driver's license) in addition to the PIV credential, and
2) The RA must examine the presented credentials for biometric data that can be linked to the Applicant (e.g., a photograph on the credential itself or a securely linked photograph of the Applicant), and

The process documentation and authentication requirements must include the following:

- The identity of the person performing the authentication and either:
  - A signed declaration by that person that he or she verified the identity of the Applicant using the format set forth at [28 U.S.C. 1746] (declaration under penalty of perjury) or
  - An auditable record linking the authentication of the person performing the identification to their verification of each Applicant.
- Unique identifying number(s) from second form of identification of the Applicant, or a facsimile of the ID(s)
- The biometric of the Applicant
- The date and time of the verification

The table below summarizes the identification requirements for each level of assurance.

Assurance Level	Identification Requirements
Rudimentary	Not supported by USPTO
Basic	Identity may be established by in-person proofing before a Registration Authority or Trusted Agent; or remotely verifying information provided by applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are consistent with the application and sufficient to identify a unique individual. Address confirmation: a) Issue credentials in a manner that confirms the address of record supplied by the applicant; or b) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice.
Medium (all policies)	Identity shall be established by in-person or supervised remote proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are one Federal Government-issued Picture I.D., one REAL ID Act compliant picture ID[2], or two Non-Federal Government I.D.s, one of which shall be a photo I.D. Any credentials presented must be unexpired. Clarification on the trust relationship between the Trusted Agent and the applicant, which is based on an in-person antecedent identity proofing event, can be found in the FBCA Supplementary Antecedent, In-Person Definition document.

[2] REAL ID Act compliant IDs are identified by the presence of the DHS REAL ID star

Assurance Level	Identification Requirements
High	Not supported by USPTO

In the event an applicant is denied a credential based on the results of the identity proofing process, the Entity shall provide a mechanism for appeal or redress of the decision.

3.2.3.2 Authentication of Human Subscribers for Role-based Certificates

Individuals who apply for a Trusted Role must have an active USPTO PIV card which serves as the identify proofing requirements (section 3.2.3.1). Applicants must have a Sponsor who holds an individual certificate issued by the same CA at the same or higher assurance level as the role-based certificate. The applicant will digitally sign an appointment letter acknowledging the Trusted Role expectations, which will be forwarded to the OAA for approval/digital signature.

3.2.3.3 Authentication of Human Subscribers for Group Certificates

Normally, a certificate shall be issued to a single Subscriber. For cases where there are several entities acting in one capacity, and where non-repudiation for transactions is not desired, a certificate may be issued that corresponds to a private key that is shared by multiple Subscribers. The USPTO RAs shall record the information identified in Section 3.2.3.1 for a Sponsor from the Information Systems Security Office (ISSO) or equivalent before issuing a group certificate.

In addition to the authentication of the Sponsor, the following procedures shall be performed for members of the group:

- The ISSO or equivalent shall be responsible for ensuring control of the private key, including maintaining a list of Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time.
- The subjectName DN must not imply that the subject is a single individual, e.g. by inclusion of a human name form.
- The list of those holding the shared private key must be provided to, and retained by, the USPTO CA or its designated representative.
- The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations).

3.2.3.4 Authentication of Devices

Some computing and communications devices (e.g., routers and 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)
- Equipment public keys

- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information for the PKI Sponsor

These certificates shall be issued only to devices under the PKI Sponsor's organizational control (i.e., require registration and validation that meets all issuing agency's requirements, as well as requiring re-validation prior to being re-issued). When a human sponsor is changed, the new Sponsor shall review the status of each device under their sponsorship to ensure it is still authorized to receive certificates. The CPS shall describe procedures to ensure that certificate accountability is maintained.

The registration information shall 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 shall 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 shall not be included in certificates.

3.2.5 Validation of Authority

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

3.2.6 Criteria for Interoperation

The FPKI Policy Authority shall determine the criteria for cross-certification with the FBCA.

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 defined in the FBCA CP and the governing MOA will be followed.

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

Assurance Level	Routine Re-key Identity Requirements for Subscriber Signature and Encryption Certificates
Basic (all policies)	Identity may be established through use of current signature key, except that identity shall be reestablished through initial registration process at least once every 15 years from the time of initial registration.
Medium (all policies)	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration. For mediumDevice and mediumDeviceHardware certificates, identity may be established through the use of current signature key or using means commensurate with the strength of the certificate being requested, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration.
Card Authentication	Identity may be established in accordance with the requirements specified in FIPS 201.

3.3.2 Identification and Authentication for Re-key after Revocation

If a certificate has been revoked other than during a renewal or update process, the subscriber is required to go through the initial registration process described in Section 3.2 to obtain a new certificate, PIV or Trusted Role.

3.4 Identification and Authentication for Revocation Request

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

3.5 Identification and Authentication for Key Recovery Requests

The Security Officer 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 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 Internal 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.

3.5.2 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 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).

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

To cross-certify with the FBCA, USPTO shall fulfill the application requirements as specified in the U.S. Government Public Key Infrastructure Cross-Certification Criteria and Methodology. The FPKIPA shall act on the application and, upon making a determination to issue a certificate and entering into the MOA with the Entity, shall authorize the FPKIMA to issue the cross-certificate to the Entity.

The USPTO PKI RA shall perform the following steps when a prospective subscriber applies for a certificate:

- Establish the applicant's authorization (by the employing or sponsoring entity) to obtain a certificate (per section 3.2.3)
- Establish the identity of the applicant and record the identity proofing process (per Section 3.2.3)
- Obtain the applicant's public key and verify the applicant's possession of the associated private key (per Section 3.2.1)
- Verify any roles or authorization information requested for inclusion in the certificate

These steps may be performed in any order, but all must be completed prior to certificate issuance.

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	An authorized agency official, the Applicant, or a Trusted Agent on behalf of the Applicant
Device Certificate	The PKI Sponsor of the device

4.1.2 Enrollment Process and Responsibilities

All communications among PKI Authorities supporting the certificate application and issuance process among PKI authorities shall be authenticated and protected from modification. Communications may be electronic or out-of-band.

Any electronic transmission of shared secrets shall be protected.

Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the key-pair of the certificate.

