Certification Practices Statement
for the
United States Patent and Trademark Office

July 14, 2023
Version 4.3

Prepared by:

United States Patent and Trademark Office
Public Key Infrastructure Policy Authority

Approval / Date: Digitally signed by Timothy Goodwin Date: 2023.07.19 12:35:30 -04'00'

Name: Timothy Goodwin

Title: Chief Information Security Officer

This page is intentionally left blank.

TABLE OF CONTENTS

1 INTRODUCTION 1-1
1.1 Overview 1-1
1.1.1 Certification Practices Statement (CPS) 1-1
1.1.2 Relationship between the CP and the CPS 1-2
1.1.3 Relationship between the FBCA and the USPTO CA 1-2
1.1.4 Scope 1-2
1.1.5 Interaction with PKIs External to the Federal Government 1-2
1.2 Document Name and Identification 1-2
1.3 PKI Participants 1-4
1.3.1 PKI Authorities 1-4
1.3.2 USPTO Certification Authority 1-6
1.3.3 Card Management System (CMS) 1-7
1.3.4 Registration Authorities (RA) 1-7
1.3.5 Certificate Status Servers (CSS) 1-7
1.3.6 Key Recovery 1-8
1.3.7 Subscribers 1-8
1.3.8 Affiliated Organizations 1-8
1.3.9 Relying Parties 1-8
1.3.10 Other Participants 1-9
1.4 Certificate Usage 1-9
1.4.1 Appropriate Certificate Uses 1-9
1.5 Policy Administration 1-10
1.5.1 1.5.1 Organization Administering the Document 1-10
1.5.2 Contact Person 1-10
1.5.3 Person Determining CPS Suitability for the Policy 1-10
1.5.4 CPS Approval Procedures 1-10
1.6 Definitions and Acronyms 1-11
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 2-1
2.1 Repositories 2-1

2.2 Publication of Certification Information 2-1
2.2.1 Publication of Certificates and Certificate Status 2-1
2.2.2 Publication of CA Information 2-2
2.3 Time or Frequency of Publication 2-2
2.4 Access Controls on Repositories 2-2
3 IDENTIFICATION AND AUTHENTICATION 3-1
3.1 Naming 3-1
3.1.1 Types of Names 3-1
3.1.2 Need for Names to be Meaningful 3-3
3.1.3 Anonymity or Pseudonymity of Subscribers 3-3
3.1.4 Rules for Interpreting Various Name Forms 3-3
3.1.5 Uniqueness of Names 3-3
3.1.6 Recognition, Authentication, and Role of Trademarks 3-4
3.2 Initial Identity Validation 3-4
3.2.1 Method to Prove Possession of Private Key 3-4
3.2.2 Authentication of Organization Identity 3-4
3.2.3 Authentication of Individual Identity 3-5
3.2.4 Non-verified Subscriber Information 3-7
3.2.5 Validation of Authority 3-7
3.2.6 Criteria for Interoperation 3-7
3.3 Identification and Authentication for Re-Key Requests 3-7
3.3.1 Identification and Authentication for Routine Re-key 3-7
3.3.2 Identification and Authentication for Re-key after Revocation 3-8
3.4 Identification and Authentication for Revocation Request 3-9
3.5 Identification and Authentication for Key Recovery Requests 3-9
3.5.1 Subscriber Requestor Authentication 3-10
3.5.2 Third-Party Requestor Authentication 3-10
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 4-1
4.1 Certificate Application 4-1
4.1.1 Who Can Submit a Certificate Application 4-1
4.1.2 Enrollment Process and Responsibilities 4-1

4.2 Certificate Application Processing 4-2
4.2.1 Performing Identification and Authentication Functions 4-3
4.2.2 Approval or Rejection of Certificate Applications 4-3
4.2.3 Time to Process Certificate Applications 4-3
4.3 Certificate Issuance 4-3
4.3.1 CA Actions during Certificate Issuance 4-3
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 4-5
4.4 Certificate Acceptance 4-5
4.4.1 Conduct Constituting Certificate Acceptance 4-6
4.4.2 Publication of the Certificate by the CA 4-6
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 4-6
4.5 Key Pair and Certificate Usage 4-6
4.5.1 Subscriber Private Key and Certificate Usage 4-6
4.5.2 Relying Party Public Key and Certificate Usage 4-6
4.6 Certificate Renewal 4-7
4.6.1 Circumstance for Certificate Renewal 4-7
4.6.2 Who May Request Renewal 4-7
4.6.3 Processing Certificate Renewal Requests 4-7
4.6.4 Notification of New Certificate Issuance to Subscriber 4-8
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 4-8
4.6.6 Publication of the Renewal Certificate by the CA 4-8
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 4-8
4.7 Certificate Re-key 4-8
4.7.1 Circumstance for Certificate Re-key 4-8
4.7.2 Who May Request Certification of a New Public Key 4-8
4.7.3 Processing Certificate Re-keying Requests 4-9
4.7.4 Notification of New Certificate Issuance to Subscriber 4-9
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 4-9
4.7.6 Publication of the Re-keyed Certificate by the CA 4-9
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 4-9
4.8 Certificate Modification 4-9

4.8.1 Circumstance for Certificate Modification 4-9
4.8.2 Who May Request Certificate Modification 4-9
4.8.3 Processing Certificate Modification Requests 4-10
4.8.4 Notification of New Certificate Issuance to Subscriber 4-10
4.8.5 Conduct Constituting Acceptance of Modified Certificate 4-10
4.8.6 Publication of the Modified Certificate by the CA 4-10
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 4-10
4.9 Certificate Revocation and Suspension 4-10
4.9.1 Circumstances for Revocation 4-10
4.9.2 Who can Request a Revocation 4-11
4.9.3 Procedure for Revocation Request 4-11
4.9.4 Revocation Grace Period 4-12
4.9.5 Time within which CA must Process the Revocation Request 4-12
4.9.6 Revocation Checking Requirements for Relying Parties 4-13
4.9.7 CRL Issuance Frequency 4-13
4.9.8 Maximum Latency for CRLs 4-13
4.9.9 On-line Revocation/Status Checking Availability 4-13
4.9.10 Online Revocation Checking Requirements 4-13
4.9.11 Other Forms of Revocation Advertisement Available 4-13
4.9.12 Special Requirements Related to Key Compromise 4-14
4.9.13 Circumstances for Suspension 4-14
4.9.14 Who Can Request Suspension 4-14
4.9.15 Procedure for Suspension Request 4-14
4.9.16 Limits on Suspension Period 4-14
4.10 Certificate Status Services 4-14
4.10.1 Operational Characteristics 4-14
4.10.2 Service Availability 4-14
4.10.3 Optional Features 4-15
4.11 End of Subscription 4-15
4.12 Key Escrow and Recovery 4-15
4.12.1 Key Escrow and Recovery Policy and Practices 4-15

4.12.2 Session Key Encapsulation and Recovery Policy and Practices 4-16
5 FACILITY, MANAGEMENT, & OPERATIONAL CONTROLS 5-1
5.1 Physical Controls 5-1
5.1.1 Site Location and Construction 5-1
5.1.2 Physical Access 5-1
5.1.3 Power and Air Conditioning 5-3
5.1.4 Water Exposures 5-4
5.1.5 Fire Prevention and Protection 5-4
5.1.6 Media Storage 5-4
5.1.7 Waste Disposal 5-4
5.1.8 Off-site Backup 5-4
5.2 Procedural Controls 5-5
5.2.1 Trusted Roles 5-5
5.2.2 Number of Persons Required per Task 5-9
5.2.3 Identification and Authentication for Each Role 5-9
5.2.4 Separation of Roles 5-9
5.3 Personnel Controls 5-10
5.3.1 Qualifications, Experience, & Clearance Requirements 5-10
5.3.2 Background Check Procedures 5-11
5.3.3 Training Requirements 5-11
5.3.4 Retraining Frequency and Requirements 5-12
5.3.5 Job Rotation Frequency and Sequence 5-12
5.3.6 Sanctions for Unauthorized Actions 5-12
5.3.7 Independent Contractor Requirements 5-12
5.3.8 Documentation Supplied to Personnel 5-12
5.4 Audit Logging Procedures 5-13
5.4.1 Types of Events Recorded 5-13
5.4.2 Frequency of Processing Data 5-16
5.4.3 Retention Period for Security Audit Data 5-17
5.4.4 Protection of Security Audit Data 5-17
5.4.5 Security Audit Data Backup Procedures 5-17

5.4.6 Security Audit Collection System (Internal vs. External) 5-18
5.4.7 Notification to Event-Causing Subject 5-18
5.4.8 Vulnerability Assessments 5-18
5.4.9 PKI Audit Log Examination Process 5-19
5.5 Records Archival 5-19
5.5.1 Types of Events Archived 5-20
5.5.2 Retention Period for Archive 5-21
5.5.3 Protection of Archive 5-21
5.5.4 Archive Backup Procedures 5-22
5.5.5 Requirements for Time-Stamping of Records 5-22
5.5.6 Archive Collection System (Internal vs. External) 5-22
5.5.7 Procedures to Obtain and Verify Archive Information 5-22
5.6 Certification Authority Key Changeover 5-23
5.7 Compromise and Disaster Recovery 5-23
5.7.1 Incident and Compromise Handling Procedures 5-24
5.7.2 Computing Resources, Software, and/or Data are Corrupted 5-25
5.7.3 Certification Authority Signature Keys Are Compromised 5-25
5.7.4 Business Continuity Capabilities after a Disaster 5-26
5.8 CA or RA Termination 5-27
6 TECHNICAL SECURITY CONTROLS 6-1
6.1 Key Pair Generation and Installation 6-1
6.1.1 Key Pair Generation 6-1
6.1.2 Private Key Delivery to Subscriber 6-2
6.1.3 Public Key Delivery to Certificate Issuer 6-3
6.1.4 CA Public Key Delivery to Subscribers/Relying Parties 6-4
6.1.5 Key Sizes and Signature Algorithms 6-4
6.1.6 Public Key Parameter Generation 6-5
6.1.7 Key Usage Purposes (as per X.509 V3 Key Usage Field) 6-5
6.2 Private Key Protection and Cryptographic Module Engineering Controls 6-6
6.2.1 Cryptographic Module Standards and Controls 6-6
6.2.2 Private Key Multi-Person Control 6-6

6.2.3 Private Key Escrow 6-7
6.2.4 Private Key Backup 6-7
6.2.5 Private Key Archival 6-8
6.2.6 Private Key Transfer into or from a Cryptographic Module 6-8
6.2.7 Private Key Storage on Cryptographic Module 6-8
6.2.8 Method of Activating Private Key 6-8
6.2.9 Method of Deactivating Private Key 6-9
6.2.10 Method of Destroying Private Key 6-10
6.2.11 Cryptographic Module Rating 6-10
6.3 Other Aspects of Key Pair Management 6-10
6.3.1 Public Key Archival 6-10
6.3.2 Certificate Operation Periods and Key Usage Periods 6-11
6.4 Activation Data 6-12
6.4.1 Activation Data Generation and Installation 6-12
6.4.2 Activation Data Protection 6-12
6.4.3 Other Aspects of Activation Data 6-13
6.5 Computer Security Controls 6-13
6.5.1 Specific Computer Security Technical Requirements 6-13
6.5.2 Computer Security Rating 6-14
6.6 Life Cycle Technical Controls 6-14
6.6.1 System Development Controls 6-14
6.6.2 Security Management Controls 6-15
6.6.3 Life-Cycle Security Ratings 6-16
6.7 Network Security Controls 6-16
6.8 Time-Stamping 6-17
7 CERTIFICATE, CRL, AND PROFILES 7-1
7.1 Certificate Profile 7-1
7.1.1 Version Numbers 7-1
7.1.2 Certificate Extensions 7-1
7.1.3 Algorithm Object Identifiers 7-1
7.1.4 Name Forms 7-1

7.1.5 Name Constraints 7-2
7.1.6 Certificate Policy Object Identifier 7-2
7.1.7 Usage of Policy Constraints Extension 7-2
7.1.8 Policy Qualifiers Syntax and Semantics 7-2
7.1.9 Processing Semantics for the Critical Certificate Policy Extension 7-2
7.1.10 Inhibit Any Policy Extension 7-2
7.2 CRL Profile 7-2
7.2.1 Version Numbers 7-2
7.2.2 CRL and CRL Entry Extensions 7-2
7.3 OCSP Profile 7-2
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 8-1
8.1 Frequency or Circumstances of Assessment 8-1
8.2 Identity/Qualification of Assessor 8-1
8.3 Assessor's Relationship to Assessed Entity 8-2
8.4 Topics Covered by Compliance Audit 8-2
8.5 Actions Taken as a Result of Deficiency 8-3
8.6 Communication of Results 8-4
9 OTHER BUISNESS AND LEGAL MATTERS 9-1
9.1 Fees 9-1
9.1.1 Certificate Issuance or Renewal Fees 9-1
9.1.2 Certificate Access Fees 9-1
9.1.3 Revocation or Status Information Access Fees 9-1
9.1.4 Fees for other Services 9-1
9.1.5 Refund Policy 9-1
9.2 Financial Responsibility 9-1
9.2.1 Insurance Coverage 9-1
9.2.2 Other Assets 9-1
9.2.3 Insurance or Warranty Coverage for End-Entities 9-1
9.3 Confidentiality of Business Information 9-2
9.3.1 Scope of Confidential Information 9-2
9.3.2 Information not within the Scope of Confidential Information 9-2

9.3.3 Responsibility to Protect Confidential Information 9-2
9.4 Privacy of Personal Information 9-2
9.4.1 Privacy Plan 9-2
9.4.2 Information Treated as Private 9-3
9.4.3 Information not Deemed Private 9-3
9.4.4 Responsibility to Protect Private Information 9-3
9.4.5 Notice and Consent to Use Private Information 9-4
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 9-4
9.4.7 Other Information Disclosure Circumstances 9-4
9.5 Intellectual Property Rights 9-4
9.6 Representations and Warranties 9-4
9.6.1 CA Representations and Warranties 9-4
9.6.2 RA Representations and Warranties 9-5
9.6.3 Subscriber Representations and Warranties 9-5
9.6.4 Relying Party Representations and Warranties 9-6
9.6.5 Representations and Warranties of Other Participants 9-6
9.7 Disclaimers of Warranties 9-7
9.8 Limitations of Liability 9-7
9.9 Indemnities 9-7
9.10 Term and Termination 9-7
9.10.1 Term 9-7
9.10.2 Termination 9-7
9.10.3 Effect of Termination and Survival 9-7
9.11 Individual Notices and Communications with Participants 9-7
9.12 Amendments 9-7
9.12.1 Procedure for Amendment 9-7
9.12.2 Notification Mechanism and Period 9-8
9.12.3 Circumstances under Which OID Must Be Changed 9-8
9.13 Dispute Resolution Provisions 9-8
9.14 Governing Law 9-8
9.15 Compliance with Applicable Law 9-8

9.16 Miscellaneous Provisions 9-8
9.16.1 Entire Agreement 9-8
9.16.2 Assignment 9-8
9.16.3 Severability 9-9
9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights) 9-9
9.16.5 Force Majeure 9-9
9.17 Other Provisions 9-9
10 BIBLIOGRAPHY 10-1
11 ACRONYMS AND ABBREVIATIONS 11-1
12 GLOSSARY 12-1

LIST OF TABLES

Table 1-1: Certificate Policies....1-3
Table 1-2: Products for Core Functions....1-6
Table 3-1: Assurance Level Naming Requirements....3-1
Table 3-2: Re-keying Identity Requirements....3-8
Table 5-1: List of Items Controlled by the Trusted Roles....5-9
Table 6-1: Certificate Authority Key Validity Period....6-11
Table 6-2: Smart Card Validity Periods....6-11
Table 6-3: Device Validity Periods....6-11
Table 6-4: OCSP Validity Periods....6-11
Table 6-5: Signing Validity Periods....6-12
Table 7-1: OIDs Used for Signatures....7-1
Table 7-2: OIDs Identifying the Algorithm for which the Subject Key was generated....7-1

REVISION HISTORY

Version	Date	Editor	Change Description
1.0	8/31/2004	Darryl E. Clemons	N/A. Original version, which was approved by Chief Information Officer.
1.1	10/1/2004	Darryl E. Clemons	In Table 1-1: United States Patent and Trademark Office Public Key Infrastructure Officer Roles and Personnel Assigned, on Pg. 1-5, the following changes were made: • Bea Bolar was added as Security Officer. • Chris Rutherford was removed as Administrator. • Francine Benjamin and Sharlene Smith were added as Registration Authorities. • Lee Sun was added as Auditor. • Fred Whiteside was removed as Security Officer. • Public Key Infrastructure Sponsor and designates were removed from the list of Trusted roles. Pages 2-4, 3-2, 4-1, B-2 and B-5, replaced abbreviations with full spelling Page 5-4, Operational Support Plan reference was added Sections 6.2.4 thru 6.8 were added to recover text lost in document production.
1.1	10/20/2004	Amit Jain	In Table 1-1: United States Patent and Trademark Office Public Key Infrastructure Officer Roles and Personnel Assigned, on Pg. 1-5, the following change was made: • Darryl E. Clemons was removed as a Registration Authority.
1.2	11/26/2004	Amit Jain	Removed the column for assigned personnel and changed format of Table 1-1. Also, edited text in the section that was relevant to that column of the table.

Version	Date	Editor	Change Description
			Section 4.5.2 and 4.5.8 were edited to include additional responsibilities placed on auditor. Section 4.5.5 was modified to better identify our security audit data backup procedures.
1.2	12/10/2004	Amit Jain, Greg McCain and Art Purcell	Changed sections 1.3.1.3, 2.7, 3.2.1, 4.4.5, 4.5.1, 4.5.5, 4.6.5, 5.3.1, and 6.4.1 to incorporate necessary modifications identified by FBCA/CPWG. Removed related authorities table from section 1.3.3 and added reference to the Operational Support Plan. Table in section 5.2.4 was modified. Section 3.1.9.1 was updated Section 4.5.9 was created and text previously in Section 4.5.8 was moved to the new section. Table 1-1 and sections 1.3.1.2, 1.3.1.3, 1.3.3, 1.4.2, 2.7, 3.2.1, 4.5.2, 4.5.5, 4.6.6, 4.5.8, 5.1.2, 5.1.8, 6.4.1, 6.6.1, 6.8 were modified for spelling, punctuation, and grammar or formatting. Section headers in Section 4 were updated to conform to the intended format.
1.2	12/14/2004	Greg McCain	Changed column title from ‘Author’ to ‘Editor’ in the Revision History table.
1.3	03/23/06	Greg McCain	Changed section 1.4.2 to modify the phone number contact information for the Director of the NTSG office. Changed various sections to reflect the physical relocation of the CA equipment.
1.4	01/03/2007	Greg McCain	Changed the sections listed below following the annual audit activities; reasons for each change are noted. Section 5.3.4 – added details for communications of notification of changes. Section 8.2 – added details regarding the internal web site and how and to whom contact would be made for notice of changes.

Version	Date	Editor	Change Description
1.5	09/12/2007	Greg McCain	Updated to reflect USPTO organizational changes related to management or operational responsibilities for: • Security Policy • Security Operations • User Account Creation and Maintenance
1.6	12/31/2009	Greg McCain	Updated to comply with the RFC 3647 format. Also, revised names of organizations to conform to new organization charts.
1.7	03/23/2010	Greg McCain	Updated following recommendations of External Auditor.
1.8	7/9/2012	Amit Jain	Updated to make changes due to HSPD-12 implementation and to keep in compliance with latest policy changes.
1.9	3/23/2016	Amit Jain and Zach Iler	Updated to bring document up to date and make changes based on previous audit.
2.0	11/8/2016	Ben Spainhour	Addition of MediumDevice and MediumDeviceHardware OIDs. Updates to align with the USPTO CP versions 2.7 and 2.7.1.
2.1	2/10/2017	Amit Jain	Addition of Basic Device OID and changes based on this addition.
3.0	11/13/2017	Richard Arnold	Updated to bring document current and make changes based on previous audit
3.1	10/01/2018	Richard Arnold	Updated to bring document current and make changes based on previous audit
3.2	04/01/2019	Richard Arnold and Amit Jain	Updated to bring document current and make changes based on previous audit
3.3	01/27/2020	Richard Arnold	Updated to bring document current and make changes based on previous audit

Version	Date	Editor	Change Description
4.0	04/28/2021	Scott Cobb	Updated to align with v4.0 USPTO CP document.
4.1	05/06/2021	Scott Cobb	Add a contingency to the full system backup (5.1.8)
4.2	06/03/2022	Scott Cobb	Remediate 2021 compliance audit findings
4.3	07/14/2023	Scott Cobb	Remediate 2022 compliance audit findings

1 INTRODUCTION

The United States Patent and Trademark Office (USPTO) established a Public Key Infrastructure Policy (PKI) for the operation of Certification Authorities (CAs). An Internal PKI program was implemented to establish a CA to serve the internal business needs and functions of the USPTO.

This Certification Practices Statement (CPS) describes the primary obligations and operational responsibilities of all USPTO Internal PKI program participants, and defines the creation, management and use of version 3 X.509 public key certificates within this program.

Public key certificates at USPTO are appropriate for use by persons and non-human entities (e.g., routers, firewalls, or software applications) in their interactions with information technology applications requiring communication between networked computer-based systems as well as for the general purposes of providing information integrity and confidentiality. Such applications include:

- User identification and authorization when accessing computing systems and programs
- Email
- Transmission of sensitive but unclassified information
- Digital signing of electronic forms and objects
- Authentication of and communications between infrastructure components such as servers, network communications equipment, and software applications

The term “X.509 certificates,” as used within this CPS, implies X.509 version 3 certificates. Also, note that the term, “Public Key Infrastructure client software” refers to the software that provides PKI functionality within the Internal Certification Authority domain. While this CPS does not require the use of public key certificates in any particular USPTO application or program, if public key certificates are used by the USPTO they must be used in accordance with this Certification Practices Statement and the X.509 Certificate Policy for the USPTO PKI. This CPS is applicable to all entities with relationships to the Internal CA, including administrators, security officers, subscribers, operators, and Relying Parties.

This CPS is consistent with the Internet Engineering Task Force Public Key Infrastructure X.509 RFC 3647, Certificate Policy, and Certification Practices Statement Framework. It also implements requirements of the USPTO Internal CA Certificate Policy.

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

1.1 Overview

1.1.1 Certification Practices Statement (CPS)

This CPS documents the practices and procedures used by USPTO to operate the Internal Certification Authority.

1.1.2 Relationship between the CP and the CPS

This CPS applies to the USPTO Internal Certification Authority which is cross-certified with the Federal Bridge CA.

The USPTO CP states what assurance can be placed on a certificate issued by the Internal CA. This CPS defines and details operational and technical practices that will ensure that the policy asserted in the USPTO CP is correctly implemented and followed in the operation of the Internal CA. In addition, it clearly defines certain special trusted roles of the overall Internal CA and the responsibilities that must be followed by persons assigned to those roles.

1.1.3 Relationship between the FBCA and the USPTO CA

The FBCA cross certification with the USPTO CA consists of mapping the policy OIDs listed in the following table:

FBCA Policy OIDs	USPTO Policy OIDs
id-fpki-certpcy-basicAssurance {2 16 840 1 101 3 2 1 3 2}	id-pto-basic-2003 {2 16 840 1 101 3 2 1 2 7}
id-fpki-certpcy-mediumAssurance {2 16 840 1 101 3 2 1 3 3}	id-pto-medium-2003 {2 16 840 1 101 3 2 1 2 8}
id-fpki-certpcy-mediumHardware {2 16 840 1 101 3 2 1 3 12}	id-pto-mediumHardware {2 16 840 1 101 3 2 1 2 9}
id-fpki-certpcy-mediumDevice {2 16 840 1 101 3 2 1 3 37}	id-pto-mediumDevice {2 16 840 1 101 3 2 1 2 11}
id-fpki-certpcy-mediumDeviceHardware {2 16 840 1 101 3 2 1 3 38}	id-pto-mediumDeviceHardware {2 16 840 1 101 3 2 1 2 12}

1.1.4 Scope

This CPS applies to certificates issued to CAs, devices, code signers, USPTO employees, contractors, and other affiliated personnel. This CPS does not apply to certificates issued to groups of people.

USPTO operates only locally trusted (OLT) CAs that issue certificates to NPE devices for 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

The Internal Certification Authority will issue certificates that meet the policy assurance levels defined in the USPTO CP.

NIST has assigned the Internet Engineering Task Force notation arc of ‘2.16.840.1.101.3.2.1.2’ for USPTO. The International Organization for Standardization notation represents this as:

uspto-policies OBJECT IDENTIFIER: = {joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) csor(3) pki(2) cert-policy(1) pto-policies(2)}

The USPTO CA is cross-certified with the FBCA and can also issue certificates that assert Federal PKI Common Policy OIDs under the 2.16.840.1.101.3.2.1.3 notational arc.

Table 1-1: Certificate Policies

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 self-signed certificate should not contain policy OIDs, but if it does, it should only contain id-pto-basic-2003, id-pto-medium-2003 and id-pto-mediumHardware OIDs.

USPTO issued certificates may contain the following policy OIDs:

Self-Issued CA certificates	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
SSL certificates	id-pto-medium-2003 (prior to 11/4/16)	2.16.840.1.101.3.2.1.2.8
	id-pto-mediumDevice (as of 11/4/16)	2.16.840.1.101.3.2.1.2.11
	id-pto-mediumDeviceHardware (as of 11/4/16)	2.16.840.1.101.3.2.1.2.12
	id-pto-basicDevice (as of 2/28/17)	2.16.840.1.101.3.2.1.2.13
Subscriber PIV Auth	id-pto-mediumHardware	2.16.840.1.101.3.2.1.2.9
	id-fpki-common-authentication	2.16.840.1.101.3.2.1.3.13
Subscriber Card Auth	id-fpki-common-cardAuth	2.16.840.1.101.3.2.1.3.17
Subscriber Digital Signature	id-pto-mediumHardware	2.16.840.1.101.3.2.1.2.9

Subscriber Encryption	id-pto-mediumHardware	2.16.840.1.101.3.2.1.2.9
PIV Content Signer (as of 5/6/2015)	id-fpki-common-piv-contentSigning	2.16.840.1.101.3.2.1.3.39
Legacy PIV Content Signer	id-fpki-common-devices	2.16.840.1.101.3.2.1.3.8

1.3 PKI Participants

1.3.1 PKI Authorities

1.3.1.1 USPTO Chief Information Officer

This CPS is established under the authority of the USPTO Chief Information Officer.

1.3.1.2 USPTO PKI Policy Authority (PA)

The USPTO Policy Authority resides inside the USPTO Cybersecurity division and governs 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 USPTO PA owns PKI policy documents and represents the interests of the USPTO to external Federal PKI entities. They are 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 Certificate Policies
- 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

1.3.1.3 USPTO PKI Policy Management Authority (PMA)

The Policy Management Authority is part of the Policy Authority. These individuals are held accountable by the USPTO Chief Information Security Officer for the overall responsibility of maintaining the USPTO CP and ensuring all USPTO PKI components (e.g., CAs, CMSs, RAs) 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 must be made at least two weeks prior to the implementation; all new artifacts (CA certificates, CRL DP, AIA, and/or SIA URLs, etc.) produced as a result of the change must be provided to the FPKIPA within 24 hours following implementation.

USPTO has an employee who serves as an agency representative to the FPKI Policy Authority. This POC will be responsible for emailing a notification to the FPKIPA contact information provided on the IDManagement.gov website (fpki@gsa.gov).

1.3.1.4 USPTO PKI Operational Authority (OA)

The Operational Authority is the organization within the USPTO that operates the USPTO Internal Certification Authority, posting those certificates issued and CRLs into the repository and ensuring the continued availability of the repository to all users.

1.3.1.5 USPTO PKI Operational Authority Administrator (OAA)

The USPTO PKI Operational Authority Administrator (OAA) is the Technical Lead of PKI Engineering in the Office of the Chief Information Officer (OCIO). This individual has primary responsibility for overseeing the proper operation of the CA including the repository, and who appoints individuals to the roles of Operational Authority Officers.

The OAA may also approve the issuance, installation and use of certificate-based credentials that carry the responsibility and authority of a Registration Authority Officer for use by the Card Management System (CMS).

The OAA has oversight responsibilities for ensuring that PKI-related operations conform to this CPS. In the event where the OAA is unavailable, a member of the OIEO management chain may act on behalf of the OAA.

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 USPTO CA, its repository and the OCSP facility. These personnel will be employees and trusted contractors who work in or for the OCIO:

- Security Officer
- Administrator
- Registration Authority
- Auditor
- IPKI Operator (System Operator)

These officers ensure all aspects of the CA services, operations, and infrastructure related to certificates issued under the USPTO CP are performed in accordance with the requirements, representations, and warranties of the CP and in accordance with the current, approved Certification Practices Statement (this document).

The general duties include the installation, configuration and certain day-to-day operations of the Internal CA. They are responsible for CA-related information maintained in the USPTO PKI repositories:

- Control over the registration process
- Identification and authentication process
- Certificate manufacturing process

- Publication of certificates
- Revocation of certificates
- Publication of Certificate Revocation Lists
- Cryptographic re-keying of USPTO PKI CA signing material
- Key recovery
- Ensuring that all aspects of the USPTO services and USPTO operations and infrastructure related to certificates issued under this CPS are performed in accordance with the requirements, representations, and warranties of this CPS.

The Operational Authority Officers execute the CA functions by using these products:

Table 1-2: Products for Core Functions

Core Function	Product
Certificate Signing Authority	Entrust Security Manager
Hardware protection of the Certification Authority signing key	SafeNet LunaSA
Registration and Administration of smart cards	ActivIdentity Card Management System
Additional Registration and Administration	HID Global (previously ActivIdentity) ActivClient - Entrust Security Manager Administration (SMA) - SafeNet Authentication Client
Online Certificate Status Protocol	HID Global (previously CoreStreet) Validation Authority and Responder
Issuance of Web-Based certificates	Entrust Enrollment Server for Web (ESW)
Smart Cards	Probaris ID

1.3.2 USPTO Certification Authority

The USPTO Internal CA is the entity operated by the Operational Authority that is authorized to create, sign, and issue public key certificates to USPTO personnel, contractor employees, non-human entities, and affiliates. The Operational Authority is responsible for all operational aspects of the issuance and management of certificates including:

- Certificate manufacturing process
- Publication of certificates
- Revocation of certificates
- Publication of Certificate Revocation Lists

- Re-key of USPTO PKI CA signing material
- Ensures all aspects of the CA services, operations, and infrastructure related to certificates issued under the USPTO CP are performed in accordance with the requirements, representations, and warranties of the CP.

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

1.3.2.1 Entity Cross-Certified Certification Authority (CA)

USPTO designates the Internal CA to receive a cross-certificate from the FBCA.

At the time of CPS publication, there are no subordinate CAs to the USPTO cross-certified CA.

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

1.3.3 Card Management System (CMS)

The Card Management System is responsible for managing smart card token content and its requirements are associated with the PIV policies only; the PA is responsible to ensure it meets the requirements described in this document.

1.3.4 Registration Authorities (RA)

The Registration Authority is the group of individuals that are in the Security Division of USPTO that issues all human subscriber smart cards. The Registration Authority is divided into four separate roles:

- Sponsor
- Enrollment Official
- Adjudicator
- Card Issuer

This RA group is the primary registration agent for the Certification Authority for PKI-sponsored human subscriber certificates and will receive all authorization and verification information for such requests.

1.3.5 Certificate Status Servers (CSS)

USPTO has an authority that provides status information about certificates on behalf of the CA through online transactions. In particular, USPTO has an Online Certificate Status Protocol (OCSP) responder to provide online status information. This authority is also known as a Certificate Status Server (CSS), where the CSS is identified in certificates as an authoritative source for revocation information. This OCSP server information is 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

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. The Security Officer Trusted Role is authorized to recover an escrowed key, which requires two-person controls (section 4.12.1.2).

1.3.7 Subscribers

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

A subscriber is the individual whose name appears as the subject in a certificate. Subscribers to the USPTO Internal PKI include USPTO personnel, USPTO contractor employees, and agency affiliates.

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 subscriber's name to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A Relying Party may use information in the certificate (such as CP identifiers or policy mapping extensions) to determine the suitability of the certificate for a particular use.

USPTO Relying Parties

USPTO Relying Parties, including applications, infrastructure components, and human subscribers, will use specific policy relating to the implementation and use of digital signatures and other PKI-based security services to determine appropriate reliance on certificates issued under this CPS.

Certificates issued to internal subscribers, including USPTO employees and support personnel, are intended to be relied upon by the USPTO and USPTO external customers, including applicants and other intellectual property offices doing business with the USPTO.

As of the release of this CPS, no external Relying Parties are identified.

Non-USPTO Relying Parties

Non-USPTO Relying Parties should make the decision whether to rely on a certificate issued under this CPS by considering all the facts and circumstances of the transaction including:

- Value of the information
- Threat environment
- Existing protection of the information environment
- Functionality of the Relying Party's application in validating the certificate
- Integrity of the authenticated or secured payload or transaction

The USPTO does not control this determination. Nonetheless, the USPTO CP contains some helpful guidance which Relying Parties may consider in making their decisions.

1.3.10 Other Participants

CAs and RAs operating under the USPTO policy will periodically require an outside auditing service. The USPTO CISO will oversee and approve the engagement of this service.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

This CPS is applicable to all certificates issued by the USPTO Internal Certification Authority which operates at the levels of assurance listed in Section 1.2 (Basic, Basic Device, Medium, Medium Hardware, Medium Device, Medium Device Hardware, and Card Authentication). The practices described in this CPS apply to the issuance and use of certificates and Certificate Revocation Lists for the certificate signing authority, personnel, trusted contractors, applications and equipment within the Internal CA domain. This CPS is also applicable for the issuance and use of Internal CA cross-certificates.

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

For USPTO personnel, PKI certificates and associated private keys may be used to replace the login and password-based authentication for network and system access, and paper-based authentication of documents by "wet signatures" in a variety of USPTO processes, such as employee authentication of time sheets, and may be used to authenticate employees for management of their administrative benefits. PKI certificates and associated private keys may be used to authenticate access to sensitive patent and trademark information, which is the intellectual property of the United States. This information may include electronic examination records of other intellectual property offices and organizations, which may be of great sensitivity. PKI-based authentication may also be used in conjunction with access control technologies to control access to pre-decisional materials related to the examination process and other USPTO documents.

The USPTO PKI is intended to support applications involving sensitive but unclassified information, which can include sensitive but unclassified data protected by provisions of the Patent Act, the Trademark Act, and the Patent Cooperation Treaty, as well as other information protected pursuant to federal statutes and regulations such as the Privacy Act.

1.4.2 Prohibited Certificate Uses

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

1.5 Policy Administration

As the Approval Authority for the USPTO PKI, the Chief Information Security Officer has the overall responsibility for ensuring conformity of PKI implementations and operations to the applicable policies. The USPTO CISO is also responsible for approving exceptions and granting waivers to the USPTO CP and any specific Certification Practices Statement, including this CPS. The USPTO CISO has appointed members of the Cybersecurity Division to be the Policy Authority and to assist and provide guidance in assuring conformance to this CPS.

1.5.1 1.5.1 Organization Administering the Document

The USPTO Policy Authority is responsible for the definition, revision and promulgation of this Certificates Practice Statement.

1.5.2 Contact Person

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

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

1.5.3 Person Determining CPS Suitability for the Policy

The USPTO Director of the Cybersecurity Division will review external auditor CP-CPS mappings to determine the suitability of this CPS for the Internal Certification Authority. If the CPS is found suitable, the Director will recommend approval to USPTO's CISO. See section 8 for further details.

1.5.4 CPS Approval Procedures

CAs issuing under this CPS are required to meet all facets of the USPTO PKI CP.

The USPTO PKI Policy Authority must make the determination that this CPS complies with the USPTO Certificate Policy for a given level of assurance. The CA must meet all requirements of

an approved CPS before commencing operations. In some cases, the USPTO PA may require the additional approval of an authorized agency. The USPTO PA will make this determination based on the nature of the system function, the type of communications, or the operating environment.

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

The USPTO PA must also notify any cross-certified entities that are expected to review and disseminate comments on the changes to the CPS.

1.6 Definitions and Acronyms

See Sections 11 and 12.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

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

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

2.2 Publication of Certification Information

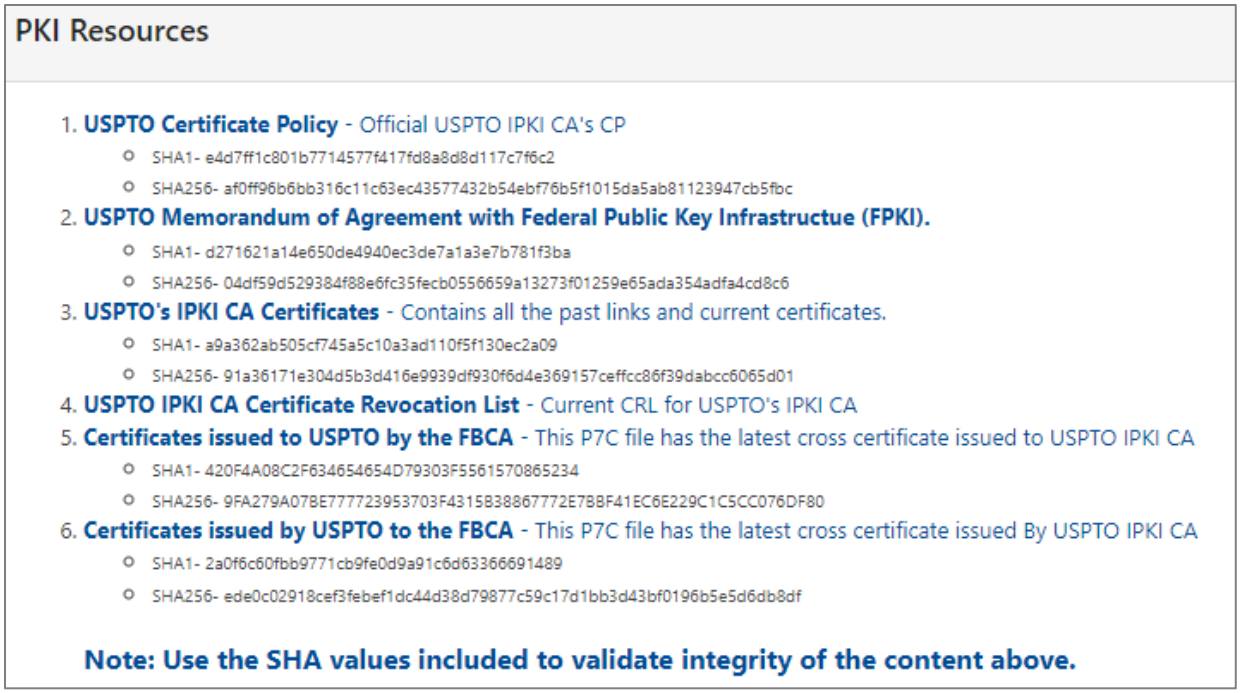
2.2.1 Publication of Certificates and Certificate Status

CA certificates and CRLs are published to an internal, online repository that is available to internal Subscribers and internal Relying Parties, it contains:

- Encryption certificates that assert one or more of the policy OIDs listed in this CPS
- Current CRLs
- Cross-certificates where appropriate
- CA's certificate for all certificate signing keys, including link certificates

CRL publishing activity is automatically monitored; if issues are detected, the Operational Authority is notified so they may take immediate action to resolve.

USPTO also operates a publicly accessible repository (http://ipki.uspto.gov). These entries are updated from the USPTO Enterprise Directory Service on a continuous basis using scripts that run at least once every 15 minutes.


PKI Resources

1. **USPTO Certificate Policy** - Official USPTO IPKI CA's CP
   - SHA1- e4d7ff1c801b7714577f417fd8a8d8d117c7f6c2
   - SHA256- af0ff96b6bb316c11c63ec43577432b54ebf76b5f1015da5ab81123947cb5fbc
2. **USPTO Memorandum of Agreement with Federal Public Key Infrastructue (FPKI).**
   - SHA1- d271621a14e650de4940ec3de7a1a3e7b781f3ba
   - SHA256- 04df59d529384f88e6fc35fecb0556659a13273f01259e65ada354adfa4cd8c6
3. **USPTO's IPKI CA Certificates** - Contains all the past links and current certificates.
   - SHA1- a9a362ab505cf745a5c10a3ad110f5f130ec2a09
   - SHA256- 91a36171e304d5b3d416e9939df930f6d4e369157ceffcc86f39dabcc6065d01
4. **USPTO IPKI CA Certificate Revocation List** - Current CRL for USPTO's IPKI CA
5. **Certificates issued to USPTO by the FBCA** - This P7C file has the latest cross certificate issued to USPTO IPKI CA
   - SHA1- 420F4A08C2F634654654D79303F5561570865234
   - SHA256- 9FA279A078E777723953703F4315838867772E7B8F41EC6E229C1C5CC076DF80
6. **Certificates issued by USPTO to the FBCA** - This P7C file has the latest cross certificate issued By USPTO IPKI CA
   - SHA1- 2a0f6c60fbb9771cb9fe0d9a91c6d63366691489
   - SHA256- ede0c02918cef3febef1dc44d38d79877c59c17d1bb3d43bf0196b5e5d6db8df

Note: Use the SHA values included to validate integrity of the content above.