Out-of-band communications shall protect the confidentiality and integrity of the data.

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

If databases or other sources are used to confirm Subscriber attributes, then these sources and associated information sent to a CA shall require:

- When information is obtained through one or more information sources, an auditable chain of custody be in place.
- All data received be protected and securely exchanged in a confidential and tamper evident manner, and protected from unauthorized access.

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

4.2 Certificate Application Processing

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

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of the subscriber must meet the requirements specified for subscriber authentication as specified in sections 3.2 and 3.3 of this CP. 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 shall inform the PKI Sponsor.

4.4 Certificate Acceptance

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

4.4.1 Conduct Constituting Certificate Acceptance

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

4.4.2 Publication of the Certificate by the CA

As specified in 2.2, all CA certificates shall be published in repositories.

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 shall 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 shall 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

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

For Medium, Medium Hardware, Basic, and Basic Hardware Assurance certificates, subscribers shall protect their private keys from access by other parties. No stipulation is made for Card Authentication.

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 shall issue CRLs specifying the current status of all unexpired certificates. It is recommended that Relying Parties process and comply with this information whenever using USPTO certificates in a transaction.

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

No stipulation.

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.

CA certificates are published as specified in 2.2.1.

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

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

After certificate rekey, the old certificate may or may not be revoked, but must not be further re-keyed, renewed or modified.

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

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

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

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

4.7.3 Processing Certificate Re-keying Requests

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

No stipulation.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

No stipulation.

4.7.6 Publication of the Re-keyed Certificate by the CA

All CA certificates must be published as specified in section 2.2.1.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate Modification

Modifying a certificate means creating a new certificate that has the same or a different key, 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 further re-keyed, renewed, or modified.

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 corresponding operating authority may request modification.

Subscribers with a currently valid certificate may request certificate modification. For device certificates, the human 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

No stipulation; as specified in Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

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

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation; 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 shall issue CRLs covering all unexpired certificates issued under this policy.

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

4.9.1 Circumstances for Revocation

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

- 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;
- The private key is suspected of compromise;
- The subscriber or other authorized party (as defined in the Certificate Authority's 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 shall be revoked and placed on the CRL. In addition, if it is determined subsequent to issuance of new certificates that a private key used to sign requests for one or more additional certificates may have been compromised at the time the requests for additional certificates were made, all certificates authorized by directly or indirectly chaining back to that compromised key shall be revoked. Revoked certificates shall be included on all new publications of the CRL until the certificates expire.

4.9.2 Who can Request a Revocation

Within the PKI, 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 associated CPS. Subscribers may request revocation of their own certificates, and PKI Sponsors may request revocation of certificates they sponsor.

The CA shall 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 shall publicly disclose the instructions through a readily accessible online means.

4.9.3 Procedure for Revocation Request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The steps involved in the process of requesting a certificate revocation shall 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; and
- 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 shall 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

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

4.9.6 Revocation Checking Requirements for Relying Parties

No stipulation.

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/CARL Issuance Frequency

CRLs and CARLs are periodically issued and posted to a repository, even if there are no changes or updates to be made, to ensure timeliness of information. CRLs may be issued more frequently than required.

Certificate status information shall 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 shall never exceed 31 days.

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

4.9.8 Maximum Latency for CRLs

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

4.9.9 Online Revocation / Status Checking Availability

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

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; and
- The alternative method must meet the issuance and latency requirements for CRLs stated in sections 4.9.7 and 4.9.8.

4.9.12 Special Requirements Related to Key Compromise

When a CA or subscriber certificate is revoked for reason of compromise or suspected compromise of a private key, the associated CRL shall be issued immediately. When an offline CA issues a periodic CRL upon revocation of a CA certificate, the CA shall also use out of band mechanisms to notify all CAs with whom it has cross-certified of the certificate revocation. The following table provides CRL issuance requirements for all other CAs.

Table 4-1: CRL Issuance Requirements for Certification Authorities

Assurance Level	Routine CRL Issuance Frequency	CRL Issuance for Loss or Compromise of Private Key
Basic (all policies)	At least every 18 hours	Within 18 hours of notification
Medium (all policies)	At least every 18 hours	Within 18 hours of notification

Assurance Level	Routine CRL Issuance Frequency	CRL Issuance for Loss or Compromise of Private Key
Medium Hardware	At least every 18 hours	Within 18 hours of notification

4.9.13 Circumstances for Suspension

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

4.9.14 Who Can Request Suspension

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

4.9.15 Procedure for Suspension Request

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

4.9.16 Limits on Suspension Period

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

4.10 Certificate Status Services

No stipulation.

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

No stipulation.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

CA private keys are never escrowed.

The CA issuing the subscriber certificate shall escrow all private encryption keys.

Subscriber key management keys must be escrowed to provide key recovery.

Key Recovery policies and practices must satisfy privacy and security requirements for USPTO CAs issuing and managing digital certificates under this CP.

Escrowed keys must be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber.

Under no circumstances shall a third party escrow a subscriber signature key.

4.12.1.1 Key Escrow Process and Responsibilities

Human subscriber private keys (i.e., decryption private keys) associated with a key management certificate must be securely escrowed. The CA must ensure that the keys are escrowed successfully prior to issuance of the key management certificates.

Subscriber private keys must be protected during transit and storage using cryptography at least as strong as the key being escrowed.

Subscribers must be notified that the private keys associated with their encryption certificates will be escrowed.

4.12.1.2 Key Recovery Process and Responsibilities

Communications between the various key recovery participants must be secured from protocol threats such as disclosure, modification, replay, and substitution. The strength of all cryptographic protocols must be equal to or greater than that of the keys they protect.

During delivery, escrowed keys must be protected against disclosure to any party except the Requestor.

When any mechanism that includes a shared secret (e.g., a password) is used to protect the key in transit, the mechanism must ensure that the Requestor and the transmitting party are the only holders of this shared secret.

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

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

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

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

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

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

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when "open" and secured when 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 shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 Physical Access for RA Equipment

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

5.1.2.3 Physical Access for CSS Equipment

Physical access control requirements for CSS Validation Authority, shall 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 shall meet the CA physical access requirements specified in 5.1.2.1.