USPTO also has OCSP responders for all internal and external online certificate status information.

2.2.2 Publication of CA Information

The USPTO CP document is publicly available from the website repository http://ipki.uspto.gov.

The USPTO CPS document will not be published, but can be provided on a need-to-know basis.

Certificates are published when they are issued to the Enterprise Directory Service repository.

2.3 Time or Frequency of Publication

This CPS document is reviewed, updated, and provided to the USPTO Policy Authority for approval on an annual basis, or as needed. It is distributed internally to USPTO employees and contractors on a need to know basis.

2.4 Access Controls on Repositories

USPTO CAs must protect any repository information not intended for public dissemination or modification. CA certificates, CRLs, and pre-generated OCSP responses in the repository must be publicly available.

The Enterprise Directory Service provides the following information to all users, whether authenticated to the UPSTO domain network or via anonymous access on USPTO's internal networks:

- CRLs
- Cross-certificates.
- CA certificates for all issued certificate signing keys.

The Enterprise Directory Service additionally provides copies of all issued public encryption certificates to users who have a non-disabled domain account and have completed a successful logon and authentication to the USPTO network domain.

Access for modification or for reading of non-public information in both the internal and public repositories is protected by Access Control Lists or other Access Control constraints that are part of the underlying repository implementation software.

The USPTO General Counsel under applicable federal laws and USPTO departmental regulations must determine allowance for any additional access to other information in the CA repositories. This CPS must define what information in the repository must be exempt from automatic availability to USPTO staff or external parties and to whom, and under what conditions, the restricted information may be made available.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

Certificates issued to Certification Authorities will use the X.500 Distinguished Name (DN) form. The common names of certificates issued to devices will uniquely identify the device and take the form of a Host Uniform Resource Locator, Internet Protocol Address, or Host Name.

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

Table 3-1: 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 optional Subject Name

Subscriber Certificate DNs

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).

All DNs assigned to USPTO personnel, contractor employees and devices must be in the *dc=uspto,dc=gov* subtree.

Below are the Distinguished Name forms used in certificates issued by the USPTO Internal CA.

Note: "*affiliate*" refers to an organizational attribute, such as department name or company.

Federal employee subscribers: *cn=lastname, firstname,cn=users,dc= uspto,dc=gov* *cn=lastname, firstname (affiliate),cn=users,dc= uspto,dc=gov*
Federal contractor subscribers and affiliate subscribers: *cn=lastname, firstname (affiliate),cn=users,dc= uspto,dc=gov*

Trusted Role holders:

cn=firstname lastname_[distinguishing initials role],ou=alternate,ou=users,ou=uspto, dc=uspto,dc=gov

cn= lastname, firstname_[distinguishing initials role],ou=alternate,ou=users,ou=uspto, dc=uspto,dc=gov

As of the release of this CPS, the DN name forms listed above will be used in certificates issued to the following Trusted Role holders:

- SO – Security Officer
- AUD – Auditor

Elevated Privilege Users:

cn= lastname_[distinguishing initials], firstname,ou=alternate,ou=users,ou=uspto, dc=uspto,dc=gov

cn= lastname-[distinguishing initials], firstname,ou=alternate,ou=users,ou=uspto, dc=uspto,dc=gov

As of the release of this CPS, the DN name forms listed above will be used in certificates issued to the following Elevated Privilege Users:

- Admin – Administrator
- DA – Domain Administrator
- SA – Service Account

Device Certificate DNs

All certificates issued to devices will be issued using the following naming rules. DNs assigned to devices will take a form appropriate to the particular purpose. This name form also applies to PIV content signing certificates.

- *cn=[device name],ou=[distinguishing group level1],ou=[distinguishing group level2], dc=uspto,dc=gov*
  where [distinguishing group level] is optional
- *cn=[device name],ou=[Domain Controllers],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

For human subscribers, the name assigned to the common name attribute is typically the subscriber's name, so that it will be easy to understand.

The common names used in certificates issued to devices will uniquely identify the device and may take the form of a Host Uniform Resource Locator, Internet Protocol Address, or Host Name.

When issuing common names in Certification Authority certificates, the common name should describe the issuer. While the issuer name in CA certificates is not generally interpreted by Relying Parties, this CPS requires the use of meaningful names by Internal CA. If the common name is used in the certificates issued by this Certification Authority, it should describe the issuer. The subject name in CA certificates must match the issuer name in certificates issued by the subject, as required by RFC 5280.

3.1.3 Anonymity or Pseudonymity of Subscribers

The USPTO CA does not issue anonymous or pseudonymous certificates.

CA certificates issued by the USPTO CA do not contain anonymous or pseudonymous identities.

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 Policy Authority.

3.1.5 Uniqueness of Names

Name uniqueness across the USPTO must be enforced. Wherever practical, a X.500 Distinguished Names allocated from the USPTO naming authority must be used. When other name forms are used, they too must be allocated in a manner which ensures name uniqueness across the USPTO. This CPS describes the allocation of names within the USPTO community. The Accounts Services Branch must ensure that duplicate names are not populated within the USPTO EDS Active Directory.

The Accounts Services Branch is the naming authority for USPTO and will ensure that all names are unique. The USPTO Office of Corporate Planning is the authoritative source of the official organizational names for the USPTO.

A single directory information tree will be assigned to the USPTO Internal PKI Certification Authority. If multiple Certification Authorities share a single directory information tree, the Policy Authority must review and approve procedures for name space control. See Sections 3.1.1 and 3.1.5.1 for details of Naming Forms and naming collision resolution details, respectively.

3.1.5.1 Name Claim Dispute Resolution Procedure

Naming collisions will be brought to the attention of the Policy Authority for resolution. The USPTO Operational Authority will revoke and re-issue all affected certificates as directed by the Policy Authority.

All name forms are added to Enterprise Directory Service prior to Subscriber certificates being created. If an organizational naming collision happens in Enterprise Directory Service, the Office of Corporate Planning will resolve it. This process should happen prior to the Operational Authority receiving them. If the Operational Authority encounters a collision, they must bring the collision to the attention of the Policy Authority for resolution.

Distinguished Names are not archived in the CA; they are set to a deactivated state. If a person who previously held a USPTO PIV card returns to USPTO, Accounts Management and the RA will verify their identity as described in 3.2.3. The Change Request to reinstate the person will generate a task for the Operational Authority (OA) to re-enable the account. A Security Officer will confirm the person returning to USPTO service has been authenticated as the previous PIV card holder and then re-activates the DN in the CA. If the SO detects an attempt to assign an existing DN to a new/different person, PIV processing will stop and this will be communicated to Accounts Management so a new, unique DN can be created.

If the RA attempts to assign an existing DN to a PIV card applicant without first notifying the OA, the PIV/CMS software will fail to issue a PIV. This safeguards against assigning an existing DN to a new and different person.

For Individual names, the OAA will direct revocation of certificates with naming conflicts.

3.1.6 Recognition, Authentication, and Role of Trademarks

Questions arising under this CPS regarding recognition, authentication and role of trademarks must be referred to the USPTO General Counsel.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The Internal Certification Authority supports RFC 4210 Internet X.509 Public Key Infrastructure Certificate Management Protocols.

Certificate request and issuance actions are performed using only the FIPS approved software products listed in Table 1-2. These programs use the PKIX-CMP protocol to prove possession of the Private Key prior to transfer of certificates.

3.2.2 Authentication of Organization Identity

The FPKIMA issues cross-certificates to Entity CAs as authorized by the FPKIPA in a Letter Of Agreement. The FPKIPA authenticates the organization identity as part of the application and MOA processes. Section 3.3.1 describes details for authentication of the USPTO cross-certified CA.

Other than issuing certificates to the Federal Bridge for the purposes of cross-certification, USPTO does not issue any other organizational certificates.

3.2.3 Authentication of Individual Identity

The CA must authenticate the identity of the individual requester prior to issuing certificates.

Existing Subscribers may be electronically authenticated by using their currently valid signature certificate or authentication certificate along with the private key, all of which resides on their current PIV card. This is commonly used during PIV card reissuance, when the Subscriber's PIV is nearing expiration.

The RA must ensure that the Subscriber is an active USPTO employee or contractor. The Subscriber's identify will be verified against the records which were collected and stored in the Probaris ID system during their initial enrollment.

The RA must follow the follow the restrictions set forth in section 3.2.3 of the USPTO CP.

3.2.3.1 Authentication of Human Subscribers

For all USPTO personnel, contractor employees or affiliates who will perform work at the USPTO and are allowed access to USPTO information systems, the USPTO Office of Administrative Services Security Division issues an official USPTO Personal Identify Verification (PIV) badge. These PIV badges will include a photographic image of the person and provide smart card identification credentials.

The USPTO will adopt procedures consistent with the NIST SP 800-79 to serve as the basis for documents required to establish sufficient identity to gain a USPTO identity badge. Issuance of PIV cards will be performed in accordance with FIPS 201.

The RA must verify the Applicant's identity information.

The Sponsor is a USPTO employee who holds a PIV card; they substantiate the need, and make the request for issuing a PIV card to the Applicant. Sponsors will verify the Applicant is either a USPTO employee or a contractor employee who will work on a USPTO contract.

A USPTO Enrollment Official will ensure all PIV Applicants have been sponsored in the Probaris ID system. The Enrollment Official will conduct the identity proofing of the Applicant and collect biometric information, a facial image, and fingerprints. The Enrollment Official reviews the PIV request and asks the applicant to provide two source identity documents; one must be a valid picture ID issued by a state or the Federal Government, to ensure that the information is the same as the PIV request. The Enrollment Official verifies the picture on the identity document is that of the Applicant. The identity source documents are scanned into the PIV Card ID system.

Individuals who receive PIV cards must undergo background checks and fingerprinting, completing one of the e-QIP Standard Form 85 questionnaires; SF-85P or SF-86.

For additional Authentication details, refer to the USPTO HSPD-12 PIV Card Issuers Operations Plan.

CAs and/or RAs must record the information set forth below for issuance of each certificate:

- The identity of the person performing the identification, and one of the following:
  - The ID Card Management System (IDMS) uses the Enrollment Official's credential to automatically create an auditable record linking the authentication of the Enrollment Official to a Sponsored applicant's identification verification. The Enrollment Official uses their credential to access the IDMS and verify the applicant's sponsorship. They complete the Enrollment by scanning documents required and approved by the current NIST controlling publication for identification verification, capture required biometric information, and use their credential to digitally sign the Enrollment completing the auditable Enrollment record.

    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)
  Note: As of the release of this CPS, USPTO does not conduct supervised remote identity proofing.
- 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 or digital signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

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

At the time of publication, USPTO does not issue derived credentials from the Internal CA.

3.2.3.2 Authentication of Human Subscribers for Role-based Certificates

Not applicable, USPTO does not issue role-based certificates.

3.2.3.3 Authentication of Human Subscribers for Group Certificates

A certificate must only be issued to a single subscriber. Group certificates or organizational certificates must not be issued under this CPS.

[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.

3.2.3.4 Authentication of Devices

NPE devices (e.g., routers, firewalls, switches, web servers, application software) may be named as certificate subjects. For medium assurance policies, the device must have a PKI Sponsor who will be verified via Active Directory. The PKI Sponsor must already be a subscriber and have been issued a certificate suitable for identity verification by this CA. The PKI Sponsor must be able to digitally sign using certificates which are equivalent to or greater than the certificate assurance level that is being requested for the device.

The PKI Sponsor will be responsible for getting a DNS name assigned to a new device and then getting it onto the network. A Change Request will be created containing the necessary details to engage the Security Officer who will create the Active Directory object. ***Note***: some Microsoft devices are automatically added to Active Directory.

Prior to certificate issuance, the authentication requirements must be captured in the USPTO Internal PKI Certificate Action Form (CAF). The CAF must include the following:

- PKI Sponsor name and digital signature including time/date
- Person performing the identify verification of the PKI Sponsor and digital signature including time/date of verification

When a certificate action requires approval of the PKI Sponsor, the Security Officer will engage the responsible individual via email. If a personnel change has occurred, the previous Sponsor will identify the new person who has acquired PKI Sponsorship responsibility for the device. All PKI Sponsors are obligated to carry out their responsibilities as described in section 9.6.3.

3.2.4 Non-verified Subscriber Information

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

3.2.5 Validation of Authority

Certificates that assert organizational authority must not be issued under this CPS. Code signing certificates fall under this requirement. ***Note***: As of the release of this CPS, USPTO does not issue code signing certificates.

3.2.6 Criteria for Interoperation

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

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-key

In the event that a routine re-key of the USPTO cross-certified CA is required, a new cross certificate will be requested from the FBCA. Before issuance, the USPTO cross-certified CA must identify itself through use of its current signature key or the initial registration process. If it

has been more than three years since a cross-certified CA was identified as required in Section 3.2, identity must be re-established through the initial registration process.

For PIV subscriber re-key, identity should be established through the use of a current signature key as described in 3.2.3.

Biometric data records are only valid for a maximum of 12 years, after which, identity must be re-established and biometrics re-collected through an in-person registration.

In the event a PIV Subscriber's signature key cannot be used, identity may be verified through the use of biometrics on file through the chain of trust defined in [FIPS 201].

Table 3-2: Re-keying Identity Requirements

Assurance Level	Routine Re-key Identity Requirements
Basic (all policies)	Identity may be established through use of current signature key, except that identity must be reestablished through the initial identity validation process at least once every 15 years from the time of initial registration. Must prove possession of corresponding private key Signature re-key every five years Private re-key every five years
Medium (all policies)	Identity may be established through use of current signature key, except that identity must be reestablished through the initial identity validation process at least once every 12 years from the time of initial registration. Must prove possession of corresponding private key. Signature re-key every three years Private re-key every three years For certificates asserting policies mapped to mediumDevice and mediumDeviceHardware certificates, identity may be established through the use of the device's current signature key or the signature key of the device's human sponsor

3.3.2 Identification and Authentication for Re-key after Revocation

After a certificate has been revoked other than during a renewal or update action, the subscriber is required to go through the initial registration process per Section 3.2, unless identity can be verified through the use of biometrics on file through the chain of trust defined in [FIPS 201].

3.4 Identification and Authentication for Revocation Request

Revocation requests for human subscribers must be completed in accordance with FIPS 201.

For active devices which are in production, certificate revocation Change Request must be approved by the Operational Authority Administrator. The SO will verify the OAA approval. The Sponsor must also digitally sign a Certificate Action Form to request revocation

Note: In the event where the OAA is unavailable, a member of the OIEO management chain may act on behalf of the OAA

For devices which have been decommissioned, revocation requests do not require OAA approval.

Type of Certificate	Who can submit a Revocation Request
CA Certificate	The USPTO Policy Authority can request revocation of a cross-certification certificate.
Human Subscriber Certificate	• Individual Subscribers may request revocation of their own certificates. • An individual in the Subscriber's USPTO supervisory chain may request revocation if the Subscriber has been terminated and is unavailable. • Authorized individuals in the OCIO Cybersecurity division may request revocation if the Subscriber is suspected of violating the Subscriber Agreement. • Accounts Management may request revocation as part of normal out-processing.
Device Certificate	The device Sponsor may request certificate revocation by filling out a CAF form and use their PIV credentials to digitally sign.

3.5 Identification and Authentication for Key Recovery Requests

The Operational Authority must verify the identity and authorization of the Requestor prior to initiating the key recovery request. The process begins with all requestors filling out a Private Key Recovery form.

A Requestor is the person that requests the recovery of a Subscriber's private decryption key. A Requestor may be the Subscriber or a third-party (e.g., supervisor or law enforcement officer) authorized to request recovery of a Subscriber's escrowed key on behalf of the Subscriber or on behalf of the organization. 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 to acquire a new active USPTO PIV card.

3.5.2 Third-Party Requestor Authentication

A Third-Party Requestor is someone other than the Subscriber, and categorized as Internal or External as described below. 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:

3.5.2.1 Internal Third-Party Requestor

An Internal Third-Party Requestor is any Requestor who is in the Subscriber's USPTO supervisory chain or otherwise authorized to obtain the Subscriber's key for the USPTO.

An individual in the supervisory chain will hold a USPTO PIV card which will serve as the identification and authentication.

Authorization will be determined by evidence provided in the Private Key Recovery form.

3.5.2.2 External Third-Party Requestor

An External Third-Party Requestor is someone (e.g., law enforcement officer) outside the USPTO agency with a legal instrument, such as a court order, to obtain the private decryption key of the Subscriber.

These individuals will be authenticated according to the evidence provided on the Private Key Recovery form. Authorization will also be established based on evidence provided on the Private Key Recovery form.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

All device certificate requests are entered into the Service Management Platform (SMP) system.

The certificate application process must provide sufficient information to:

- Establish the applicant's authorization (by the employing or sponsoring entity) to obtain a certificate (per section 3.2.3). All applicants who have been authenticated for USPTO employment or contractors who have been sponsored are authorized to be issued certificates; also referred to as authorized persons.
- 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

4.1.1 Who Can Submit a Certificate Application

Type of Certificate	Who can submit an application
CA Certificate and OCSP Responder Certificates	An authorized representative of the applicant CA must submit applications for CA certificates. Any request for a subordinate CA certificate must be reviewed by the USPTO Policy Authority who must recommend approval or disapproval of the issuance. If a subordinate CA certificate is issued, all other cross-certified parties must be notified.
Human Subscriber Certificate	An authorized agency official or the Applicant. The RA must follow the USPTO procedures, as per FIPS 201, for all Subscriber certificate applications.
Device Certificate	The PKI Sponsor of the device

4.1.2 Enrollment Process and Responsibilities

Subscriber Enrollment

The PIV/CMS system is used to enroll, personalize, issue and manage smart card identity credentials under HSPD-12 and FIPS 201 guidelines. This end-to-end system manages personal identity credentials used for physical and logical access control systems. Subscribers are responsible for providing accurate information on their certificate applications. Out-of-band communications must protect the confidentiality and integrity of the data.

USPTO contracted with Probaris to establish a PIV/CMS FIPS 201 compliant system composed of COTS components that are integrated into the USPTO infrastructure:

Enrollment encompasses the in-person identity proofing activities required for medium assurance credentials. During enrollment, two key identity and vetting processes are performed:

1. Establishing the applicant's identity
2. Capturing and validating the applicant's identity data

During the identity proofing process, the Applicant is required to appear in person and must provide two forms of identity source documents. These primary and secondary identity documents are identified in FIPS 201 and are also listed on the USTPO Security Services Center website: https://ptoweb.uspto.gov/ptointranet/ptosecurity/hspd/hspd_fips_id.htm

The Enrollment Official reviews the PIV request and compares the information provided on the identity documents to ensure the information is the same. The Enrollment Official validates them as being authentic, and verifies the picture on the identity document is that of the Applicant.

For additional details, refer to the USPTO HSPD-12 Enrollment and Identity Proofing SOP.

The applicant's photograph and fingerprints are captured during enrollment and placed on the credentials for electronic identity validation when the credentials are presented for access to secure areas.

NPE/Device Enrollment

The Security Officer is responsible for manually entering devices into Active Directory. Some other devices have software which enables automatic enrollment so that the certificate is bound to the device it is issued to using FIPS-140-2 level 2 or higher requirements. The certificate private key is generated on the device and a thin client handles the communication with the Certification Authority. Device enrollment is an integral part of certificate issuance process, see section 4.3.1 for device enrollment details.

4.2 Certificate Application Processing

Information gathered in the certificate application processes must be verified as accurate and complete before certificates are issued. PKI Authorities must follow the procedures detailed in section 4.1.2.

Human Applicants

Each PIV applicant must complete a Personnel Background Investigation with the Office of Personnel Management (OPM). Applicants will make this request via the Defense Counterintelligence and Security Agency (DCSA) e-QIP web-based automated system. The RA verifies HSPD-12 requirements have been met through checks with OPM and/or DoD indices with investigative results provided to the Sponsor. The RA follows the adjudication process by reviewing the SF85, SF85P, SF86 forms for correctness. These background investigation results are uploaded into Probaris ID to form a record.

For additional details, refer to the USPTO HSPD-12 PIV Card Issuers Operations Plan.

NPE/Device Certificates

The Service Management Platform (SMP) is used to process Change Requests (CHG) for device certificate applications. To register in SMP, applicants must submit a request to the SMP system administrators who will perform verification checks prior granting SMP CHG privileges.

The system of record for obtaining a PIV card and becoming a subscriber serves as the verification of identification and authentication.

All communications among PKI Authorities supporting the certificate application and issuance process must be authenticated and protected from modification; any electronic transmission of shared secrets must be protected. Communications may be electronic or out-of-band.

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of the Subscriber must meet the requirements specified in sections 3.2 and 3.3 of this CPS.

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 device certificate applications is at the discretion of the USPTO Operational Authority Officers or their designees. For rejected applications, an email notification will be sent to the applicant describing the reasons why and recommended actions to take.

4.2.3 Time to Process Certificate Applications

Certificate applications must be processed and a certificate issued within 90 days of identity verification as per the procedures established by the USPTO Security Division.

The Enrollment Official is responsible for verifying identity proofing of the PIV card Applicant and ensuring the successful completion of the background checks. Once successfully confirmed, the PIV card issuance step occurs during this same in-person session, essentially in real-time.

NPE device certificate requests are processed using the SMP system which requires all users to register. By using SMP to create a CHG request; this immediately confirms identity verification. The Entrust SMA Administration Policy sets the Activation code lifetime to less than 90 days, after which time, the certificate can no longer issued without restarting a new request.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Certificate Issuance Process for General Subscribers

The USPTO Security Division must follow USPTO procedures, in accordance with FIPS 201, when issuing certificates to general subscriber smart cards.

Steps for issuing certificates to General Subscribers:

- Subscriber submits a certificate application or has one submitted on their behalf.

- Subscriber's identity and authority for a General Subscriber smart card is verified.
- The Security Service Center (SSC) provides on-site badging services and manages the sponsorship, enrollment, and issuance of General Subscriber certificates via a USPTO PIV card through the PIV/CMS software.

Certificate Issuance Process for Administrator Cards

USPTO provides Administrator Cards to individuals who serve in an IT administrator capacity and require elevated permissions. These cards are used for logical access to USPTO AIS systems, but are not recognized by the physical access systems.

Steps for issuing certificates to persons with elevated IT administrator privileges:

- Applicants must have an active USPTO PIV card. Their exiting PIV card enrollment data in Probaris ID is used to issue the Admin Cards; a new enrollment is not required nor supported.
- Applicants must be sponsored by a USPTO employee who is authorized to grant credentials to USPTO employees and contractors.
- Admin Cards will be encoded with only one certificate; an Authentication certificate which is tied to a unique, distinct Admin UPN (User Principal Name).
- Admin Card expiration date cannot exceed one year and it cannot exceed the lifespan of the user's PIV card.
- Admin Card stock may be printed with the user's name but will not have an expiration date printed. This will allow reissuance of the same physical card.
- Admin Card owners cannot use the Self-Service Portal (SSP); service must be done in person at the SSC.

Certificate Issuance Process for Trusted Role Subscribers

Once the new Trusted Role applicant has been appointed by the OAA to hold a Security Officer or Auditor role, follow these steps to allow access to the CA via the Entrust SMA.

1. A Domain account (e.g. "%First initial LastName%SO") is created in the USPTO Active Directory for the new SO/AUD.
2. A current SO role holder stages the profile for the new SO/AUD in SMA.
3. Reference Code & Authcodes are given to the new SO/AUD in a secure manner (encrypted email).
4. The new SO/AUD is given a new SafeNet iKey token (ATM 5510 FIPS approved model) which is then initialized by using the SAC client with a shared secret the new SO/AUD creates.
5. The new SO/AUD uses SMA to pick up their SO profile using the Reference Code & Authcodes in the SMA on the iKey 5110 token.

The SMA is configured to use a PKCS11 driver to communicate with the SafeNet iKey 5110 tokens.

Certificate Issuance Process for Medium Device Policies

Steps for issuing certificates to devices that assert Medium policies (excluding PIV cards):

- The PKI Sponsor authorizes a Change Request to create a certificate; it must contain the necessary information as detailed by the Certificate Request Procedure.
- The Security Officer will create an Active Directory object for an internal certificate.
- The SO initiates an Entrust Security Manager Administration (SMA) session using their specially issued SO token and follows standard Entrust procedures to find the device entry in the USPTO EDS Active Directory, and generates activation codes. The reference numbers are sent to the applicant.
- The applicant uses these reference numbers to generate a Certificate Signing Request (CSR) containing the public key which is then sent to the SO.
- SO opens Entrust ESW and uses the CSR to create and stage the certificate.
- SO creates a Certificate Action Form and sends it to the applicant for completion and digital signature using the Sponsor's USPTO PIV card signing certificate.
- Once the SO receives the completed and signed CAF, the certificate is delivered.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The CAs must inform the subscriber (or other certificate subject) of the creation of a certificate and make the certificate available to the subscriber.

The Enrollment Official conducts an in-person identity proofing of the PIV card Applicant and ensures the background checks have been successfully completed. The Applicant then goes before a Card Issuer to complete the PIV card activation steps which occur during this same in-person session, essentially in real-time. When the Applicant electronically signs for the PIV card, and receives information about its usage, this serves as notification of issuance of certificate.

For NPE device certificates, the PKI Sponsor is included in email correspondence pertaining to certificate issuance.

OCSP responder certificates are managed within the Operational Authority PKI team; there is no need for additional notifications.

4.4 Certificate Acceptance

Before using their private key, a PKI Authority must explain to the subscriber his or her responsibilities as defined in the procedures established by the USPTO Security Division, in accordance with the details of FIPS 201. This includes signing a Subscriber Agreement.

For all levels of assurance certificates for device entities, except basic assurance for computing devices, the subscriber or PKI Sponsor must sign a Certificate Action Form containing the obligations regarding protection of the private key and the use of the certificates prior to being issued any certificates.

4.4.1 Conduct Constituting Certificate Acceptance

Failure to object to the certificate or its contents constitutes acceptance of the certificate.

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

4.4.2 Publication of the Certificate by the CA

CA certificates are published in repositories as specified in section 2.2. Whenever the Internal CA is re-keyed, the new CA cross-certificate will be published onto the http://ipki.uspto.gov website.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

USPTO has an employee who serves as an agency representative to the FPKI Policy Authority. This POC will be responsible for emailing a notification to the FPKIPA contact information provided on the IDManagement.gov website (fpki@gsa.gov).

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

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

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

4.5.2 Relying Party Public Key and Certificate Usage

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

All CA certificates will have both *basicConstraints* and *keyUsage* extensions marked as "critical". Non-CA, end entity certificates have *keyUsage* extension marked "critical" and *basicConstraints* is not marked "critical".

4.6 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number.

When the Federal PKI policy was changed to limit the OCSP certificate validation to 120 days, USPTO began renewing this certificate as described in section 4.6.3.

Subscriber certificates issued under this policy must not be renewed.

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 all certificate subject information remains unchanged. In addition, the validity period of the certificate must meet the requirements specified in Section 6.3.2.

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

OCSP Certificate Renewal

The OCSP keys have a 3-year validity period but allowable certificate life is set to 120 days, so renewal is done frequently per steps below:

- Security Officer calculates the end date of the OCSP cert to be 120 days from the day of renewal.
- SO logs into Entrust SMA and updates the OCSP signing profile with the new expiry date and places the profile in recovery.
- SO gives the reference number to the Administrator who then logs into the VA console to create a CSR using the reference number and existing RSA-2048 or RSA-3072 keys in the HSM partition (SKI in the cert).
- Admin gives the CSR to SO for completion and SO completes the PKCS10 to PKCS7.
- Admin logs into the VA console and uploads the new VA signing certs in all VAs (4 instances) and issues new CRLs and processes them in the VA application.
- Once the proofs are processed, the Admin & SO check the new proofs are signed with new cert.

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 means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key), a different serial number, and may be assigned a different validity period.

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

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

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

Web certificates must follow these procedures, except they have a maximum 2-year lifetime.

4.7.1 Circumstance for Certificate Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that subscribers periodically obtain new keys and re-establish their identities. Section 6.3.2 establishes usage periods for private keys for both CAs and subscribers. Examples of circumstances requiring certificate re-key include: expiration, loss or compromise, issuance of a new hardware token, and hardware token failure. An additional reason for certificate re-key is to support name changes for human subscribers.

4.7.2 Who May Request Certification of a New Public Key

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

The Operational Authority is responsible for operating and maintaining the Internal CA. If a functional technical interdependency occurs which requires re-keying the CA, the Security Officer will initiate the request. SOs may also use the Entrust toolkit programs to request certification of a new public key on behalf of a subscriber.

Subscribers with a currently valid certificate may request certification of a new public key.

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

Re-key requests will be completed as defined in the procedures established by the USPTO Security Division, in accordance with the details of FIPS 201. Requests may also be considered as made when conducted through PKIX-CMP protocols. Re-key follows the same processing steps as initial certificate issuance.

4.7.4 Notification of New Certificate Issuance to Subscriber

As specified in Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

As specified in Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

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

As specified in Section 4.4.3.

4.8 Certificate Modification

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

Certificate modifications will be performed for human subscriber name change purposes and new keys will always be generated. Name change requires proof of name change which re-key does not check.

4.8.1 Circumstance for Certificate Modification

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

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

4.8.2 Who May Request Certificate Modification

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

Subscribers with a currently valid certificate may request certificate modification. CAs and RAs may request certificate modification on behalf of a subscriber.

For device certificates, the human sponsor of the device may request certificate modification.

4.8.3 Processing Certificate Modification Requests

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

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

4.8.4 Notification of New Certificate Issuance to Subscriber

As specified in Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

As specified in Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

As specified in 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

As specified in Section 4.4.3.

4.9 Certificate Revocation and Suspension

USPTO must notify the FPKIPA at least two weeks prior to the revocation of a CA certificate, whenever possible.

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

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

Certificate suspension is not allowed.

4.9.1 Circumstances for Revocation

Revocation procedures for human subscribers must be completed as defined in the procedures established by the USPTO Security Division, in accordance with FIPS 201.

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

- Privilege attributes asserted in the subscriber's certificate are reduced. Notification of this must come from a member of the USPTO Operational Authority either in-person, by phone, by Change Request, or by email.
- The subscriber can be shown to have violated the stipulations of its Subscriber Agreement. Notification of this must come from USPTO Security Managers or the USPTO General Counsel's Office either in-person, by phone, by Change Request, or by email.
- The private key is suspected of compromise. Key compromise situations require a report to be filed with the Policy Authority indicating the circumstances under which the compromise occurred. If accidental, on the part of the Subscriber, no further action is required. Otherwise the Policy Authority will determine if a possible follow up investigation and potential action is required.
- The subscriber, or other authorized party as detailed in Section 3.4 and Section 4.9.2, requests that the subscriber's certificate be revoked.

Whenever any of the above circumstances occur, the associated certificate must 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 must be revoked. Procedures in sections 4.9.2 and 4.9.3 will be followed.

Revoked certificates must be included on all new publications of the CRL until the certificates expire.

4.9.2 Who can Request a Revocation

The CA may summarily revoke certificates within its domain. A written notice and brief explanation for the revocation may subsequently be provided to the subscriber, unless laws, regulations or operating policies defined by USPTO preclude such notification.

The Policy Authority of any cross-certified Certification Authority or the USPTO Policy Authority can request revocation of a cross-certification certificate. The USPTO Policy Authority will review and approve or deny all requests to revoke a cross-certification certificate.

Requests for revocation of subscriber certificates must be completed as defined in the procedures established by the USPTO Security Division, in accordance with the details of FIPS 201.

PKI Sponsors are authorized to submit requests to revoke device certificates.

4.9.3 Procedure for Revocation Request

If it is determined that a private key used to authorize the issuance of one or more certificates may have been compromised, all certificates directly or indirectly authorized by that private key since the date of actual or suspected compromise must be revoked or must be verified as appropriately issued.

Subscriber Certificates

Authorized requestors wishing to revoke a certificate for human subscribers must follow the procedures established by the USPTO Security Division, in accordance with the details of FIPS 201.

Device Certificates

When device certificates are nearing expiration, the PKI Sponsor must take action to ensure continued operation.

- Create and submit a Change Request with separate tasks to 1) renew the certificate and 2) to revoke the old certificate. ***Note***: In the event where the device is no longer in service, there is no need for a certificate renewal task.
- Once the Change Request is validated to include all necessary information, it is approved and the Security Officer will execute the steps to issue the new device certificates (details section 4.3.1).
- After the PKI Sponsor confirms the new certificates have been installed and successfully tested, a Certificate Action Form (CAF) will be completed, signed and sent to request revocation of the old certificates.

The Security officer will use the CA software application to complete the revocation process by placing the revoked certificate's serial number and other identifying information on a CRL. Then the CRL must be posted in the USPTO repository, in addition to any other revocation mechanisms used.

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 must be revoked by the Security Officer.

Revoked certificates must be included on all new publications of the CRL until the certificates expire.

To request a revocation due to a suspected private key compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to certificates, send an email to PKITeam@uspto.gov.

4.9.4 Revocation Grace Period

There is no grace period for revocation.

4.9.5 Time within which CA must Process the Revocation Request

The CA will revoke certificates as quickly as practical upon receipt of a proper revocation request.

Operational Authority Security Officers must process those requests that are not automatically completed as part of routine hardware token updates. SO's must be available to complete revocations during USPTO's normal business hours. Within those normal business hours,

revocation requests must be processed before the next CRL is published, excepting those requests received within two hours of CRL issuance. Revocation requests received within two hours of CRL issuance must be processed before the following CRL is published.

4.9.6 Revocation Checking Requirements for Relying Parties

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

4.9.7 CRL Issuance Frequency

The Certification Authority server is configured to issue Certificate Revocation Lists (CRL) at least every 18 hours. Additional CRLs will be issued upon certificate revocation. Upon issuance, the new CRLs will be published in USPTO EDS Active Directory and other directories as appropriate as soon as is practically possible, but in no case, later than 18 hours following the revocation. The USPTO Certification Authority overwrites the outdated CRL entry in the repository with the most current CRL, which effectively supersedes the outdated copy of the CRL from the repository.

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

4.9.8 Maximum Latency for CRLs

The Entrust Security Manager software is set to publish CRLs immediately to the repository upon generation.

4.9.9 On-line Revocation/Status Checking Availability

An online certificate status protocol (OCSP) responder is available to be used to check certificate status information. The OCSP responder will be automatically updated by the validation authority. The OCSP responses must not be older than 18 hours at a minimum.

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 Advertisement Available

USPTO does not support other forms of Revocation Advertisement.

4.9.12 Special Requirements Related to Key Compromise

In the event of a Certification Authority key compromise, a Certificate Revocation List must be published at the earliest feasible time revoking all certificates issued by that Certification Authority. The CRL issuance must occur within 18 hours of notification.

In the event of a Certification Authority compromise of a cross-certified Certification Authority, the Certification Authority must publish a CRL revoking that cross-certificate.

In the event of a CA certificate revocation or subscriber certificate revocation because of compromise, or suspected compromise, of a private key, a CRL must be issued within 18 hours of notification.

If the Certification Authority distributed its public key in a trusted certificate, the Certification Authority must perform the following operations:

- Generate a new signing key pair and corresponding trusted certificate
- Initiate procedures to notify subscribers of the compromise
- Securely distribute the trusted certificate

If the Certification Authority's public key appears as the subject public key in certificates issued by other Certification Authorities, the Certification Authority will notify the issuers of these certificates as soon as is practicably possible.

4.9.13 Circumstances for Suspension

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

4.9.14 Who Can Request Suspension

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

4.9.15 Procedure for Suspension Request

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

4.9.16 Limits on Suspension Period

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

4.10 Certificate Status Services

Refer to Section 4.9.9 for OCSP.

4.10.1 Operational Characteristics

Not applicable.

4.10.2 Service Availability

Not applicable.

4.10.3 Optional Features

Not applicable.

4.11 End of Subscription

Not applicable.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The CA issuing the Subscriber certificate must escrow all private decryption keys. Escrowed keys must be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber.

The escrowed keys are kept in the CA database which is encrypted with keys which are generated and protected by the CA. Transfer of escrowed keys to subscribers is managed by PKIX-CMP protocols that are part of programs that use Entrust toolkits.

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

4.12.1.1 Key Escrow Process and Responsibilities

Subscriber private decryption keys are securely escrowed in the encrypted CA database prior to issuing the key management certificates to the Subscriber.

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

All Requestors must fill out a Private Key Recovery Form and digitally sign. This form will provide adequate evidence that authenticates and authorizes (e.g. court order) the key recovery request.

Who Can Submit a Key Recovery Request?

- Subscribers are USPTO employees and contractors who are authenticated via their PIV card and are authorized to request recovery of their own escrowed keys.
- Internal Third-Party Requestors are USPTO employees who are authenticated via their PIV card and must provide adequate evidence to authorize their request to recover another Subscriber's private decryption key. For example, someone in USPTO Management who is in the Subscriber's supervisory chain.
- External Third-Party Requestors are individuals outside the USPTO agency who must provide adequate evidence to authenticate and authorize their request to recover a

Subscriber's private decryption key. This process does not require consent or knowledge on the part of the Subscriber who originally held that key.

How are Key Recovery Requests Processed?

- Once a Private Key Recovery form has been approved, the Security Officers are authorized to recover an escrowed Subscriber decryption key. The SO holds a unique credential which resides on a dedicated ikey USB token that has privileges allowing access to the Entrust CA database for the purpose of recovering a Subscriber's private decryption key from escrow. This ikey USB token is kept in the Administrator lockbox, and can only be accessed under two-person controls.
- The SO is not required to notify Subscribers of a Third-Party key recovery.

Key Recovery During Token Issuance

When a Subscriber is issued a new certificate on a hardware token, private key management keys for the Subscriber may be recovered as part of the issuance process as long as the CA uses secure means to inject the key history onto the hardware token directly.

Automatic retrieval of encryption key pairs will be allowed for human entities who are properly authorized to recover their issued certificates and will be accomplished through the use of the security protection provided by Public Key Infrastructure X.509-Certificate Management Protocol. This is part of the normal RA processes for renewing PIV cards; loading the previous decryption keys onto a Subscriber's PIV card.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

The CA must not support session key encapsulation or recovery.

5 FACILITY, MANAGEMENT, & OPERATIONAL CONTROLS

5.1 Physical Controls

Certification Authority and Registration Authority equipment must be protected from unauthorized access at all times; especially while the cryptographic module is installed and activated. Certification Authorities and Registration Authorities must implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. Certification Authority Hardware Security Module tokens and other cryptographic tokens or smart cards issued to Trusted Role individuals must be protected against theft, loss, and unauthorized use.

5.1.1 Site Location and Construction

The Internal Certification Authority is located in the USPTO production Data Center in Alexandria, VA. The building's construction was completed and the building was first occupied in 2004. The building is constructed of reinforced concrete and steel and met all commercial building codes required at the time.

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

The Internal Certification Authority equipment rack is located in the USPTO production Data Center. A guard desk monitors the Data Center entrance on a 24x7x365 basis.

Persons allowed unaccompanied access to the Data Center must possess a USPTO issued photo identity and proximity-based access authorization badge and must have been authorized unaccompanied access by the Physical Security Office and will have registered a private PIN number to be used in conjunction with the badge. The badge must be scanned and the PIN number entered by each person as they enter and exit the Data Center.

Persons not authorized for unaccompanied access, must be accompanied by an authorized person and must register with the guards and receive a temporary proximity badge. Such persons will also be required to scan their badge and enter the assigned, temporary PIN.

Certain PKI servers (CA, VA, CMS, Domain Controller) and the HSMs are all housed in secure racks with locks on all external panels and doors. These locks differ from all other rack locks in the USPTO Production Center. The PKI rack keys are kept in a safe located in the CIO Command Center office area.