5.1.3 Power and Air Conditioning

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

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

5.1.4 Water Exposures

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

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

5.1.5 Fire Prevention and Protection

The facility housing the CA shall be protected with smoke and fire detectors. The facility includes zoned ceiling sprinkler and a zoned Halon-based fire suppression system.

5.1.6 Media Storage

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

5.1.7 Waste Disposal

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

5.1.8 Off-site Backup

Full system backups, sufficient to recover from system failure, shall be made on a periodic schedule. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an offsite location (separate from the CA equipment). Only the latest backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA 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 diligent and trustworthy as described in the next section. The functions performed in these roles form the basis of trust in the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first approach is to ensure that the person filling the role is trustworthy and properly trained. The second is to distribute the functions of the role among several people, so that any malicious activity requires collusion.

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 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 shall comply with 5.2.4, and requirements for two person control with 5.2.2, regardless of the titles and numbers of Trusted Roles.

5.2.2 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

5.2.3 Identification and Authentication for Each Role

At all assurance levels, an individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.2.4 Separation of Roles

Role separation, when required as set forth below, may be enforced either by the CA equipment, or procedurally, or by both means.

Requirements for the separation of roles, and limitations on use of procedural mechanisms to implement role separation, are described below for each level of assurance:

Assurance Level	Role Separation Rules
Basic	Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role; however, no one individual shall assume both the Officer and Administrator roles. This may be enforced procedurally. No individual shall be assigned more than one identity.
Medium (all policies)	Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may only assume one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA, CMS, and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and assume both the Auditor and Officer roles. No individual shall have more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

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

All persons filling trusted roles as identified in Section 5.2.1 shall be selected on the basis of loyalty, trustworthiness and integrity. Employees and contractors who fill these trusted roles shall be U.S. citizens. The requirements governing the qualifications, selection, and oversight of individuals who operate, manage, oversee, and audit the CA shall be set forth in the CPS. The Operational Authority shall identify at least one individual or group responsible and accountable for the operation of each CA with USPTO.

5.3.2 Background Check Procedures

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

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

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

A competent adjudication authority using a process consistent with Executive Order 12968 August 1995 or later, or an equivalent level shall adjudicate the background investigation.

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

5.3.3 Training Requirements

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

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

Documentation detailing the following shall be kept:

- The name and role of the person receiving training;
- The scope of the training; and
- The dates of the training.

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

The Policy Authority shall 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 Contracting Personnel Requirements

Contractor personnel employed to operate any part of the CA shall 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 shall be provided to the personnel filling that role. This documentation includes:

- This CP;
- Relevant portions of the CPS, Contingency Plan, and key recovery procedure;
- Any relevant statutes, policies, and/or contracts; and any relevant programmatic documentation (e.g., Life Cycle Management documentation); and
- Any handbooks, guidelines, or instructional manuals that have been developed to ensure that personnel filling trusted roles are adequately trained.

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

5.4 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the CA. For CAs operated in a virtual machine environment (VME), audit logs shall be generated for all applicable events on both the virtual machine (VM) and isolation kernel (i.e. hypervisor).

Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanisms shall be used. All security audit logs, both electronic and non-electronic, shall be retained and managed as records, and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with the retention period for archives as described in Section 5.5.2.

5.4.1 Types of Events Recorded

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

- The type of event;
- The date and time the event occurred;
- A success or failure indicator when executing the CA's signing process;

- A success or failure indicator when performing certificate revocation; and
- The identity of the entity and/or operator of the CA that caused the event.

A message from any source requesting an action by the CA is an auditable event. The message must include message date and time, source, destination, and contents.

At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

Auditable Event	Basic	Medium
SECURITY AUDIT		
Any changes to the Audit parameters, e.g., audit frequency and type of event audited	X	X
Any attempt to delete or modify the Audit logs	X	X
Obtaining a third-party time-stamp	X	X
IDENTIFICATION AND AUTHENTICATION		
Successful and unsuccessful attempts to assume a role	X	X
The value of maximum authentication attempts is changed	X	X
Maximum authentication attempts unsuccessful authentication attempts occur during user login	X	X
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X
An administrator changes the type of authenticator, e.g., from password to biometrics	X	X
LOCAL DATA ENTRY		
All security-relevant data that is entered in the system	X	X
REMOTE DATA ENTRY		
All security-relevant messages that are received by the system	X	X
DATA EXPORT AND OUTPUT		
All successful and unsuccessful requests for confidential and security-relevant information	X	X
KEY GENERATION		
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X
PRIVATE KEY LOAD AND STORAGE		

Auditable Event	Basic	Medium
The loading of Component private keys	X	X
All access to certificate subject private keys retained within the CA for key recovery purposes	X	X
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE		
All changes to the trusted public keys, including additions and deletions	X	X
SECRET KEY STORAGE		
The manual entry of secret keys used for authentication	X	X
PRIVATE AND SECRET KEY EXPORT		
The export of private and secret keys (keys used for a single session or message are excluded)	X	X
CERTIFICATE REGISTRATION		
All certificate requests	X	X
CERTIFICATE REVOCATION		
All certificate revocation requests	X	X
CERTIFICATE STATUS CHANGE APPROVAL		
The approval or rejection of a certificate status change request	X	X
CA CONFIGURATION		
Any security-relevant changes to the configuration of the CA	X	X
ACCOUNT ADMINISTRATION		
Roles and users are added or deleted	X	X
The access control privileges of a user account or a role are modified	X	X
CERTIFICATE PROFILE MANAGEMENT		
All changes to the certificate profile	X	X
REVOCATION PROFILE MANAGEMENT		
All changes to the revocation profile	X	X
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT		
All changes to the certificate revocation list profile	X	X
MISCELLANEOUS		
Appointment of an individual to a trusted role	X	X
Designation of personnel for multiparty control	X	X