The Security Officer holds the combination to open the outer safe that contains the PKI Administrator lockbox. Opening the lockbox is a strictly controlled, two-person process. A Security Officer has the "first key" and only Administrators hold the "second key" and both are required to open the lockbox to gain access to the rack keys. The SO and Administrator are both required to sign a logbook kept inside lockbox, noting the date and time of removal and replacement of the rack key.

The cryptographic modules for the Certification Authority server(s) are installed inside the secure racks. Access to the cryptographic modules will require the presence of at least two authorized persons. No removable cryptographic modules are in use for the Internal CA. The security mechanisms are commensurate with the level of threat in the equipment environment. The physical security requirements for medium assurance Certification Authorities are intended to:

- 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
- Be manually or electronically monitored for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically

Security guards on a 24x7x365 basis monitor the USPTO production Data Center. If for any reason, the facility is to be left unattended, a security check of the facility housing the Certification Authority equipment must occur. At a minimum, the check verifies 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

The Network Engineering Division is responsible for making such checks. A log identifying the person performing a check at each instance must be maintained. If the facility is not continuously attended, the last person to depart must initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 Physical Access for RA Equipment

RA actions are performed by specifically assigned Trusted Role Registration Authorities and in some cases, Trusted Role Security Officers. The actions are performed on USPTO workstations or contractor workstations approved for use to access USPTO’s internal networks.

In addition, an RA function is provided by the Card Management System servers.

USPTO workstations and contractor workstations approved for access to USPTO’s internal networks are protected by the following physical and logical controls:

- On campus offices and workrooms can only be accessed if the person possesses a USPTO issued ID badge that includes an embedded access control identification device (HID CHIP).
- Access via USPTO’s Virtual Private Networks requires two factor authentication and is protected with specifically assigned firewalls.
- The workstations must have up-to-date virus checking software and up-to-date definitions.

- Access to any of the software that provides RA functions requires the use of an issued smart card or token. If the smart card or token is removed from the reader, access to the RA software is broken.

The Card Management System servers are under the same physical and logical access controls as the CA servers, as detailed in Section 5.1.2.1.

5.1.2.3 Physical Access for CSS Equipment

Physical access control requirements for CSS Validation Authority, must meet the CA physical access requirements specified in 5.1.2.1. The responders reside in the USPTO DMZ, so they can respond to requests from outside of USPTO. Communication between the responders and Validation Authorities will be controlled by the USPTO firewalls.

5.1.2.4 Physical Access for CMS Equipment

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

5.1.3 Power and Air Conditioning

The Internal Certification Authority facility is supplied with power and air conditioning sufficient to create a reliable operating environment. In addition, back-up capability is provided for sufficient continued operation to allow an orderly shutdown of application and system actions.

The electrical power and air conditioning systems have systems monitors in the Network Control Center of the Data Center, which is generally manned on a 24x7x365 basis.

Electrical power is provided from two separate, commercial power grids. The grids feed through a high-speed switch that can detect loss of power from the primary grid and trip over to the second power grid. The power is then directed through motor generators, which are part of a Pillar system, including diesel backup generators. The Pillar system can store enough energy to keep the motor generators operating until the diesel backup generators spin-up to full speed. This typically only takes a few seconds.

Power from each motor generator is fed to Power Distribution Units and from there to Remote Power Panels (RPPs). Each rack in the Data Center receives power from each of the two motor generator feeds via the RPPs. Each of the core IPKI host systems has dual, on-line power supplies which are connected to the two separate rack power feeds, one supply to each of the feeds.

In addition, in the event of a catastrophic failure of both grid feeds AND both Pillar backup systems, there are electrical supply connections at the ground floor of the building complex, into which a mobile generator system can be attached.

5.1.4 Water Exposures

Certification Authority equipment is installed on raised, computer room flooring. The USPTO production Data Center, in Alexandria, VA, is on a floor sufficiently above the ground that floodwater is not a concern.

5.1.5 Fire Prevention and Protection

The facility housing the Certification Authority is provided with smoke and fire detectors. The facility includes zoned ceiling sprinklers.

USPTO has facility management processes, which employ and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes. In accordance with the USPTO Campus Lease Agreement, the building management contractor tests all life safety systems (e.g., fire alarm, sprinkler, smoke control, emergency lighting) at least twice a year or as required by Code, whichever is more stringent, to ensure proper operation. The emergency lighting systems cover all emergency exits and evacuation routes. Even though power does not go down in the Data Center or Labs, these life safety systems are periodically tested.

5.1.6 Media Storage

Media used by the Internal Certification Authority is stored in a climate-controlled environment to protect media from damage due to extremes of temperature, humidity and electro-magnetic exposure.

The Internal CA servers' disk drives are co-located in the controlled rack in the USPTO data center. Protections are the same as those detailed in Section 5.1.2.1.

Media that contains security audits, or archive or backup information are stored in the USPTO security safe located in the USPTO Madison West building. The building is operated by a GSA contractor in a manner that provides a normal, business, physical environment.

5.1.7 Waste Disposal

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

Archived CDs and DVDs must be detailed in section 5.5.

5.1.8 Off-site Backup

System backups, sufficient to recover from system failure, must be made on a periodic schedule. USPTO has established online communications to a system in an offsite facility in Manassas, VA, with daily transmissions of backup data sufficient to rebuild the CA if necessary. In addition, only the latest backup is retained and stored in the security safe located in the USPTO Madison West building. Physical and procedural controls commensurate to that of the operational Certification Authority system are employed.

Hourly, incremental backups of the CA database are performed and saved on the server.

At least once, in every 24-hour period, the incremental backups are consolidated and a full backup is completed on the server.

Monday through Saturday, a backup of the database is made as part of a local, full backup facility that is completely contained within the physically controlled equipment racks of the other Certification Authority system.

The full backup archives are rotated weekly, into the USPTO PKI Security safe under at least two-person control. In the event where physical access to the facility where the CA is located is restricted or inaccessible, the USPTO Chief Information Officer will determine the necessary course of action.

5.2 Procedural Controls

5.2.1 Trusted Roles

The people selected to fill these roles are appointed by the Operational Authority Administrator, and must be extraordinarily responsible to ensure the integrity of the CA is maintained.

5.2.1.1 Certification Authority Trusted Roles

The Certificate Policy requirements are outlined into four role categories; 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

The USPTO Trusted Roles staff list and contact information on the IPKI Website will be reviewed at least quarterly.

5.2.1.1.1 Administrator

Administrators primarily act as the Master Users for the Certification Authority. Their Entrust Authority Master User Console passwords are documented and stored in a safe approved by the Operational Authority. The Administrators will also hold special Hardware Security Module PEDS and generate and manage the operation of the Hardware Security Module password for the assigned CA and OCSP Validation Authority partitions.

The Administrators have authority to:

- Install, configure and maintain the Certification Authority
- Establish and maintain the Certification Authority system accounts
- Generate and backup Certification Authority keys
- Perform the Partition Owner duties of the CA Hardware Security Modules

- Perform all Certification Authority key generation, update and recovery activities
- Start the Certification Authority when necessary
- Manage the Certification Authority to Repository related activities
- Manage the Certificate Revocation List/Certification Authority Revocation List publishing activities
- Create new 'soft' Security Officer accounts if directed by the Operational Authority.
- Recover Security Officer accounts
- Secure the storage and distribution of the backups and upgrades to an off-site location

The names of the administrators will be made available to the Compliance Auditor during each compliance audit.

5.2.1.1.2 Security Officer

A Security Officer account is created during the first installation of the Entrust Authority. This account is known as the *First Officer*. This account is a 'soft' account. The OAA will designate a trusted person to activate and be responsible for this account. The First Officer, drawing from selected USPTO personnel and as directed by the Operational Authority may create additional Security Officer Accounts. After the initial setup has been completed, the First Officer account credentials are then revoked.

The main role of Security Officers is to set and administer the Certification Authority's security policy as it applies to all subscribers and Trusted Roles and select and issue credentials to the trusted roles. A USPTO Security Officer has the following privileges and responsibilities:

- Performs cross-certification activities; i.e. agreements, issue resolution, updates, revocation
- Registers personnel into new Security Officer and Auditor trusted roles; issues applicable certificates
- Registers personnel into new Registration Authority roles and issues applicable certificates; manages RA profiles and privileges
- Configures certificate contents, profiles, templates
- Export and import certificate definitions
- Perform Administrator, Security Officer and Domain owner duties for the CA Hardware Security Modules
- Creates Active Directory entries that are necessary for certificate issuance
- Issues and revokes device (web/SSL) certificates
- Perform key recovery as directed by authorized individuals

The Security Officer's accounts, certificates, and keys will be stored on a USPTO hardware token.

The Security Officers will also hold special Hardware Security Module PEDS and generate and manage the operation of the Hardware Security Module administrator password for the Hardware Security Modules assigned to the CA.

The names of the Security Officers will be made available to the Compliance Auditor during each compliance audit.

5.2.1.1.3 Auditor

The Auditor is an agent used primarily for auditing of internal and external processes. Auditor accounts for the Certification Authority will be created and their associated certificates and keys will be stored on a hardware token issued by the USPTO. The names of the Auditors will be made available to the compliance auditor during each compliance audit.

Auditors must be responsible for:

- Reviewing, maintaining, and archiving audit logs
- Reviewing Security Policy, user properties, various reports
- Performing or overseeing internal compliance audits to ensure that the Certification Authority system is operating in accordance with the appropriate CPS
- Labeling monthly backup DVDs with the following information:
    - Title: “IPKI Monthly Backup”
    - Backup date
    - Classification
    - Fully Qualified Domain Names of the machines being backed up
- Labeling the DVD envelope with the following information:
    - Title: “IPKI Monthly Backup”
    - Classification of the information on the DVD media

Auditors must not request or approve certificate issuance.

Auditors must not be allowed to audit any of their own work from a previous role.

5.2.1.1.4 Operator

The Operator is responsible for initially installing and configuring the Certification Authority operating system and for performing ongoing system administration duties such as account management, access control management, system configuration management, database maintenance, software upgrades, compromise reporting, and for performing backups.

The Operator will be responsible for the following activities:

- The initial installation and configuration of the base computing systems, operating system and other USPTO enterprise applications such as:
    - Virus detection software
    - Intrusion detection software

  - Performance monitoring and alerting software
- Configuring, operating and monitoring the local backup systems
- Performing console logon for all users at the Certification Authority, Card Management System, PKI domain controllers, and the Validation Authority servers.
- Performance system backups
- Secure storage and distribution of backups and upgrades to an off-site location

The names of the designated operators will be made available to the compliance auditor during each compliance audit.

Persons filling this role will specifically not be directly responsible nor take direct action to install, recover or upgrade Certification Authority generation components. The installation of the Certification Authority, as noted in Section 5.2.1.1, is the responsibility of the Administrators and Security Officers; however, they will often need to coordinate with an Operator.

5.2.1.2 Registration Authority Trusted Roles

The Registration Authority is the group of individuals who are in the Security Division of USPTO and issues all human subscriber smart cards along with PIV certificates. The RA role is considered to be an Officer as described in 5.2.1.1, and is further divided into four separate roles, as per FIPS 201:

- Sponsor
- Enrollment Official
- Adjudicator
- Card Issuer

This RA group is the primary registration agent for the Certification Authority for PKI-sponsored human subscriber certificates and will be the recipients of all authorization and verification information for such requests

5.2.1.3 Public Key Infrastructure (PKI) Sponsor

A PKI Sponsor fills the role of a Subscriber for non-human devices that are named as public key certificate subjects, and is responsible for controlling their certificates and keys. The PKI sponsor works with SOs to register devices (e.g. routers, firewalls, software programs, web-servers) and is responsible for meeting the obligations of subscribers as defined throughout this document.

PKI Sponsors will not be issued separate smart cards with identities and/or certificates that distinguish them as such. They are issued general subscriber certificates and USPTO smart cards which are used to authorize device certificate issuance.

PKI Sponsors will be issued individual certificates by the Operational Authority Administrator at the same or higher assurance level as the sponsored certificate and are responsible for meeting the obligations of subscribers.

PKI Sponsors may also fill the role of Subscriber as appropriate for disabled personnel.

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.

The tasks listed below require multi-person controls:

- CA key generation*
- CA signing key activation*
- CA private key backup
- Generating private keys on the HSM
- Recover Subscriber private decryption keys from escrow as authorized by the Key Recovery form

Note: An Auditor must witness the CA key generation and CA signing key activation.

Any private keys which are generated on, and backed up from, the HSM will be under two-person controls. These include:

- CSS/VA
- Common PIV Content Signing Key

5.2.3 Identification and Authentication for Each Role

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

5.2.4 Separation of Roles

Individual CA personnel must be specifically designated to assume only one trusted role; Administrator, Security Officer, Registration Authority, Auditor, or Operator.

- Auditors must not request or approve certificate issuance.
- Auditors must not be allowed to audit any of their own work from a previous role.

The following controls are in place for identification and authentication for each Trusted Role.

Table 5-1: List of Items Controlled by the Trusted Roles

Trusted Role	Controls
Administrator	Physical keys to the Administrator lockboxes Password for Entrust Master User Hardware Security Module PED devices and HSM partition passwords

Trusted Role	Controls
Security Officer	Safe combinations Physical guard keys to the lockboxes; used in conjunction with Admin & Auditor keys to open their respective lockboxes. SafeNet iKey 4000 USB Authenticator with Internal Certification Authority credential associated with Entrust Security Officer policy that is separate from a general Subscriber smart card and will have a common name in the Distinguished Name of the certificate that identifies that the holder is a Security Officer. Hardware Security Module PED devices and HSM administrator password.
Auditor	Physical keys to the Auditor lockboxes SafeNet iKey 4000 USB Authenticator with Internal Certification Authority credentials associated with an Entrust Auditor policy. This token is separate from a general subscriber smart card and will have a common name in the Distinguished Name of the certificate that identifies that the holder is an Auditor.
Operator	IPKI domain user ID & password Entrust SM service account admin password Entrust SQL database user ID & password VA SQL database ID & password
Registration Authorities	Roles and responsibilities have been established as per the procedures established by the Security Division according to the guidance of NIST SP 800-79-2 RAs are granted login permissions to Probaris ID and ActivID CMS

5.3 Personnel Controls

5.3.1 Qualifications, Experience, & Clearance Requirements

USPTO personnel and contractor employees are subject to the requirements for a background check. Determination of this requirement is based on job duties and an overall assessment of the

damage that an individual, by virtue of occupying the position, can cause to the integrity of the USPTO, its operations or to the national security.

All persons filling trusted roles as identified in section 5.2.1 must be selected on the basis of loyalty to the United States, trustworthiness and integrity. USPTO personnel and contractor employees must be U.S. citizens to be assigned to fill these trusted roles. The requirements governing the qualifications, selection, and oversight of individuals who operate, manage, oversee, and audit the Certification Authority are in the sections that follow.

5.3.2 Background Check Procedures

The background check procedures have been established by the Security Division, according to the guidance of NIST Special Publications 800-79-2.

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

- Employment
- Education
- Place of residence
- Law Enforcement
- References

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

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

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

5.3.3 Training Requirements

The Operational Authority will ensure appropriate training for personnel involved in USPTO Internal PKI operations. Every Trusted Role member will be trained upon their initial appointment to that role. Training must be in accordance with each specific role. Topics will include:

- Operation of the Certification Authority and component software and hardware
- Operational and security procedures
- Stipulations of the CP and CPS along with local guidance
- All PKI software versions in use on the CA and RA
- All PKI duties that personnel are expected to perform
- Disaster recovery and business continuity procedures

- Key Recovery System security principles and mechanisms

The specific training required will depend on the equipment used and the personnel selected. The Operational Authority will establish an initial training plan for a Certification Authority and its components installation, and document training completed by the PKI personnel. The training is the responsibility of the Operational Authority.

Documentation must be kept that detail the:

- Name and role of the trainee
- Scope of the training
- Dates of the training

5.3.4 Retraining Frequency and Requirements

The USPTO Operational Authority will notify PKI Trusted Role personnel of any changes in the Certificate Policy or Certification Practices Statement that will affect Certification Authority operation. Any significant change to the Certification Authority operation will have an awareness and training plan. Examples include major CA software or hardware upgrades, changes in automated security systems, and relocation of equipment.

The Operational Authority conducts periodic training and maintains a record of the training received by each person appointed to a PKI Trusted Role.

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. The Auditor Appointment Letter has a statement noting to obey the separation of duties.

5.3.6 Sanctions for Unauthorized Actions

The Policy Authority must take appropriate administrative and disciplinary actions against personnel who have performed actions not authorized by the USPTO Internal CP, this CPS document, or other procedures published by the Operational Authority.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to operate any part of the Public Key Infrastructure must be subject to the same criteria as USPTO employees and any additional requirements as defined in this CPS. Currently, there are no additional requirements.

5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role is provided to the personnel filling that role. This documentation includes, but is not limited to:

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

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

5.4 Audit Logging Procedures

All material security events on the Certification Authority's system are automatically recorded in audit log files. Such files are securely archived as per Section 5.5 and in accordance with other applicable USPTO information systems security policies.

Audit log files are generated for all events relating to the security of the CA, as listed in section 5.4.1. For CA-related applications (e.g. OCSP) which are operated in a virtual machine environment, audit logs must be generated for all applicable events on the application software and all system software layers.

As specified in the Certificate Policy, there are other auditable events that are not captured in electronic audit logs. These events, such as physical access events, are manually recorded in paper logs. The Operational Authority is responsible for ensuring that all manual audit log events, as defined by the Policy Authority and the compliance auditor are properly logged and the logs maintained as required.

5.4.1 Types of Events Recorded

All security auditing capabilities of the underlying Certification Authority operating system and the PKI CA applications are enabled at installation and during operation.

The Windows Operation System Event Auditing facility is on. The Entrust CA software, Entrust Security Manager, performs protected, signed auditing of all CA events by default. At a minimum, each audit record includes the following:

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

The following table describes and identifies additional audit events that are recorded:

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

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

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

SECURITY AUDIT

- Any changes to the Audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs

IDENTIFICATION AND AUTHENTICATION

- Platform or CA application level authentication attempts
- The value of maximum authentication attempts is changed
- The number of unsuccessful authentication attempts exceeds the maximum authentication attempts during user login
- An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
- An Administrator changes the type of authenticator, e.g., from smart card login to password

DATA ENTRY AND OUTPUT

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

KEY GENERATION

- Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)

PRIVATE KEY LOAD AND STORAGE

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

TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE

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

PRIVATE AND SECRET KEY EXPORT

- The export of private and secret keys (keys used for a single session or message are excluded)

CERTIFICATE REGISTRATION

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

CERTIFICATE REVOCATION

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

CERTIFICATE STATUS CHANGE APPROVAL

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

CA CONFIGURATION

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

ACCOUNT ADMINISTRATION

- Roles and users are added or deleted
- The access control privileges of a user account or a role are modified

CERTIFICATE PROFILE MANAGEMENT

- All changes to the certificate profile

CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT

- All changes to the certificate revocation list profile

MISCELLANEOUS

- Appointment of an individual to a designated Trusted Role
- Installation of the Operating System
- Installation of the CA
- Installing hardware cryptographic modules
- Removing hardware cryptographic modules
- Destruction of cryptographic modules
- System Startup
- Logon Attempts to CA Applications
- Receipt of Hardware/Software
- Attempts to set passwords
- Attempts to modify passwords
- Backing up CA internal database
- Restoring CA internal database
- Records of manipulation of critical files (e.g., creation, renaming, moving), critical files will vary between installation, and must be identified in the relevant documentation
- The date and time any CA artifact are posted to a public repository
- Access to CA internal database
- All certificate compromise notification requests
- Loading tokens with certificates

- Shipment and receipt of tokens containing key material, or tokens that allow access to key material (e.g., HSM operator cards)
- Zeroizing tokens
- Re-key of the CA

CONFIGURATION CHANGES TO THE CA SERVER:

- Hardware
- Software
- Operating System
- Patches
- Security Profiles

PHYSICAL ACCESS / SITE SECURITY

- Personnel Access to room housing CA
- Access to the CA server
- Known or suspected violations of physical security

ANOMALIES

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

5.4.2 Frequency of Processing Data

A USPTO Auditor will review the audit trail, for policy violations or other significant events, at least as often as specified in the Certificate Policy. The audit trail is made available during any compliance audits. A statistically significant random sample comprising from 1 to 5 percent of the entries will be selected from the security audit data provided that no less than 50 entries of such data will be examined. If activity is less than 50 entries then all of the entries should be reviewed by the auditor. The process to be followed is detailed in section 5.4.9 of this CPS.

The Auditor examines the security audit data, paying particular attention to anomalies and suspicious entries. All security alerts and irregularities are explained in an audit log summary. The Auditor reviews include verifying that the log has not been tampered with, and then briefly inspecting log entries with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews are documented.

This audit log review schedule applies to the CA, CSS, and CMS.

5.4.3 Retention Period for Security Audit Data

The audit log data is kept live on the Certification Authority hardware for at least two months. Security audit log data is also archived in accordance with Section 5.5 of this CPS. Removal of audit logs or backed up security audit logs is directed and witnessed by a USPTO IPKI Trusted Role Auditor. The actual removal is performed by a Trusted Role Operator.

5.4.4 Protection of Security Audit Data

Current physical logs (e.g., rack key issuance logs), from both Alexandria and Manassas Data Centers, will be secured in offices or areas with controlled access. Only authorized personnel will have access to the physical log and only authorized personnel will make entries in physical log or other paper audit records.

The electronic CA audit log is stored in regular operating system flat files. Each CA audit log file consists of an audit header, which contains information about the audits in the file and list of events. A Message Authentication Code is created for each of the audit events and the audit log header. Each CA audit log file has a different audit key used to generate the Message Authentication Code. The Entrust master key for the Certification Authority is used to encrypt the audit key; the encrypted audit key is stored in the audit header.

The CA audit log can be spread across many files. A new CA audit log file is created when the current audit log file reaches a preset size of 1 Mbytes.

The security audit data must not be open for reading or modification by any human, or by any automated process other than those that perform security audit processing. Certification Authority system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data.

Security audit data archive is witnessed by a Trusted Role Auditor who takes possession of any archive media and moves it to their lockbox in the security safe. The Trusted Role Auditor does not have modify access. Further details can be found in Section 5.4.5.

5.4.5 Security Audit Data Backup Procedures

Electronic files considered as security audit logs and audit summaries, should summaries be produced, are backed up on a daily basis, as part of the overall daily system backup. These backups are stored on a local storage subsystem.

On a monthly basis, on each of the servers identified as part of the USPTO Internal PKI core, copies of all security audit logs and audit summaries, should summaries be produced, are made and stored on the local file system. These local file copies are kept for at least two months. Also, each month on each of the core servers, an archive copy of that month’s saved security audit files is stored on DVD media, using a single DVD that is local to one of the protected core servers.

The archived CD-R’s or DVDs are each labeled to indicate from which server the files were copied and the month and year of the particular security audit files. The labels will also include a security classification. The security classification will also be written on the outside of any covers or sleeves used with the CD-Rs and DVDs. These archived CD-Rs and DVDs are stored

in a secured location separate from the Certification Authority equipment and are under the control of USPTO Internal PKI Security Officers and Auditors at all times.

Manual security audit logs are collected on a periodic basis and also stored in a secured cabinet in a Trusted Role Security Officer's office.

5.4.6 Security Audit Collection System (Internal vs. External)

The audit backup system is external to the Entrust Authority Security Manager software.

The security audit process must run independently and must not in any way be under the control of the Certification Authority. The Windows Operating System baselines, including setting of the events logging, is managed by the Windows System Security Group. Only assigned, Trusted Role Operators have logon privileges to the core CA, CMS and IPKI Domain Controller system servers. Security audit processes must 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 must determine whether to suspend Certification Authority operation until the problem is corrected. The Policy Authority must be notified immediately of such condition and of the decision to suspend Certification Authority operation.

Audit collection systems must 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

The USPTO CP imposes no requirement to notify a subject that an event was audited.

5.4.8 Vulnerability Assessments

All systems deployed on USPTO networks are included in USPTO comprehensive and continuous Security Authorization activities. The IPKI Trusted Role personnel work closely with Security Authorization assessors to provide technical and process information that does not compromise the auditable integrity of the core IPKI systems. All systems are assessed and scanned for security vulnerabilities on approved schedules. USPTO uses the Nessus Network Monitor tools to perform vulnerability scans to generate analysis reports which are sent to the system owners. Any corrective actions are reviewed, and scheduled for implementation using standard USPTO change management processes.

The Operational Authority is also watchful for anomalies and attempts to violate the integrity of the system, including the equipment, its physical location, and its personnel. The IPKI Auditor inspects the CA and CMS audit logs at least monthly. A record of the audit is kept by the Auditor. Any suspicious activity is detected by USPTO CIO Command Center (C3) and is reported to the Department of Commerce Computer Emergency Response Team. The review includes looking for events such as repeated failed actions, requests for privileged information, attempted access of system files, unauthenticated responses and continuity of security audit data. Suspicious activity will also be reported to the Policy Authority.

5.4.9 PKI Audit Log Examination Process

The auditor must examine the logs no less than monthly and must report his findings on the PKI Audit Log Examination Report.

The auditor's findings must include an indication that no suspicious activity was found, if that is the case, as well as a description of any suspicious activity indicated by the audit. The PKI Auditor may consult with other PKI trusted roles, particularly the Operator or Administrator, or other technical staff in their analysis of the suspicious activity.

A brief note will be made of the explanation of any activity, to include suspicious activity, which was explained as a technical anomaly or otherwise and be kept as part of the log examination record.

If anything at all seems suspicious, it will be noted in the review notes. The PKI Audit Log Examination Report will be copied to the PKI backup DVD, and placed in the Alexandria Campus safe.

If upon consultation with appropriate trusted role holders or technical staff, the activity is not adequately explained, the finding must be sent to USPTO Cybersecurity Division for formal investigation as a security incident.

The Cybersecurity Division is in charge of the Incident Handling and Response service at USPTO. The Cybersecurity Division must follow its established investigation process, initiate disciplinary procedures as required and issue an investigation report the results of which must be shared with the PKI Auditor.

The auditors log examination must be recorded on the PKI Audit Log Examination Report form. One copy of the form must be retained by the Auditor and one copy must be printed, holographically signed (ink signature) and date and retained as part of the auditor's notebook that is maintained by the Internal PKI Security Officer(s).

5.5 Records Archival

All software applications required to process the archival data must be archived to ensure that data can be viewed or examined at a later point in time[2]. USPTO standard applications, such as Operating Systems and enterprise backup software for master and client roles, will only be archived if and when the use of a particular product or version of that product is no longer going

[2] In this Certification Practices Statement, "archival", "archived" and "archive" should be understood to refer to the body of records generated by the Public Key Infrastructure that are managed over time according to applicable Federal and USPTO record management policies. It is unlikely that any of the Certification Authority records will be Archival as that term is used in records management, i.e., required to be preserved indefinitely, although some records may be long term temporary records. Records relating to the operation of the Certification Authority shall be preserved in a manner consistent with the Federal Records Act and with National Archives and Records Administration regulations and guidance published as Records Management Guidance for Public Key Infrastructure-Unique Administrative Records, as well as, USPTO Records Management Policy.

to be used in production at USPTO, or the archived data is known to not be backwards compatible for reading by such newer products or versions.

5.5.1 Types of Events Archived

Archival records for the Certification Authority must be sufficiently detailed to establish the proper operation of the Public Key Infrastructure or the validity of any certificate (including those revoked or expired) issued by the Certification Authority.

The following table identifies the archive records that are retained:

- Certificate Policy
- Certification Practice Statement
- Contractual obligations
- Other agreements concerning operations of the CA
- System and equipment configuration
- Modifications and updates to system or configuration
- All records related to certificate request authorization, approval and signature, whether generated directly on the CA or generated as part of a related external system or process
- All records related to certificate revocation, whether generated directly on the CA or generated as part of a related external system or process
- Subscriber identity Authentication data as per Section 3.2.3
- Documentation of receipt and acceptance of certificates
- Subscriber Agreements
- Documentation of receipt of tokens
- All certificates issued or published
- Record of Certification Authority Re-key
- Other data or applications to verify archive contents
- Audit summary reports generated by internal reviews and documentation generated during third party audits
- Any changes to the Audit parameters, e.g., audit frequency, type of event audited.
- Any attempt to delete or modify the Audit logs.
- Whenever the CA generates a key (Not mandatory for single session or one-time use symmetric keys).
- All access to certificate subject private keys retained for key recovery purposes.
- Audit summary reports generated by internal reviews and documentation generated during third party audits
- The export of private and secret keys (keys used for a single session or message are excluded).
- The approval or rejection of a certificate status change request.
- Appointment of an individual to a Trusted Role.
- Destruction of cryptographic modules.
- All certificate compromise notifications.
- Remedial action taken as a result of violations of physical security.

- Violations of Certificate Policy
- Violations of Certification Practice Statement.
- Auditor Training

5.5.2 Retention Period for Archive

Archive retention periods begin at the CA key generation event. Whenever the CA is re-keyed, a new retention period begins for each subsequent key generation event.

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

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

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

5.5.3 Protection of Archive

The archive data will be digitally signed when appropriate. This will provide an integrity check that can be used to verify the data has not been modified.

Long-term archive data for the Certification Authority is recorded on DVD read-only media, written in a manner to exclude allowing multi-session writing, and stored in the security safe in the USPTO Madison West building. Short-term backup media is also stored in the security safe in the USPTO Madison West building. The archive media is protected by physical security in that it is retained such that only Trusted Role Auditor personnel have access. Security Archives are protected by the physical security practices defined in section 5.1.

The archives will be labeled with the Certification Authority Distinguished Name and the date.

The distinguish name for the Internal Certification Authority is:

"*cn=USPTO_INTR_CA1,cn=AIA,cn=Public Key Services,cn=Services,cn=Configuration, dc=uspto,dc=gov*"

A list of Trusted Role persons that have the permissions necessary to access and delete the on-line archive files will be maintained at the Certification Authority site, and all accesses will be recorded. These records will be made available to the auditors during compliance audits.

No unauthorized user must be able to modify or delete the archive, but archived records may be moved to another medium. Any transfer to another medium will be performed by a Trusted Role Security Officer and will be witnessed by a Trusted Role Auditor. Both the Auditor and Security Officer must sign a statement that details the records transferred and how the original records

were disposed, if disposal occurred. The new media will be labeled with the same information as the original media and will also be labeled to note that the records were transferred and the date of transfer. The Security Officer will use a workstation on a USPTO internal network and will ensure that no intermediate, scratch, or temporary copies of the records are left on the workstation once the transfer to the new medium is complete.

The contents of the archive must 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. Any archived record that contains private keys, for example escrowed private encryption keys, must only be transferred via trusted, secure communications channels, or must be hand delivered to a specifically authorized recipient who must 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 and that the specific recipient must sign a receipt which is returned to USPTO.

5.5.4 Archive Backup Procedures

USPTO does not back up its archived records.

5.5.5 Requirements for Time-Stamping of Records

The Internal PKI servers use their own system clocks for time stamping purposes. These servers' system clocks are kept synchronized with a USPTO Authoritative Time Service via the Network Time Protocol. The USPTO Authoritative Time Service receives its master time updates from a NIST approved service.

5.5.6 Archive Collection System (Internal vs. External)

Certification Authority archive data will be collected as part of the routine system backup procedures and will include explicit file copies of Certification Authority files that do not reside in the underlying Certification Authority database.

5.5.7 Procedures to Obtain and Verify Archive Information

The Operational Authority will provide access to archive information to the Compliance Auditor or other authorized requestor. The Operational Authority is responsible for ensuring that the request comes from an authorized source. The archive condition is verified during every compliance audit.

Access to the archive record DVDs is protected by two-person controls:

- The archive is held inside the Auditor's lockbox, which is stored in the C3 safe; providing two layers/levels of protection.
- Only the Security Officers hold the combination to open the C3 safe; it is not accessible by any of the other Trusted Roles.

- After the SO opens the safe, the Auditor can then retrieve the auditor lockbox. Opening the Auditor's lockbox is under two-person controls, requiring two keys to open: 1) the master key held by the SO and 2) the auditor key held by the Auditor.

See Section 5.5.3 for information on how to request archived records.

5.6 Certification Authority Key Changeover

The certificates for the Certification Authority are set up for manual key update. A Key Generation Ceremony for Key Changeover is required, similar to the key generation portion of the initial Key Generation Ceremony. The key changeover requirements are detailed in the Internal PKI/Smart Card Installation Key-Signing Ceremony Activities Plan, version 1.0.

To minimize risk to the Public Key Infrastructure through compromise of a Certification Authority's private signing key, the private signing key will 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 Certificate Revocation Lists that contain certificates signed with that key, then the old key must be retained and protected.

The Certification Authority's signing key must have a validity period as described in section 6.3.2.

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

All RAs, Operators, Auditors, Administrators, and Security Officers that were not present at the key update activity will be notified by email that the key updated occurred. Subscribers who specifically request notification of such events will also be notified by email.

The CA generates key rollover certificates, where the new public key is signed by the old private key, and vice versa, when a key update action occurs.

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

5.7 Compromise and Disaster Recovery

The Certification Authority has recovery procedures in place to reconstitute the Certification Authority within 72 hours in the event of a catastrophic failure.

Recovery events will be well-documented, including actions taken, problems encountered during the recovery & reconstitution effort, and lessons learned. It is the responsibility of the Contingency Plan (CP) team to document their actions during the recovery & reconstitution

effort, and to provide that documentation to the CP Coordinator. Documentation that should be collected after a contingency activation include:

- Activity logs (recovery steps, time when steps were initiated and completed, problems encountered while executing activities);
- Functionality and data testing results;
- Lessons learned documentation; and
- After Action Report.

See the ID-Auth Information System Contingency Plan (ISCP) for additional information.

5.7.1 Incident and Compromise Handling Procedures

The USPTO PKI Policy Authority must be notified if any CAs operating under this policy experiences the following:

- Suspected or detected compromise of the CA systems
- Suspected or detected compromise of a certificate status server (CSS) if 1) the CSS certificate has a lifetime of more than 72 hours and 2) the CSS certificate cannot be revoked (e.g., an OCSP responder certificate with the id-pkix-ocsp-nocheck extension)
- Physical or electronic penetration of CA systems
- Successful denial of service attacks on CA components
- Any incident preventing the CA from issuing a CRL within 24 hours of the issuance of the previous CRL

In the event of an incident as described above, the USPTO must notify the FPKIPA within 24 hours of incident discovery, along with preliminary remediation analysis.

Once the incident has been resolved, the Operational Authority, working in conjunction with the USPTO PA, must provide notification directly to the FPKIPA, including detailed measures taken to remediate the incident. The notice must include the following:

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

The notification provided directly to the FPKIPA must also include detailed measures taken to remediate the incident.

If the Certification Authority’s signing key is compromised, the Policy Authority will determine if the Certification Authority key may be updated or the Certification Authority must be terminated.

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

In the event of an inoperative Certification Authority due to equipment damage, software or Operating System failure, or data corruption, where all copies of the Certification Authority signature keys are **not** destroyed, the following steps, at a minimum, are taken to recover a secure environment:

- The Certification Authority infrastructure (hardware and software) will be re-built and/or restored from backup as necessary.
- The directory data, encryption certificates, and CRLs are restored if the directory becomes unusable and must be restored from backup or if the directory is suspected to be corrupt.
- If Certification Authority equipment is damaged or rendered inoperative, but the Certification Authority signature keys are not destroyed, Certification Authority operation must be reestablished as quickly as possible, giving priority to the ability to generate certificate status information. The USPTO Policy Management Authority must be notified as soon as possible.

5.7.3 Certification Authority Signature Keys Are Compromised

In the event of the compromise, or loss (such that a compromise is possible), of the Certification Authority key, the Operational Authority will inform the USPTO Policy Authority via secure email or person-to-person communication. The USPTO PA must then provide details of the compromise to the FPKIPA, so they can prepare to revoke the cross-certificates.

The USPTO PA will authorize the Operational Authority to revoke the CA certificate, and may also authorize generating a new CA certificate to publish into the directory.

The Operational Authority will notify all entities and Subscribers of the CA key compromise via secure email, if possible. When the new CA certificate becomes available, all entities and Subscribers will have the opportunity to install the new CA certificate.

If desired and approved by both parties, the USPTO PA will direct the Operational Authority to complete a new cross-certificate process.

The USPTO Internal CA does not distribute its private keys, in any form, outside of its assigned hardware cryptographic modules with the exception of the secure backup tokens for the hardware cryptographic modules.

The Operational Authority must also investigate and report to the FPKIPA what caused the compromise or loss, and what measures have been taken to preclude recurrence.

Within 10 business days of incident resolution, a notice will be posted on the public web page: http://ipki.uspto.gov. See Section 5.7.1 for contents of the notice.

5.7.4 Business Continuity Capabilities after a Disaster

In the event of a disaster whereby the Certification Authority installation is physically damaged and all copies of the Certification Authority signature key are destroyed, the following steps, as a minimum, will be taken to reestablish a secure environment:

- The USPTO Policy Authority must be immediately and securely notified and must take whatever action is deemed appropriate, including notifying the Federal PKI PA.
- The Certification Authority infrastructure (hardware and software) will be re-built at a backup facility by reestablishing the Certification Authority equipment, generating new private and public keys, being re-certified, and re-issuing all cross certificates.
- The Certification Authority infrastructure will be recovered using backups (from previous local or off-site backups that were stored).
- The directory data, encryption certificates and CRLs, will be restored to the directory.

Notification Related to Compromise or Disaster

In any event involving Certification Authority key compromise or a disaster rendering the Certification Authority non-functional, the USPTO Policy Authority must securely notify all appropriate cross-certified Certification Authorities (e.g., the Federal Bridge Certification Authority) of the situation relating to compromise or disaster at the earliest feasible time in accordance with applicable Memorandums of Agreement and any other contractual agreements. If the Certification Authority signature keys are compromised or lost such that compromise is possible even though uncertain, the PKI Operational Authority Administrator will cause an investigation to be conducted and report to the FPKIPA concerning the cause of the compromise or loss and what measures have been taken to prevent recurrence. The FPKIPA, will in turn, notify the appropriate authorities in accordance with applicable Memorandums of Agreement and any other contractual agreements.

Certification Authority Cannot Generate Certificate Revocation Lists

In the event of an inoperative Certification Authority, where all copies of the Certification Authority signature keys are **not** destroyed, the following steps, at a minimum, will be taken to recover a secure environment:

- The Certification Authority infrastructure (hardware and software) will be re-built and/or restored from backup as necessary.
- The directory data, encryption certificates and CRL, are restored if the directory becomes unusable and must be restored from backup or if the directory is suspected to be corrupt.
- If the Certification Authority cannot issue a CRL prior to the time specified in the next update field of its currently valid Certificate Revocation List, then the USPTO PA must be immediately and securely notified. This notification will allow Relying Parties to protect their interests. The USPTO PA must determine whether to revoke the certificate issued to the Certification Authority. The Certification Authority must reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS.

- The CA must immediately and securely advise the USPTO PA in the event of a disaster where the CA installation is physically damaged and all copies of the CA signature keys are destroyed.

5.8 CA or RA Termination

In the event that the Certification Authority ceases operation or is otherwise terminated:

- All subscribers and Relying Parties must be promptly notified of the cessation.
- All Certification Authorities with cross-certification agreements that are current at the time of cessation will be informed so that cross-certificates to the Certification Authority may be revoked.
- All certificates issued by the Certification Authority must be revoked no later than the time of cessation.
- All current and archived Certification Authority identity proofing, certificate, validation, revocation/suspension, renewal, policy and practices, billing, and audit data must be archived as specified in Section 5.5.
- Any issued certificates that have not expired, must be revoked and a final long term CRL with a nextUpdate time past the validity period of all issued certificates must be generated. This final CRL must 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 FBCA will be destroyed.
- The RA must archive all audit logs and other records prior to termination and destroy its private keys upon termination. Archived audit logs must be retained for 3 years as described in 5.5.2.

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

SafeNet LunaSA Hardware Security Modules validated to FIPS 140 Security Level 3 are used to generate and store the CA private key. Security Officers and Administrators use SafeNet LunaSA PED keys and partition passwords to setup and allow the Certification Authority to access the assigned SafeNet LunaSA partition for key generation and subsequent invocations.

The Internal CA key generation procedures are documented and generate auditable evidence as proof that proper procedures are followed. These procedures detail how the appropriate separations of duties were used during the initial USPTO Internal PKI/Smart Card Installation Key-Signing Ceremony, version 1.0. An independent third party validated the key generation ceremony.

Subsequent CA key updates are completed under detailed installation instructions that maintain appropriate separations of duties and are witnessed by an Auditor.