Auditable Event	Basic	Medium
Installation of the operating system	X	X
Installation of the CA	X	X
Installing hardware cryptographic modules	If applicable	X
Removing hardware cryptographic modules	If applicable	X
Destruction of cryptographic modules	X	X
System Startup	X	X
Logon Attempts to CA Apps	X	X
Receipt of Hardware / Software		X
Attempts to set passwords	X	X
Attempts to modify passwords	X	X
Backing up CA internal database	X	X
Restoring CA internal database	X	X
File manipulation (e.g., creation, renaming, moving)		X
Posting of any material to a repository		X
Access to CA internal database		X
All certificate compromise notification requests	X	X
Loading tokens with certificates		X
Shipment of tokens		X
Zeroizing tokens	X	X
Re-key of the CA	X	X
Configuration changes to the CA server involving:		
- -Hardware	X	X
- -Software	X	X

Auditable Event	Basic	Medium
- -Operating System	X	X
- -Patches	X	X
- -Security Profiles		X
PHYSICAL ACCESS / SITE SECURITY		
Personnel Access to room housing CA		X
Access to the CA server		X
Known or suspected violations of physical security	X	X
ANOMALIES		
Software Error conditions	X	X
Software check integrity failures	X	X
Receipt of improper messages		X
Misrouted messages		X
Network attacks (suspected or confirmed)	X	X
Equipment failure	X	X
Electrical power outages		X
Alternate power supply failure		X
Obvious and significant network service or access failures		X
Violations of Certificate Policy	X	X
Violations of Certification Practice Statement	X	X
Resetting operating system clock	X	X

5.4.2 Frequency of Processing Data

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 shall align with the CA audit log processing frequency.

All significant events shall be explained in an audit log summary.

Assurance Level	Review Audit Log
Basic (all policies)	At least once per month
Medium (all policies)	At least once per month

5.4.3 Retention Period for Security Audit Data

Audit logs must remain on site until they have been reviewed, in addition to being archived as described in Section 5.5. The individual who removes audit logs from the CA or system shall be an official different from the individuals who, in combination, control the CA signature key.

5.4.4 Protection of Security Audit Data

The USPTO Internal CA system configuration and procedures must be implemented together to ensure that:

- Only personnel assigned to trusted roles have read access to the logs;
- Only authorized people may archive audit logs;
- Audit logs are not modified.

The entity performing security audit data archive need not have modify access, but procedures must be implemented to protect archived data from deletion or destruction prior to the end of the security audit data retention period (note that deletion requires modification access).

Security audit data shall be moved to a safe, secure storage location separate from the CA equipment.

5.4.5 Security Audit Data Backup Procedures

Audit logs and audit summaries, should they be produced, shall be backed up at least monthly. A copy of audit logs shall be sent off-site in accordance with the CPS on no less than a monthly basis.

5.4.6 Security Audit Collection System (Internal vs. External)

The audit log collection system may or may not be external to the CA system. Security audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated security audit system has failed and the integrity of the system or confidentiality of the information protected by the system is at risk, the Operational Authority Administrator shall determine whether to suspend CA operation until the problem is corrected. Audit collection systems shall be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files).

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

The Operational Authority shall perform routine self-assessment of security controls for evidence of malicious activity.

5.5 Records Archival

CA archive records shall be sufficiently detailed to establish the proper operation of the CA or the validity of any certificate (including those revoked or expired) issued by the CA. Procedures detailing how to create, verify, package, transmit, and store archive information shall be published in the CPS.

5.5.1 Types of Events Archived

- At a minimum, the following data shall be recorded for archive for all assurance levels:
- CA accreditation (if applicable)
- Certificate policy
- Certification Practice Statement
- Contractual obligations and other agreements concerning operations of the CA
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- Revocation requests
- 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
- Record of Re-Key
- All CRLs and CARLs issued and/or published
- All Audit Logs
- Other data or applications to verify archive contents
- Compliance Auditor reports
- Any changes to the Audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- Whenever the CA generates a key (Not mandatory for single session or one-time use symmetric keys)
- All access to certificate subject private keys retained within the CA for key recovery purposes
- All changes to the trusted public keys, including additional and deletions
- The export of private and secret keys (keys used for a single session or message are excluded)
- The approval or rejection of a certificate status change request

- Appointment of an individual to a Trusted Role
- Destruction of cryptographic modules
- All certificate compromise notifications
- Remedial action taken as a result of violations of physical security
- Violations of Certificate Policy
- Violations of Certificate Practice Statement
- Auditor Training

5.5.2 Retention Period for Archive

The USPTO PKI shall retain archive records for the minimum retention periods as identified below.

Assurance Level	Minimum Retention Period
All Basic levels	7 years and 6 months
All Medium levels	10 years and 6 months

5.5.3 Protection of Archive

No unauthorized user shall be able to write to, modify or delete the archive, but archived records may be moved to another medium. The contents of the archive shall not be released except as determined by the Policy Authority at the direction of the USPTO General Counsel in accordance with USPTO policy, or as required by law and in accordance with Departmental and USPTO regulations. Records of individual transactions may be released upon request of any subscribers involved in the transaction, or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the CA.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Alternatively, an entity may retain data using whatever procedures, if any, the National Archives and Records Administration has recommended. Applications required to process the archive data shall also be maintained for a period determined by the Policy Authority.

The USPTO PKI shall follow the USPTO Records Schedule approved by the National Archives and Records Administration for records generated in the establishment and operation of the USPTO CA.

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 shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time stamping are maintained in synchrony with an authoritative time source.

5.5.6 Archive Collection System (Internal vs. External)

Archive data may be collected in any expedient manner.

5.5.7 Procedures to Obtain Archive Information

Information held in USPTO CA record archives will be retrieved from archive and transmitted to requesting entities using standard operating procedures for records management and transfer of information as practiced by USPTO. The contact information for requesting archived records shall be specified in the relevant CPS.

The contents of the archive shall not be released except as determined by the Policy Authority at the direction of the USPTO General Counsel in accordance with USPTO policy, or as required by law and in accordance with departmental and USPTO regulations.

Any archived record that contains private keys, for example escrowed private encryption keys, shall only be transferred via trusted, secure communications channels, or shall be hand delivered to a specifically authorized recipient who shall give a signed receipt for the delivery. If authorized by the USPTO General Counsel, transfer of archived records that contain private keys may be through a commercial delivery service, using a method that requires a single specified recipient that must sign a receipt which is returned to USPTO.

5.6 Certification Authority Key Changeover

The CA's signing key shall 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. From that time on, only the new key will be used for certificate signing purposes. 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 shall be available for all Relying Parties until the validity period of all issued certificates has past. 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 shall notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed.