Up till December 31, 2010, the Internal CA used Secure Hash Algorithm-1 when generating digital signatures. On or after January 1, 2011, signatures on certificates and CRLs will be generated using, at a minimum, Secure Hash Algorithm-256.

The Certification Authority key pair generation will be in compliance with Public Key Cryptographic Standard #1, including the tests for primality. The private key will never be exposed outside the module in unencrypted form. Secure backup copies of the CA keys will be created in order to support the high availability CA configuration and Disaster Recovery.

An independent third party must validate the execution of the key generation procedures either by witnessing the generation or by examining the signed and documented record of the key generation.

If CA Hardware Security Modules are replaced, the CA will be re-keyed. Previous HSMs and their contained keys will be kept within the CA server or controlled rack enclosure at least until such time as any certificates issued using the earlier CA keys are expired, recovered or revoked. Alternatively, replaced HSMs may be removed from the CA server or controlled rack only if they are fully zeroized. Any such zeroization and removal will be witnessed by a USPTO PKI Auditor who must record the serial number of the HSM and the date and time that the zeroization took place.

6.1.1.2 Subscriber Key Pair Generation

The process of requesting credentials will be managed by the Entrust Security Manager Administration software, Entrust Enrollment Server for Web software, Entrust Security Manager

command line processes, or software that uses approved Entrust toolkit modules. In all cases, the core cryptographic software routines will be FIPS 140 Level 2 or higher approved.

For credentials that will be stored on USPTO smart cards and tokens, the generation of signing key-pairs will occur on the cryptographic modules that are part of the USPTO smart cards or tokens. The smart cards and tokens do not allow exposure of plaintext secret keys outside of the cryptographic modules. These smart cards and tokens are FIPS 140 Level 2 or higher certified modules. The subscriber's encryption key pairs will be generated at the Certification Authority machine, and securely delivered to the subscriber.

For credentials that will not be stored on hardware tokens, typically for NPE devices or software applications at USPTO whose certificate requests and installation are managed by PKI Sponsors, the generation of signing key-pairs will occur on software cryptographic modules that are part of the NPE device controlling software or firmware. The public signature key is delivered to the Certification Authority typically in a Public Key Cryptographic Standard #10 request.

6.1.1.3 CSS Key Pair Generation

Cryptographic keying material used by CSSs to sign status information must be generated in FIPS 140 Level 2 or higher validated cryptographic modules.

6.1.1.4 PIV Content Signing Key Pair Generation

Cryptographic keying material used by PIV issuing systems or devices for Common PIV Content Signing must be generated in FIPS 140 Level 2 or higher validated cryptographic modules. For all other PIV issuing systems or devices, the module(s) are FIPS 140 Level 2 or higher. Key generation procedures must be documented.

6.1.2 Private Key Delivery to Subscriber

All subscriber private signature keys will be generated and remain within the crypto boundary of the cryptographic module used to generate the key-pairs used in the certificate request.

In the case where the Certification Authority generates encryption key-pairs, the Certification Authority will deliver, through tokens or smart cards, the private and public keys using the security protection provided by Public Key Infrastructure X.509-Certificate Management Protocol.

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 using the security protection provided by Public Key Infrastructure X.509-Certificate Management Protocol. In all cases, the following requirements must be met:

- Anyone who generates a private signing key for a Subscriber must 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 must acknowledge receipt of the private key(s).
- Delivery must 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 must be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data must be delivered using a separate secure channel.
    - For shared key applications, organizational identities, and network devices, see also Section 3.2.

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

6.1.3 Public Key Delivery to Certificate Issuer

The CMS and CA applications are closely integrated to establish a delivery mechanism to bind a Subscriber's public keys to their verified identify.

Digital Signature Based Certificates

During the PIV card encoding process, the CMS application instructs the PIV card to generate three new asymmetric key pairs:

- PIV Authentication,
- Digital Signature
- Card Authentication

After the key pairs are created, CSRs containing the public keys are created for the three certificates, then CMS invokes the Entrust toolkit (embedded within CMS software) to complete the PKCS10/CSR request by the CA over a TLS/XAP protocol.

After the CMS application receives the certificates created by the CA, it completes the PKCS7 operation by writing the certs to the protected container of the PIV card.

Encryption Certificates

The encryption key and certificate are always created on the CA and pushed to the PIV card via the CMS application. The CMS application uses a TLS channel to write the encryption's cert (private key & cert) to the protected container of the card.

Transport certificate is used within the CMS application to build a TLS tunnel between the PIV card and the CA Entrust toolkit, so no other elements can see or capture what the CA is sending to the card. This same method is also used to write previously escrowed keys/certs to the card-if there are any.

6.1.4 CA Public Key Delivery to Subscribers/Relying Parties

The Certification Authority's signature verification certificate will be provided to all subscribers during the certificate issuance phase described in Section 4.3. The communication between the Certification Authority and the Card Management System is protected using the Public Key Infrastructure X.509-Certificate Management Protocol.

Relying Parties must also be granted access to the CA's public key certificate in order to establish and verify certification trust paths. In order to distribute the CA public key certificate, the CA publishes its public key certificate in the USPTO EDS Active Directory and in a container that is available via anonymous read-only access.

Additionally, the CA's verification certificate may be distributed via a Secure Socket Layer protected USPTO web site or other means as directed by the Policy Authority.

The Federal Bridge Certification Authority (FBCA) posts the cross-certificates it issues in the FBCA repository. The Internal CA must issue a certificate to the FBCA for posting to their repository concurrent with the issuance of a FBCA certificate to the Internal CA. The Internal CA will then make a copy of the FBCA public key available in the USPTO Internal CA certificate, which facilitates trust path validation. For the Internal CA to issue cross-certificates to the FBCA, the FBCA must transport its public key to the Internal CA in a secure, out-of-band fashion to affect certificate issuance.

6.1.5 Key Sizes and Signature Algorithms

All FIPS-approved signature algorithms are considered acceptable.

If the USPTO Policy Authority determines that the security of a particular algorithm may be compromised, the CA must revoke all certificates signed using that algorithm and all certificates that assert that algorithm for the Subscriber (in order to support continued compliance with the Memorandum of Agreement).

This CPS requires use of RSA PKCS #1 signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy contain RSA public keys.

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

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

End entity certificates issued under id-pto-basic-2003 or id-pto-medium-2003 will contain RSA public keys that are at least 2048 bits.

6.1.6 Public Key Parameter Generation

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

Parameter quality checking (including primality testing for prime numbers) must 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 must 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.

Public keys that are bound into CA certificates must be used only for signing certificates and CRLs. CA certificates whose subject public key is to be used to verify other certificates must assert the keyCertSign bit. CA certificates whose subject public key is to be used to verify CRLs must assert the cRLSign bit. If the CA certificate is to be used to verify both certificate and CRLs, both the keyCertSign and cRLSign bits must be asserted.

Certificates to be used for digital signatures (including authentication) must assert the digitalSignature and nonRepudiation bits. Certificates to be used for key transport must assert the keyEncipherment bit for Rivest, Shamir, and Adleman keys. Certificates to be used for key agreement must assert the keyAgreement bit for Diffie-Hellman or elliptic curve Diffie-Hellman keys.

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 must be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CPS. Such "dual-use" certificates must never assert the nonRepudiation bit, and must 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 must always be present and must not contain anyExtendedKeyUsage {2.5.29.37.0}. Extended Key Usage OIDs must be consistent with key usage bits asserted.

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

The dataEncipherment, encipherOnly, and decipherOnly bits must not be asserted in certificates.

The Entrust Security Manager software that is used to realize the Certification Authority uses certificate templates and a master certificate specification file to construct certificates. The certificate templates used for all types of issued certificates enforce the key usage bit settings noted here.

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 the latest version of the FIPS 140 series, *Security Requirements for Cryptographic Modules*.

Certification Authority signing private key storage is performed using a pair of SafeNet LunaSA hardware cryptographic modules that are validated to FIPS 140-2 Security Level 3.

Private Key storage for Certification Authority Subscribers who will store their credentials on USPTO smart cards is performed using a hardware cryptographic module that is validated to FIPS 140 Security Level 2 or higher. PIV cards must only be issued using card stock that has been tested and approved by the FIPS 201 Evaluation Program and listed on the GSA Approved Products List (APL). Card stock that has been removed from the APL may continue to be issued for no more than one year after GSA approved replacement card stock is available. PIV cards issued using the deprecated card stock may continue to be used until the current Subscriber certificates expire, unless otherwise notified by the FPKIPA/FPKIMA.

Private Key storage for Certification Authority subscribers who may store their credentials in a software form (such as Web Servers, Applications programs, or communications hardware devices) will use software cryptographic modules that are validated to FIPS 140 Level 2 or higher.

All cryptographic modules operate such that the private asymmetric cryptographic keys are never output in plaintext.

6.2.1.1 Custodial Subscriber Key Stores

Not applicable.

6.2.2 Private Key Multi-Person Control

A two-person process will control access to the Certification Authority signing key. The CA's private signing key, and any cloned copies, are generated and stored on a Hardware Security Module, as defined in Section 6.1.1 and 6.2.1. The SafeNet LunaSA Pin Entry Device (PED) hardware tokens and certain passwords must be used to authorize access to the HSMs.

The USPTO HSMs do not allow remote logon, therefore, a Security Officer and an Administrator will have to be present at the CA console to use their SafeNet PED tokens and/or SafeNet LunaSA passwords to authorize access by the CA to the HSM.

A Trusted Role Operator will also need to be present to logon to the system console before a Security Officer can authenticate and authorize access to and use of the HSM.

Practice Note: USPTO has set the LunaSA HSMs used for the Certification Authority to allow auto-activation of the partition that holds the CA key. This is being allowed because the auto-activation may only occur if the HSM loses power for less than a few minutes. This allows the HSMs to resume operation and the CA to access its keys following brief power outages without specific intervention by Trusted Role personnel. Auto-activation will not take place if the outage

is longer than a few minutes and it will then be necessary for a Trusted Role Operator, Security Officer and Administrator to work at the console of the CA, at the secured rack, to reactivate the HSM and the CA partition on the HSM.

6.2.3 Private Key Escrow

CA private keys are never escrowed.

Subscriber key management keys are escrowed in the CA database to enable key recovery as described in section 4.12.1.

6.2.4 Private Key Backup

CA Private Signature Key

The Certification Authority Private Signing Key will be backed up and can be recovered.

The SafeNet LunaSA Hardware Security Modules used by the CA provide for backup of the contents of configured partitions. The backup is made to a secure Luna Remote Backup HSM. The actual backup process requires two-person control executed by a Security Officer and an Admin. Those persons must use their SafeNet PED tokens, token PINs, and additionally the Admin, in the role of the Partition Owner, must use their Partition Password. Restoration of the keys is accomplished using the secure Luna Remote Backup HSM and requires actions by a Security Officer and an Admin.

One copy of the Luna Remote Backup HSM is kept in the USPTO PKI safe which is located in a building separate from that which houses the CA and SafeNet LunaSA Hardware Security Modules. Additionally, there is one copy of the Signing Key at USPTO's Alternate Processing Site location in Manassas, VA.

Subscriber Private Key

A subscriber's private signing key is never backed up, in order to provide support for non-repudiation services.

Subscriber Private Key Management Key

All subscriber encryption key pairs are backed up in the USPTO Certification Authority encrypted database. The Entrust Security Management software maintains a full backup of the Certification Authority database automatically.

CSS Private Key

CSS private keys will be backed up. All copies must be accounted for and protected in the same manner as the original.

Common PIV Content Signing Key

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

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

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 must 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 are not escrowed or archived.

Private encryption keys are escrowed by the Certification Authority service.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Private keys are generated within the cryptographic module. Use of FIPS 140, Level 3 approved SafeNet LunaSA Hardware Cryptographic Modules prevents exposure of unencrypted key outside the cryptographic modules.

Private keys associated with signature certificates must be generated by and remain in a cryptographic module during normal operation.

In the event that the 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 plain-text form outside the cryptographic module boundary.

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

The only permitted entries of private keys into cryptographic modules are for the Certification Authority to deliver private encryption keys to the subscriber and for the controlled restoration of the Certification Authority keys to a replacement or backup Hardware Security Model as detailed in Section 6.2.4.1.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS 140.

6.2.8 Method of Activating Private Key

The Certification Authority cryptographic module retrieves and activates the CA private signing key only when needed. The CA private signing key is never exposed outside of the cryptographic module.

Subscribers must be authenticated to cryptographic modules before the activation of any private key(s). The subscriber authenticates to the cryptographic module by the use of a Personal Identification Number (PIN) or password, whichever is appropriate for the cryptographic module

in use (e.g.; PIN for smart card hardware tokens and password for the keystore of a Java, OpenSSL cryptographic module).

When pass-phrases or PINs are used, they must be a minimum of six (6) characters. Entry of activation data is protected from disclosure (i.e., the data is not 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	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	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 Key

The Certification Authority's private signature key is not open for access when the certificate issuance application is stopped, or the underlying operating system is shutdown.

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 must be removed and stored in a secure container as outlined in Section 5.1.2, when not in use.

The cryptographic modules are physically protected from unauthorized access by being contained within the Internal CA's cabinet in the USPTO Data Center which is never left unattended.

Access to the hardware security module partition that contains the CA private key is limited to only the CA servers which are specifically and bi-directionally registered via strong cryptographic credentials with the hardware security modules.

For those subscribers using a hardware cryptographic token, the subscriber's token will be deactivated by removing the smart card from the reader.

6.2.10 Method of Destroying Private Key

The Internal CA signing key is held on a hardware device. If required, the Certification Authority signing key would be destroyed using zeroization.

Subscriber PIV cards contain a hardware cryptographic token, and are fully reinitialized using a vendor-supplied utility that will zeroize the token during revocation. Subscriber private signature keys will be overwritten during reissuance or other update actions.

Subscriber PIV cards must be surrendered to the Security Service Center (SSC) and destroyed under the following circumstances:

- When the PIV card has expired
- Employee or contractor has left USPTO (termination of employment, end of contract, etc.)
- When the PIV card is replaced with a new card due to name change, reissuance, re-enrollment, etc.
- When the PIV card is lost, stolen, or out of direct control of the owner, in accordance with FIPS 201, the card must be destroyed.
- When the PIV card has topographical defects (e.g., scratches, poor color, fading, etc.) or printing errors.

When a PIV card is returned to the USPTO SSC, the card will be:

- Revoked in the physical access control database
- Revoked in the HSPD-12 Card system
- Physically destroyed with concern for PII data

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 encryption keys are archived automatically by the Certification Authority.

6.3.2 Certificate Operation Periods and Key Usage Periods

Manual key updates must be performed when needed. Such updates will be documented and follow all multi-person requirements for CA keys specified in this CPS.

Table 6-1: Certificate Authority Key Validity Period

Key Type	Private Key	Certificate
Signature	10 years	10 years

The maximum key validity periods for certificates issued to smart cards are as follows:

Table 6-2: Smart Card Validity Periods

Key Type	Private Key	Certificate
Subscriber Encryption	Not Applicable	3 years
Subscriber Signature	3 years	3 years
Card Auth	3 years	3 years
Subscriber Authentication	3 years	3 years

The maximum key validity periods for certificates issued to PKI Sponsors for use on devices, software applications or for code and content signing are as follows:

Table 6-3: Device Validity Periods

Key Type	Private Key	Certificate
Encryption	Not Applicable	2 years
Signature Non-Repudiation	100% Certificate Validity	2 years

Table 6-4: OCSP Validity Periods

Key Type	Private Key	Certificate
OCSP Responder	3 years	120 Days

Table 6-5: Signing Validity Periods

Key Type	Private Key	Certificate
Content Signing	3 years	8 years
Code Signing	3 years	8 years

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data (i.e., biometrics, password or Personal Identification Number) will be used to protect access for use of a token, smart card, PIV card or private keys.

Password-type activation data (i.e., not biometric or Personal Identification Number) used by the subscribers is required to meet the following criteria:

Passwords for user accounts must have at least twelve (12) non-blank characters.

Passwords must contain characters from at least three (3) of the following four (4) categories:

- English upper case letters: A, B, C.....Z
- English lower case letters: a, b, c.....z
- Westernized Arabic numerals: 0, 1, 2.....9
- Non-alphanumeric special characters (e.g., punctuation symbols such as ` ~ ! @)

Passwords must not contain common words, nouns, pronouns, acronyms, contractions, and geographic locations (i.e., dictionary words)

PIN type activation data used with subscriber hardware tokens and smart/PIV cards is required to meet the following criteria:

- At least 6 numbers.

Where passwords are used as activation data, the password data must be generated in conformance with OCIO-POL-21. Where USPTO CA uses passwords as activation data for the CA signing key, at a minimum the activation data must be changed upon CA re-key. If the activation data must be transmitted, it must be via an appropriately protected channel.

6.4.2 Activation Data Protection

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

- memorized
- biometric in nature, or

- recorded and secured at the level of assurance associated with the activation of the cryptographic module, and must not be stored with the cryptographic module.

If activation data is written down, it must be secured at the level of the data that the associated cryptographic module is used to protect, and must not be stored with the cryptographic module. In the case of the Certification Authority Hardware Security Model Administrator and Operator, see Section 6.2.4.1.

Activation data for private keys associated with certificates asserting individual identities must never be shared.

PKI Sponsors must ensure that activation data for private keys associated with certificates they sponsor is restricted to those in the organization authorized to use the private keys.

The activation data protection mechanism for Certification Authority equipment or applications include a facility to temporarily lock out further access attempts, after three failed login attempts.

6.4.3 Other Aspects of Activation Data

Procedures to change pass phrases or Personal Identification Numbers for the Hardware Security Modules can be found in the SafeNet LunaSA on-line Help documentation included on SafeNet LunaSA Client Software and Documentation Release CD.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The Certification Authority server instantiation was tightly controlled and audited as part of the key generation ceremony. The initial Certification Authority software loaded on the Certification Authority server was from original manufacturer distribution media. Updates are downloaded from the manufacturer web-site and are only available to authorized users. Procedures to protect the integrity of software loaded onto CA servers is detailed in section 6.6.1.

The Certification Authority server is built on a Windows operating system with the following security features enabled: identification and authentication for all users, discretionary access control, and security audit. The Windows operating system is designed and configured to provide self-protection and process isolation.

The Certification Authority server operates with the minimal number of local accounts required. No one will be able to perform remote login. The Certification Authority will only run the network services required to operate the Certification Authority. Other services may be started and used for maintenance and update purposes, but will be returned to the off or manual state when the maintenance or update action is completed.

The following general computer security functions are provided by the operating system, supporting applications or through a combination of these in conjunction with physical safeguards:

- authenticate the identity of users before permitting access to the system or applications;

- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see Section 5.4)
- enforce domain integrity boundaries for security critical processes;
- require use of cryptography for session communication and database security;
- require self-test security-related CA services;
- require a trusted path for identification of all users;
- provide residual information protection; and
- require recovery from key or system failure.

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

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

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

The Certification Authority equipment is hosted on evaluated platforms in support of computer security assurance requirements.

6.5.2 Computer Security Rating

Not applicable.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The Certification Authority server hardware is dedicated for use as the Certification Authority within the USPTO Public Key Infrastructure.

The Certification Authority software is dedicated to providing the Certification Authority functions. Only Operational Authority-approved software has been loaded on the Certification Authority servers.

The CA hardware has been installed in the CA facility in accordance with the physical security safeguards as defined in Section 5.1. These physical safeguards serve to restrict access to the CA hardware to a limited number of trusted individuals. These physical safeguards in combination with the network security controls defined in Section 6.7 restrict the ability for malicious software to be installed on the CA hardware.

The System Development Controls for the Certification Authority are as follows:

- The CA only uses well-known commercial off-the-shelf software.
- Hardware and software procured to operate the CA was purchased in a fashion to reduce the likelihood that any particular component was tampered with.
- All hardware was shipped or delivered via controlled methods that provided a continuous chain of accountability, from the purchase location to the CA physical location.
- The CA hardware and software must be dedicated to performing the one task of acting as the root of trust for the issuance and management of certificates. There must be no other applications, hardware devices, network connections, or component software installed that are not an integral part of the CA operation or the approved USPTO Operating System baseline.
- Proper care is taken to prevent malicious software from being loaded onto the CA equipment, only applications required to perform the operation of the CA are installed and these applications were obtained from sources authorized by local policy. Hashes of downloaded software are taken at the time of download and verified before software is loaded onto CA equipment to prevent unauthorized modification in the intervening time period. Registration Authority hardware and software must be scanned for malicious code on first use and periodically thereafter. USPTO Cybersecurity performs routine periodic vulnerability scans and sends the analysis reports to the system owners for evaluation and action. Refer to Section 5.4.8.
- Hardware and software updates must be purchased or developed in the same manner as original equipment, and must be installed by trusted and trained personnel following formal approval under the USPTO Change Management processes.