CAs that distribute self-signed certificates shall generate key rollover certificates, where the new public key is signed by the old private key, and vice versa. This permits acceptance of newly issued certificates and CRLs without distribution of the new self-signed certificate to current users. Key rollover certificates are optional for CAs that do not distribute self-signed certificates.

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

5.7 Compromise and Disaster Recovery

The CA and repository shall 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 shall implement features to provide high levels of reliability. The following subsections outline the policy for instances that may prevent such maintenance of reliability.

The CA shall 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 following:

- Suspected or detected compromise of the CA systems;
- Physical or electronic penetration of CA systems;
- Successful denial of service attacks on CA components; or
- Any incident preventing the CA from issuing a CRL within 24 hours of the issuance of the previous CRL.

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

In the event of an incident as described above, the CA must notify the Policy Authority within 24 hours of incident discovery, along with preliminary remediation analysis. The notification provided directly to the Policy Authority shall also include detailed measures taken to remediate the incident.

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 shall respond as follows:

- Before returning to operation, ensure that the system's integrity has been restored.
- If the CA signature keys are not destroyed, CA operation shall be reestablished 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 shall 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 shall be notified as soon as possible.

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 FPKI PA, 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 generate new keys in accordance with section 6.1.1.1.

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

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

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

The organization operating the CA shall 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 within 72 hours of failure.

In the case of a disaster whereby the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the Policy Authority shall be immediately and securely notified, and the Policy Authority shall take whatever action it deems appropriate.

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

5.8 Certification Authority Termination

In the event of termination of the CA operation, certificates signed by the CA shall be revoked. Prior to CA termination, the CA shall provide archived data to the Policy Authorities' approved archival facility, and the Policy Authority shall securely notify all appropriate authorities (e.g., the FBCA and cross-certified CAs.) of the situation at the earliest feasible time in accordance with applicable Memoranda of Agreement and any other contractual agreements. Any issued certificates that have not expired, shall be revoked and a final long term CRL with a nextUpdate time past the validity period of all issued certificates shall be generated. This final CRL shall be available for all Relying Parties until the validity period of all issued certificates has past. Once the last CRL has been issued, the private signing key(s) of the USPTO CA will be destroyed.

In the event that an Entity CA terminates operation, the Entity shall provide notice to the FBCA prior to termination.

Whenever possible, the FPKIPA shall be notified at least two weeks prior to the termination of any CA operated by an Entity cross certified with the FBCA. For emergency termination, CAs shall follow the notification procedures in Section 5.7.

.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

Cryptographic keying material used by CAs to sign certificates, CRLs, or status information shall be generated in a FIPS 140, Security Level 2 or higher, validated cryptographic module. Multiparty control is required for CA key pair generation. 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. This documentation must be detailed enough to show that appropriate role separation is used. An independent third party shall validate the process for all medium level assurance Certificate Authorities; 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

The subscriber, PKI Sponsor (for devices), CA, or RA may generate subscriber key pairs. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in section 6.1.2 must also be met.

Key generation shall be performed using a FIPS approved method.

Subscriber key pairs shall be generated in FIPS 140 Level 2 hardware cryptographic modules as specified in Section 6.2.1.

For PIV, all keys, with the exception of key management, must be generated on the card.

6.1.1.3 CSS Key Pair Generation

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

6.1.2 Private Key Delivery to Subscriber

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

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

- Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private key to the Subscriber.
- The private key must be protected from activation, compromise, or modification during the delivery process.
- The Subscriber shall acknowledge receipt of the private key(s).
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers.
    - For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it.
    - For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.
    - For shared key applications, organizational identities, and network devices, see also Section 3.2.

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

6.1.3 Public Key Delivery to Certificate Issuer

For CAs operating at the Basic or Medium (all policies) level of assurance, 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 shall bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate.

6.1.4 CA Public Key Delivery to Relying Parties

When a CA updates its signature key pair, the CA shall distribute the new public key in a secure fashion. The new public key may be distributed in a self-signed certificate, in a key rollover certificate, or in a new CA (e.g., cross-) certificate obtained from the issuer(s) of the current CA certificate(s).

Self-signed certificates shall be conveyed to Relying Parties in a secure fashion to preclude substitution attacks. Acceptable methods for trusted certificate delivery include, but are not limited to:

- The CA/RA loading trusted certificates onto tokens delivered to Relying Parties via secure mechanisms;

- Secure distribution of trusted certificates through secure out-of-band mechanisms;
- Comparison of 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); and
- Loading trusted certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.

Key rollover certificates are signed with the CA's current private key, so secure distribution is not required. To ensure the availability of the new public key, the key rollover certificates should be distributed using repositories.

6.1.5 Key Sizes and Signature Algorithms

All FIPS-approved signature algorithms are considered acceptable; additional restrictions on key sizes are detailed below.

For CAs that distribute self-signed certificates to Relying Parties, the CA's subject public keys in such certificates shall be at least 2048 bits for RSA, or at least 224 bits for ECDSA. Public keys in all self-signed certificates generated after 12/31/2010 that expire after 12/31/2030 shall be at least 3072 bits for RSA, or at least 256 bits for ECDSA.

CAs that generate certificates and CRLs under this policy shall use signature keys of at least 1024 bits for RSA or DSA, and at least 160 bits for ECDSA. Beginning 01/01/2011, all valid certificates shall be signed with keys of at least 2048 bits for RSA or at least 224 bits for ECDSA. All certificates, except self-signed certificates, that expire after 12/31/2030 shall be signed with keys of at least 3072 bits for RSA or at least 256 bits for ECDSA.

CAs that generate certificates and CRLs under this policy shall use SHA-224, SHA-256, SHA-384, or SHA-512 hash algorithm when generating digital signatures. Signatures on certificates and CRLs that are issued after 12/31/2010 shall be generated using, at a minimum, SHA-224. Signatures on certificates and CRLs that are issued after 12/31/2030 shall be generated using, at a minimum, SHA-256.

Where implemented, CSSs shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs.

End-entity certificates shall contain public keys that are at least 1024 bit for RSA, DSA, or Diffie-Hellman, or 160 bits for elliptic curve algorithms. The following special conditions also apply:

- End-entity certificates that expire after 12/31/2030 shall contain public keys that are at least 3072 bits for RSA or DSA, or 256 bits for elliptic curve algorithms.
- End-entity certificates that include a keyUsage extension that only asserts the *digitalSignature* bit that expire on or after 12/31/2013 shall contain public keys that are at least 2048 bits for RSA or DSA, or 224 bits for elliptic curve algorithms.
- Beginning 01/01/2011, all valid end-entity certificates that include a keyUsage extension that asserts the *nonRepudiation*, *keyEncipherment*, *dataEncipherment*, or *keyAgreement*

bit shall contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

- Beginning 01/01/2011, all valid end-entity certificates that do not include a keyUsage extension shall contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

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 shall require at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys through 12/31/2010.

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 2048 bit RSA or equivalent for the asymmetric keys after 12/31/2010 through 12/31.2030.

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 3072 bit RSA or equivalent for the asymmetric keys after 12/31/2030.

6.1.6 Public Key Parameters Generation

Public key parameters for signature algorithms defined in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186.

Parameter quality checking (including primality testing for prime numbers) shall be performed in accordance with FIPS 186.

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

Public keys that are bound into subscriber certificates shall be used only for signing or encrypting, but not both, except as specified below. The use of a specific key is constrained by the key usage extension in the X.509 certificate.

USPTO CA issued certificates and CA certificates shall set two key usage bits: *cRLSign* and/or *keyCertSign*. Where the subject signs OCSP responses, the certificate may also set the *digitalSignature* and/or *nonRepudiation* bits.

Subscriber certificates shall assert key usages based on the intended application of the key pair. Certificates to be used for digital signatures (including authentication) shall set the *digitalSignature* and *nonRepudiation* bits. Certificates to be used for key transport shall set the *keyEncipherment* bit. Certificates to be used for key agreement shall set the *keyAgreement* bit.

Certificates may include a single key for use with encryption and signature in support of legacy Secure Multipurpose Internet Mail Extensions applications. Such "dual-use" certificates shall be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CP. Such "dual-use" certificates shall never assert the

nonRepudiation bit, and shall not be used for authenticating data that will be verified on the basis of the dual-use certificate at a future time.

For End Entity certificates issued after June 30, 2019, the Extended Key Usage extension shall always be present and shall not contain *anyExtendedKeyUsage* {2.5.29.37.0}. Extended Key Usage OIDs shall be consistent with key usage bits asserted.

If a certificate is used for authentication of ephemeral keys, the key usage bit in the certificate must assert the *digitalSignature* bit and may or may not assert *keyEncryption* and *keyAgreement* depending on the public key in the certificate.

Certificates that assert id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth, or id-fpki-common-cardAuth are used solely for authentication.

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 shall 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 (All Policies)	Level 2 (Hardware or Software)	Level 1 (Hardware or Software)	Level 1 (Hardware or Software)
Medium (All Policies)	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
Card Authentication	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

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

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

PIV Cards shall 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.

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

6.2.1.1 Custodial Subscriber Key Stores

Custodial Subscriber Key Stores hold keys for a number of Subscriber certificates in one location. When a collection of private keys for Subscriber certificates are held in a single location there is a higher risk associated with compromise of that cryptographic module than that of a single Subscriber.

Cryptographic modules for Custodial Subscriber Key Stores shall be no less than FIPS 140 Level 2 Hardware.

In addition, authentication to the Cryptographic Device in order to activate the private key associated with a given certificate shall require authentication commensurate with the assurance level of the certificate.

6.2.2 Private Key Multi-Person Control

A single person shall 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 shall be under the same multi-person control as the original CA signing key. The names of the parties used for two-person control shall be maintained on a list that shall be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

6.2.3.1 Escrow of CA Private Signature Key

Under no circumstances shall a CA signature key used to sign certificates or CRLs be escrowed.

6.2.3.2 Escrow of CA Encryption Keys

Subscriber keys intended for encryption purposes may be escrowed to provide for key recovery in order that encrypted data may be recovered. The method for key escrow and recovery shall be described in the CA's CPS or Key Recovery Policy.

6.2.3.3 Escrow of Subscriber Private Signature Keys

Subscriber private signature keys shall not be escrowed.

6.2.3.4 Escrow of Subscriber Private Encryption and Dual Use Keys

Subscriber dual use keys shall not be escrowed. If a device has a separate key management key certificate, the key management private key may 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

6.2.4.1 Backup of Certification Authority Private Signature Key

The CA private signature keys shall be backed up under the same multi-person control as the original signature key, as specified in Section 5.2.2.

Backup of CA private signature keys is required to facilitate disaster recovery. Where required by Section 5.2.2, Entity CA private signature keys shall be backed up under multi-person control.

At least one copy of the CA private signature key shall be stored off site. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original.

6.2.4.2 Backup of Subscriber Private Signature Keys

Subscriber private signature keys associated with certificates asserting any mediumHardware OID may not be backed up or copied.

At the Basic or Medium levels of assurance, subscriber private signature keys whose corresponding public key is contained in a certificate asserting the CA under this policy may be backed up or copied, but must be held in the subscriber's control. Backed up subscriber private keys shall be stored in encrypted form and protected at a level no lower than stipulated for the primary instance of the key.

6.2.4.3 Backup of Subscriber Private Key Management Key

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

6.2.4.4 Backup of CSS Private Key

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

6.2.4.5 Backup of Common PIV Content Signing Key

The Common PIV Content Signing private signature keys shall be backed up under multi-person control. At least one copy of the private signature key shall be stored in a secondary location. All copies of the Common PIV Content Signing private signature key shall be accounted for and protected in the same manner as the original. Backed up Common PIV Content private signature

keys shall not be exported or stored in plaintext form outside the cryptographic module. Backup procedures shall be documented.

6.2.4.6 Backup of Device Private Keys

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

6.2.5 Private Key Archival

Private signature keys shall not be escrowed nor archived. CAs that retain subscriber private encryption keys for business continuity purposes shall archive such subscriber private keys, in accordance with section 5.5.

6.2.6 Private Key Transfer into or from a Cryptographic Module

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

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

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS 140.

6.2.8 Method of Activating Private Keys

At the Medium or Medium Hardware level of assurance, CA signing key activation requires multiparty control as specified in section 5.2.2.

The subscriber must be authenticated to the cryptographic module before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. When pass-phrases or PINs are used, they shall be a minimum of six (6) characters. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

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

Common Policy requirements for subscriber private key activation are listed in the following table:

Policy Asserted	Activation Requirements
id-fpki-common-hardware id-fpki-common-authentication id-fpki-common-derived-pivAuth id-fpki-common-derived-pivAuth-hardware	Passphrases, PINs or biometrics
id-fpki-common-devices	May be configured to activate the private key without requiring a human sponsor or authorized administrator to authenticate to the cryptographic token. The appropriate physical and logical access controls must be implemented for the device and its cryptographic token.
id-fpki-common-piv-contentSigning	May be configured to activate the private key without requiring a human sponsor or authorized administrator to authenticate to the cryptographic token. The appropriate physical and logical access controls must be implemented for content signing operations conformant with PIV issuance requirements (FIPS 201). The strength of the security controls must be commensurate with the level of threat in the PIV credential issuance system's environment, and must protect the hardware, software, and the cryptographic token and its activation data from compromise.
id-fpki-common-cardAuth	None

6.2.9 Method of Deactivating Private Keys

Cryptographic modules which have been activated, must not be left unattended or otherwise open to unauthorized access. After use, they must be deactivated, e.g. via a manual logout procedure, or by a passive timeout. CA cryptographic modules shall 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 shall destroy CA, RA, and CSS (e.g., OCSP server) private signature keys when they are no longer needed. Subscribers shall either surrender their cryptographic module to CA/RA personnel for destruction or destroy their private signature keys, when they are no longer needed or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a "zeroize" command. Physical destruction of hardware 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

The USPTO CA distributes a self-signed certificate for use as a trust anchor and shall limit the use of the associated private key to a maximum of 10 years.

Code and content signers may use their private keys for three years; the lifetime of the associated public keys shall not exceed eight years. Subscribers' signature private keys and certificates have a maximum lifetime of three years. Subscriber key management certificates have a maximum lifetime of 3 years; use of subscriber key management private keys is unrestricted.

For OCSP responders operating under this policy, the maximum key usage period is three years, with a certificate lifetime of 120 days.

Subscriber signature private keys and certificates have a maximum lifetime of three years. Subscriber key management certificates have a maximum lifetime of 3 years. The usage period for subscriber key management private keys is not restricted.

PIV authentication certificates, card authentication certificates, and digital signature certificates have a maximum lifetime of three years and must expire no later than the PIV card expiration date. PIV content signing certificates should not expire before the PIV card expires.

CAs must not issue subscriber certificates that extend beyond the expiration date of their own certificates and public keys.

The validity period of the subscriber certificate must not exceed the routine re-key Identity Requirements as specified in Section 3.3.1.

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, shall have an appropriate level of strength for the keys or data to be protected. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module. Where a USPTO CA uses passwords as activation data for the CA signing key, at a minimum the activation data shall be changed upon CA re-key. The password data shall be generated in conformance with FIPS 140 Level 2.

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 shall be:

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

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 shall include the following functionality:

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

For those portions of the CA operating in a Virtual Machine Environment (VME), the following security functions also pertain to the hypervisor:

- Require authenticated logins.
- Provide discretionary access control.

- Provide a security audit capability.
- Enforce separation of duties for PKI roles.
- Prohibit object reuse or require separation for CA random access memory.
- Require use of cryptography for session communication and database security.
- Archive CA history and audit data.
- Require self-test security-related FBCA services.
- Enforce domain integrity boundaries for security-critical processes.

The computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA and its ancillary parts shall include the following functionality (in a VME, these functions are applicable to both the VM and hypervisor):

- 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.
- Support recovery from key or system failure.

For Certificate Status Servers operating under this policy, the computer security functions listed below are required (in a VME, these functions are applicable to both the VM and hypervisor):

- 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.
- Support recovery from key or system failure.

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

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

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

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The System Development Controls for the CA are as follows:

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

6.6.2 Security Management Controls

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

No stipulation.

6.7 Network Security Controls

Network security controls shall be employed to protect the USPTO CA and its repositories. Networking equipment shall turn off unused network ports and services. Any network software present shall be necessary to the functioning of the equipment.

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

CA equipment, RAs, CMSs, repositories, directories, and remote workstations used to administer the CAs, and certificate status servers shall be located on internal networks behind boundary/perimeter network defenses and afforded protections consistent with commercial electronic commerce practices for network security controls. Services allowed to and from the CA equipment shall be limited to those required to perform CA functions. Other CA equipment may enable additional services consistent with local policy.

6.8 Time-Stamping

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

7 CERTIFICATE, CARL/CRL, AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version Numbers

The CA shall 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 shall comply with both the RFC 5280 and the Federal certificate and CRL profile guidelines.

CA certificates shall not include critical private extensions.

7.1.3 Algorithm Object Identifiers

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

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
id-RSASSA-PSS	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}
ecdsa-with-Sha224	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1}
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 shall be used to specify the hash in an RSASSA-PSS digital signature:

id-sha256	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1}
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 object identifiers for identifying the algorithm for which the subject key was generated.

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-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 shall be specified as one of the following named curves:

ansip192r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 1}
ansit163k1	{iso(1) identified-organization(3) certicom(132) curve(0) 1}
ansit163r2	{iso(1) identified-organization(3) certicom(132) curve(0) 15}
ansip224r1	{iso(1) identified-organization(3) certicom(132) curve(0) 33}
ansit233k1	{iso(1) identified-organization(3) certicom(132) curve(0) 26}
ansit233r1	{iso(1) identified-organization(3) certicom(132) curve(0) 27}
ansip256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}
ansit283k1	{iso(1) identified-organization(3) certicom(132) curve(0) 16}
ansit283r1	{iso(1) identified-organization(3) certicom(132) curve(0) 17}
ansip384r1	{iso(1) identified-organization(3) certicom(132) curve(0) 34}
ansit409k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 36 }
ansit409r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 37 }
ansip521r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 35 }
ansit571k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 38 }
ansit571r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 39 }

7.1.4 Name Forms

Where required as set forth in Section 3.1.1, the subject and issuer fields of the base certificate shall 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 shall assert name constraints in CA certificates as required.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this policy shall assert the object identifier appropriate to the level of assurance with which it was issued.

7.1.7 Usage of Policy Constraints Extension

CAs may assert policy constraints in CA certificates as required.

When this extension appears, at least one of *requireExplicitPolicy* or *inhibitPolicyMapping* must be present. When present, this extension should be marked as noncritical*****, to support legacy applications that cannot process *policyConstraints*. 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 will be set to 0.

******Note*: The recommended criticality setting is different from RFC 5280

7.1.8 Policy Qualifiers Syntax and Semantics

USPTO CAs shall 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 shall not contain a critical certificate policies extension.

7.1.10 Inhibit Any Policy Extension

The CAs may assert *InhibitAnyPolicy* in CA certificates. When present, this extension should be marked as noncritical*****, to support legacy applications that cannot process *InhibitAnyPolicy*. Skip Certs shall be set to 0, since certificate policies are required in the Federal PKI.

******Note*: The recommended criticality setting is different from RFC 5280.

7.2 CRL Profile

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

7.2.1 Version Numbers

CAs shall issue X.509 Version 2 CRLs and CARLs.

7.2.2 CRL and CRL Entry Extensions

Detailed CRL profiles addressing the use of each extension shall 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 shall sign responses using algorithms designated for CRL signing.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

All USPTO CAs are subject to an annual review by the FPKIPA to ensure their 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 their 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, one populated, representative PIV card must be submitted to the FIPS 201 Evaluation Program for testing.

8.2 Identity/Qualifications of Assessor

The auditor shall demonstrate competence in the field of compliance audits. The auditor must 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 shall be a private firm, that is independent from the entities being audited, or it shall be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. An example of the latter situation may be an agency inspector general. To insure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's CA Facility or Certificate Practices Statement. The Policy Authority shall determine whether a compliance auditor meets this requirement.

8.4 Topics Covered by Compliance Audit

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

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 shall be performed:

- The compliance auditor shall document the discrepancy and provide a copy to the USPTO Operational Authority;
- The compliance auditor shall 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 shall 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 shall submit an audit compliance annual review package to the FPKIPA. This package shall 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 shall identify the versions of the CP and CPS used in the assessment. Additionally, where necessary, the results shall 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 shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction, and shall 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 not requiring protection shall be made publicly available.

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

9.3.1 Scope of Confidential Information

The following information shall 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.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

A Privacy Threshold Assessment is conducted 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 shall protect all subscribers' personally identifying information (PII) from unauthorized disclosure. The contents of the archives maintained by the USPTO Operational Authority shall not be released except as required by law.

Collection of PII shall 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 shall 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 shall 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.

Certificates that contain the FASC-N in the subject alternative name extension, such as PIV Authentication Certificates, shall not be distributed via public repositories (e.g., via LDAP or HTTP).

9.4.4 Responsibility to Protect Private Information

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

All information collected as part of the identity proofing process shall be protected to ensure confidentiality and integrity. In the event the Entity terminates PKI activities, it shall 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 shall be immediately directed to the USPTO General Counsel. Any request for release of information shall 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 shall 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, USPTO PKI Operational Authority and USPTO PKI Operational Authority Officers.

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.

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

- Providing to the Policy Authority a CPS, 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 shall 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 shall 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 (or human sponsor for device certificates) shall be required to sign a document containing the requirements the subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. Wherever possible, subscriber documents must be digitally signed.

Subscribers shall:

- 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 shall be made directly or indirectly through mechanisms consistent with the CA's CPS;

- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates;
- PKI Sponsors assume the obligations of subscribers for the certificates associated with their devices.

9.6.4 Relying Parties Representations and Warranties

None.

9.6.5 Representations and Warranties of Affiliated Organizations

Affiliated Organizations shall authorize the affiliation of subscribers with the organization, and shall 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 shall 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 shall 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 shall review this policy at least once every year. Corrections, updates, or suggested changes to this CP shall 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 shall 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) shall 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 shall 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 https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-annual-review-requirements.pdf	V 1.0	April 11, 2017
FCPCA CP	X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework	V 2.2	12-1-2021
FBCA CP	X.509 Certificate Policy for the Federal Bridge Certificate Authority (FBCA)	V 2.35	15 April 2019
FIPS 140-3	Security Requirements for Cryptographic Modules https://csrc.nist.gov/		03-22-2019
FIPS 186-4	http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf		July 2013
FIPS 201-2	http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf		August 2013
FIPS 201-3	https://csrc.nist.gov/publications/detail/fips/201/3/final		January 2022
FOIAACT	http://www.usdoj.gov/oip/foiastat.htm		
FPKI-PA	https://www.idmanagement.gov/topics/fpkipa/		
ISO9594-8	ftp://ftp.bull.com/pub/OSIdirectotry/ITU/97x509final.doc		1997
ITMRA	http://www4.law.cornell.edu/uscode/40/1452.html		
NAG69C	Information System Security Policy and Certification Practice Statement for Certification Authorities,	Rev. C	November 1999
NARARMP	http://www.archives.gov/records-mgmt/policy/final-pki-guidance		14 March 2002
NSD42	National Policy for the Security of National Security Telecom and Information Systems		5 July 1990
RFC3447	Public Key Cryptographic Standard (PKCS) #1 v2.1: Rivest, Shamir, and Adleman Cryptography Standard http://www.ietf.org/rfc/rfc3447.txt		February 2003
RFC7292	PKCS #12: Personal Information Exchange Syntax	1.1	July 2014

Number	Title	Revision	Date
RFC4210	*Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)* https://tools.ietf.org/html/rfc4210		September 2005
RFC5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile		May 2008
RFC3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Chokhani, Ford, Sabettt, and Wu.		November 2003
SP 800-63-3	Digital Identity Guidelines	3	02 March 2020
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

CA	Certification Authority
CARL	Certification Authority Revocation List
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
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)

Term	Definition
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.
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 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.

Term	Definition
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]