6.6.2 Security Management Controls

The installation and configuration of the Certification Authority software was performed under very strict, scripted guidelines as part of the key generation ceremony with each step being videotaped and audited by a Compliance Auditor.

The USPTO follows a formal software implementation methodology whereby all PKI software upgrades and/or modifications to production systems are first installed and evaluated in a test environment and evaluated by the Operational Authority.

At the completion of the evaluation period, the Operational Authority submits to the OAA a software or hardware modification change request indicating the specific hardware device, software title and version number to be modified. In addition, the report indicates the new hardware device, software title and version number, as well as a list of modifications or

enhancements that the new hardware or software provides. The OAA is responsible for reviewing and approving the production software or hardware modification request. If the OAA approves the request, it will be returned to the Operational Authority in the method of an approved change record. ***Note***: In the event where the OAA is unavailable, a member of the OIEO management chain may act on behalf of the OAA.

The configuration of the Certification Authority system, in addition to any modifications and upgrades, is documented and controlled. The Certification Authority software, when first loaded, was verified as being that supplied from the vendor, with no modifications, and was the version intended for use. USPTO Life Cycle Management includes regular periodic configuration management audits. The auditor must perform the configuration management audit on an annual basis.

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

6.6.3 Life-Cycle Security Ratings

Not applicable.

6.7 Network Security Controls

Remote access to the Certification Authority server is secured using the following security features:

- For Registration and Administration – the Entrust Administration Service Handler protocol is used.
- For Certificate Issuance Request purposes – Public Key Infrastructure X.509-Certificate Management Protocol is used.

The CA servers are placed behind boundary/perimeter network defenses and afforded protections consistent with commercial electronic commerce practices for network security.

Services allowed to and from the CA servers are limited to those required to perform their basic CA functions. Services such as XAP and SEP are enabled on the CA so that trusted PKI Operators are able to perform their duties. USPTO recognized Operating System baseline services are also permitted to support reasonable day-to-day operation of commercial electronic commerce computing systems (e.g. – DNS, NTP, One-way Domain Trust, LDAP).

CA equipment is protected against known network attacks. All unused network ports and services are turned off. Any network software present on the CA equipment is necessary to the functioning of the Certification Authority application.

USPTO boundary control devices used to protect the network on which PKI equipment is hosted deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network. In addition, all Registration Authority activities not performed directly within the Internal PKI network domain require the appropriate Trusted Role individual to complete an additional authentication to the boundary control devices.

USPTO does not allow remote workstation access to the CA equipment.

6.8 Time-Stamping

Times asserted by CA servers, Card Management System servers, or CA Domain servers are based on the underlying day/time service of their respective operating systems. USPTO uses NIST qualified Network Time Protocol servers to synchronize date/time information to USPTO production servers.

If a manual day/time update is required, such an action will be recorded in the server logs.

7 CERTIFICATE, CRL, AND PROFILES

7.1 Certificate Profile

Certificates issued by the USPTO Internal Certification Authority must conform to the Federal guidelines:

- Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile
- Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles

7.1.1 Version Numbers

The USPTO Internal Certification Authority must issue X.509 Version 3 certificates (populate version field with integer "2").

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles. These profiles are written to prescribe an appropriate amount of control over an infrastructure, yet be flexible enough to meet the needs of the various CAs and communities. The USPTO Internal Certification Authority must comply with RFC 5280 and the Federal guidelines noted in section 7.1. Private extensions must not be used.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CPS must using one of the following OIDs for signatures.

Table 7-1: OIDs Used for Signatures

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11} (1.2.840.113549.1.1.11)
sha384WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 } (1.2.840.113549.1.1.12)

Certificates issued under this CPS will use the following object identifiers for identifying the algorithm for which the subject key was generated.

Table 7-2: OIDs Identifying the Algorithm for which the Subject Key was generated

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

7.1.4 Name Forms

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

7.1.5 Name Constraints

Not applicable.

7.1.6 Certificate Policy Object Identifier

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

7.1.7 Usage of Policy Constraints Extension

The USPTO Internal Certification Authority must assert policy constraints in CA certificates as required.

7.1.8 Policy Qualifiers Syntax and Semantics

The USPTO Internal Certification Authority will not issue certificates containing policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Certificates issued under this CPS must not contain a critical certificate policies extension.

7.1.10 Inhibit Any Policy Extension

USPTO does not assert the *InhibitAnyPolicy* in CA certificates.

7.2 CRL Profile

CRLs issued by the USPTO Internal CA must conform to the CRL profile specified in [FPKI-PROF] CRL Extension Profiles.

7.2.1 Version Numbers

The USPTO Internal Certification Authority must issue X.509 Version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

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

7.3 OCSP Profile

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

- CSSs operated under this policy must use OCSP version 1.
- Critical OCSP extensions must not be used.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

All USPTO CAs are subject to an annual review by the FPKIPA to ensure 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 the CP must have a compliance audit mechanism in place to ensure that requirements of the CP and this CPS are being implemented and enforced.

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

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

The USPTO Operational Authority may also conduct its own, internal, periodic and aperiodic compliance audits. The Operational Authority must state the reason for any aperiodic compliance audit in its summary report.

The internal auditor or compliance auditor must have the right to review the periodic and aperiodic internal audits conducted by the Operational Authority.

The compliance audit mechanism will consist of the auditing capabilities of Internal PKI and its components to capture and store audit and event log, and the USPTO security guards and PKI staff to correctly capture and maintain paper access logs. This mechanism will also include the storage of the compliance audit logs data for long-term archiving as stated in this CPS.

8.1 Frequency or Circumstances of Assessment

CAs and RAs operating under this policy must be subject to an annual compliance audit in accordance with the *FPKI Annual Review Requirements document* [AUDIT]. The Policy Authority may also conduct its own audits and evaluations of the Internal CA and any Registration Authorities as part of its normal inspection and security evaluation programs in place at the USPTO.

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/Qualification of Assessor

Independent auditors must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the USPTO CP and this CPS. The compliance auditor must perform PKI or Information stem compliance audits as a primary responsibility. The Policy Authority designates to the Operational Authority in coordination with the Chief Information Officer Internal Auditor, the right to assess the skills, experience, and competency of the designated auditors and may deny an audit request or scheduled audit if there is a clear deficiency in the auditor’s qualifications.

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor may be any of the following:

- A private firm specializing in compliance audits
- A compliance auditor working under the direction of the Inspector General's Office of the Department of Commerce
- An auditor, internal to USPTO, but sufficiently independent of the responsibility for the successful operation and conformance of the Internal CA to the CP and this CPS

The compliance auditor may NOT execute any of the trusted roles identified in the USPTO CP or this CPS. The Policy Authority must approve any independent or external compliance auditors.

8.4 Topics Covered by Compliance Audit

The overall goal of the audit is to verify that the Certification Authority system complies with practices and procedures described in this CPS during operation and administration of the Internal CA function and associated components, and to verify the continued validity of the CP and its mapping to any cross-certified entities.

In addition, the compliance audit must verify that the USPTO Internal PKI is correctly implementing the provisions of any Memorandums of Agreement with cross-certified entities.

Within each compliance audit, the auditor verifies the continued compatibility between the CP and this CPS. The audit also verifies that, at a minimum, the operational and technical controls used by the Internal CA and associated components satisfy the following elements of this CPS and the CP:

Identification & Authentication:

- Initial registration
- Routine re-key
- Re-key after revocation
- Revocation request
- Key recovery

Operational Requirements:

- Certificate application
- Certificate issuance
- Certificate acceptance
- Certificate suspension/revocation
- Computer security audit procedures
- Records archival
- Certification authority key changeover
- Compromise and disaster recovery

Physical, Procedural & Personnel Security:

- Physical security controls
- Procedural controls
- Personnel security controls

Technical Security Controls:

- Key pair generation & installation
- Private Key protection
- Other aspects of key management
- Activation data
- Computer security controls
- Lifecycle technical controls
- Network security controls
- Cryptographic module engineering controls

Certificate & Certificate Revocation List Profiles:

- Certificate profile
- Certificate revocation list profile

Specification Administration:

- Specification change procedures
- Publication and notification procedures

All aspects of the Certification Authority system will be subject to a compliance audit on the schedule noted in section 8.1.

8.5 Actions Taken as a Result of Deficiency

The USPTO Compliance Auditor must notify the USPTO Operational Authority and the USPTO Policy Authority of the results of the compliance audit in the form of a report.

Upon notification, the USPTO Policy Authority and USPTO Operational Authority will review the compliance audit results and the recommendations to determine the action to be taken.

Based on the compliance audit findings of the USPTO, the possible courses of actions include:

- Continue to operate as usual, pending remedial action;
- Continue to operate but at a lower assurance level, pending remedial action; or
- Suspend operation (this alternative will execute the procedures described in Section 4.9 for revocation of certificates).

For any deficiencies identified in a compliance audit, the Policy Authority, with input from Operational Authority, will determine which action will be taken. If it is determined to be a "material discrepancy" relative to the applicable requirements, the Policy Authority must notify immediately all appropriate entities in accordance with applicable Memorandums of Agreement, Memorandums of Understanding, and/or other entities with which the USPTO has contract agreements. The party responsible for correcting the discrepancy must propose a remedy, including expected time for completion, to the Policy Authority.

All deficiencies identified by the auditor must be recorded in a compliance audit report. The Operational Authority will notify the Certification Authority system of the deficiencies and the corrective actions that will be taken. The results of the audit will be reported to the audited Certification Authority system.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the Policy Authority may decide to halt temporarily operations of the Internal CA or Registration Authority, to revoke a certificate issued to the Certification Authority (if applicable) or Registration Authority or take other actions it deems appropriate. The Policy Authority will balance the need for continuation of USPTO business supported by the Public Key Infrastructure against the risk posed by the discrepancy, the presence of a remediation plan and the impact of any action on the trust placed in the USPTO and its PKI supported activities.

If the Policy Authority takes the first or second action, the Operational Authority is responsible for ensuring implementation of corrective actions. Otherwise, the Operational Authority submits a request to the Policy Authority for a temporary waiver pending the capability to take corrective action. At that time or earlier if agreed by the Policy Authority, the audit team will reassess deficiency areas. If, upon reassessment, the Internal CA has not taken corrective actions or received a waiver, the Policy Authority will determine if more severe action (e.g., last action above) is required.

If the Policy Authority takes the last action, the Internal CA must revoke all certificates issued by the Certification Authority and Registration Authority, including cross-certification certificates, prior to suspension of the service. The Policy Authority will develop procedures for making and implementing such determination. The Operational Authority will conduct this revocation in accordance with Section 4.9 of this CPS. The Policy Authority and Operational Authority are responsible for reporting the status of corrective action to the auditors as necessary. The Policy Authority and the auditor together will determine when reassessment is to occur. Upon reassessment, if the Internal CA has corrected the deficiencies, the Internal CA will resume service and issue new certificates to subscribers and possibly external Certification Authorities, depending on conditions specified in individual cross-certification agreements.

8.6 Communication of Results

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

9 OTHER BUISNESS 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

Not applicable.

9.1.2 Certificate Access Fees

No fee will be charged for access to CA certificates.

9.1.3 Revocation or Status Information Access Fees

No fee will be charged for access to CRLs or OCSP status information.

9.1.4 Fees for other Services

Not applicable.

9.1.5 Refund Policy

Not applicable.

9.2 Financial Responsibility

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

Issuance of certificates in accordance with this CPS does not make a Certification Authority, or any Registration Authority, an agent, fiduciary, trustee, or other representative of subscribers or Relying Parties.

9.2.1 Insurance Coverage

Not applicable.

9.2.2 Other Assets

Not applicable.

9.2.3 Insurance or Warranty Coverage for End-Entities

Not applicable.

9.3 Confidentiality of Business Information

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

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

9.3.1 Scope of Confidential Information

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

- Information concerning the events leading up to and the investigation of a revocation, and
- Information protected by the Privacy Act of 1974.

9.3.2 Information not within the Scope of Confidential Information

Not applicable.

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The USPTO Internal CA will publish only CA certificates, cross-certificates, link-certificates, and CRLs in a publicly accessible directory repository. No Personally Identifying Information for subscribers will be publicly disclosed.

The Privacy Threshold Analysis (PTA) questionnaire is used to determine the necessity of a Privacy Impact Assessment (PIA). Since the ID-Auth systems collect, maintain, and disseminate PII for federal employees and contractors, the Operational Authority actively participates in the PIA process.

The Department of Commerce Privacy Program Plan is created to describe the mission and strategy for safeguarding personal privacy in accordance with the Privacy Act of 1974:

- Describes the privacy program structure
- Highlights resources dedicated to the privacy program
- Describes the roles of the privacy officials and staff
- Set goals and objectives of the privacy program
- Establishes program management controls to meet privacy requirements and manage privacy risks

9.4.2 Information Treated as Private

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

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

The Certification Authority will treat any information collected as part of registration, certification, or key recovery and not directly asserted in the certificate as sensitive. The Certification Authority must not disclose it to unauthorized parties. This includes escrowed keys and activation data. Audit logs associated with the operation of the Internal CA are sensitive and may only be disclosed to compliance auditors, the Policy Authority, and approved parties under a non-disclosure agreement or in compliance with Freedom of Information Act or legal discovery. The private signing key corresponding to a public key in a signing certificate held by the entity named in the certificate is sensitive information. All information that is not in the repository but is stored in the Certification Authority must be encrypted to preserve confidentiality and will be considered as sensitive. This information must be available to only to USPTO officials performing their duties.

Certificates issued by the Internal CA must only contain information that is relevant and necessary to effect secure transactions with the certificate. For the purpose of proper administration of the certificates, the Internal CA may request non-certificate information to be used in managing the certificates within the USPTO. Non-Certificate information that may be used in managing certificates in USPTO is:

- Employee badge numbers
- Office phone numbers
- Business addresses
- Employee room numbers

9.4.3 Information not Deemed Private

Information included in certificates is not subject to protections outlined in section 9.4.2.

9.4.4 Responsibility to Protect Private Information

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

All information collected as part of the identity proofing process must be protected to ensure confidentiality and integrity. In the event the Entity terminates PKI activities, it must be

responsible for disposing of or destroying sensitive information, including PII, in a secure manner, and maintaining its protection from unauthorized access until destruction.

9.4.5 Notice and Consent to Use Private Information

The USPTO PKI Operational Authority or USPTO PKI Operational Authority Officers are 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

A CA or RA will not disclose certificate or certificate-related information to any third party unless authorized by USPTO PKI CP, required by law, government rule or regulation, or order of a court of competent jurisdiction. Any third party request or court order for release of information must be immediately directed to the USPTO General Counsel. Any request for release of information must be processed according to 41 CFR 105-60.605.

9.4.7 Other Information Disclosure Circumstances

Not applicable.

9.5 Intellectual Property Rights

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

9.6 Representations and Warranties

The obligations described below pertain to all USPTO CAs, USPTO PKI Operational Authority and USPTO PKI Operational Authority Officers.

9.6.1 CA Representations and Warranties

USPTO CA certificates are issued and revoked at the sole discretion of the USPTO PKI Policy Authority.

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

The Certification Authority will 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;
- Conforming to the stipulations of this CPS;
- Ensuring that registration information is accepted only from Registration Authorities who understand and are obligated to comply with the USPTO PKI CP and this 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 and where appropriate, publishing information to that affect in the PKI repositories;
- Complying with the requirements set forth in applicable Memorandum of Agreement, Memorandum of Understanding, and contractual agreements with cross-certified CAs and/or other entities; and
- 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.

A CA that is found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 8.5.

9.6.2 RA Representations and Warranties

An RA who performs registration functions as described in the USPTO CP must comply with the stipulations of the USPTO PKI CP and comply with this CPS when approved by the Policy Authority. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities. An RA supporting this policy must conform to the stipulations of this document, including:

- Conforming to the general stipulations of the approved CPS
- Performing identity validation as specified in the approved CPS
- Approving certificate generation requests and ensuring that only valid and appropriate information is included in such request
- Maintaining evidence that due diligence was exercised in validating information used to specify information contained in issued certificates, whether such validation was performed by an RA
- Ensuring that obligations are imposed on subscribers in accordance with Section 9.6.3 and informing subscribers of the consequences of not complying with those obligations

9.6.3 Subscriber Representations and Warranties

A subscriber must sign a Subscriber agreement form containing the requirements, obligations, terms, conditions and restrictions the subscriber must meet before being issued the certificate.

Subscribers who sign the form agree to::

- Accurately represent themselves in all communications with the PKI authorities and other subscribers;
- Protect their private keys private keys at all times from loss, unauthorized disclosure, or suspicion of compromise;
- Maintain secure control of their PIV card and private keys at all times and will report the loss, or theft, compromise, or damage within 24 hours;

- Subscribers must provide accurate identification and authentication information during key recovery request. After their escrowed key(s) has been recovered, the Subscriber must determine whether revocation of the public key certificate associated with the recovered key is necessary. The Subscriber must request the revocation, if necessary.
- Use certificates provided by the USPTO PKI only for transactions related to USPTO business.

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

9.6.4 Relying Party Representations and Warranties

Parties who rely upon the certificates defined in this CPS that are issued by the USPTO Internal Certification Authority must:

- Perform a risk analysis to decide whether the level of assurance provided by the certificate is adequate to protect the Relying Party based upon the intended use;
- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- Check each certificate for validity, using procedures described in the X.509 standard [International Organization of Standardization 9594-8], prior to reliance;
- Establish trust in the CA that issued a certificate by verifying the certification path in accordance with the guidelines set by the X.509 Version 3 Amendment; and
- When necessary, preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data.[3]

9.6.5 Representations and Warranties of Other Participants

The USPTO may issue certificates to subscribers other than employees of the U.S. Government, such as contractor employees, commercial vendors, and agents, for the convenience of the Government and without fee, when those subscribers have a bona fide need to possess a certificate issued by the USPTO CA and such issuance is requested by an appropriate USPTO official such as a Contracting Officer or Task Manager or other appropriate USPTO official acting as PKI Sponsor. The CA or RA must inform such subscribers of the stipulations of this section by including the following provisions in the Subscriber Agreements. These subscribers are, at the minimum, under the same policy obligations as those specified for a USPTO employee. The Director, Office of Organizational Policy and Governance, in consultation with

[3] Data format changes associated with application upgrades and normal data migration may invalidate digital signatures. Therefore, for records requiring long term storage, a more appropriate and cost effective strategy includes validating the signature and creating a record of the successful validation of the original signed data which is itself preserved as a record. This approach is in accordance with National Archives and Records Administration Records Management Guidance for PKI-Unique Administrative Records.

the USPTO PKI Sponsor, may impose additional conditions and qualifications for such subscribers.

9.7 Disclaimers of Warranties

The CA may not disclaim any responsibilities described in this CPS.

9.8 Limitations of Liability

This CPS is not intended to and does not create any new right or benefit, substantive or procedural, enforceable at law by any party against the U.S. Government, its agencies or instrumentalities, its officers or employees, or any other person.

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

9.9 Indemnities

Not applicable.

9.10 Term and Termination

9.10.1 Term

This CPS becomes effective when approved by the USPTO PKI Policy Authority. This CPS has no specified term.

9.10.2 Termination

Termination of this CPS is at the discretion of the USPTO PKI Policy Authority.

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

Not applicable.

9.12 Amendments

9.12.1 Procedure for Amendment

This CPS is reviewed, approved and amended by personnel detailed in Section 1.5 of this document.

9.12.2 Notification Mechanism and Period

Proposed changes to this CPS must be distributed electronically to USPTO PKI Policy Authority members and observers.

9.12.3 Circumstances under Which OID Must Be Changed

OIDs published in certificates issued under this CPS 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

Any disputes with the operation of the USPTO Internal Certification Authority will be directed to the USPTO PKI Policy Authority. A dispute must at a minimum:

- Be in written form. This can include communication via electronic means, such as email.
- Detail the exact practice from this CPS that is in question or detail a practice that is not but should be included in this CPS.

The USPTO PKI Operational Authority will review the dispute and provide a written analysis to the USPTO Policy Authority of the dispute and an explanation of whether the Operational Authority agrees or not with the practice in dispute. If the Operational Authority agrees that the practice is incorrect or a particular practice is not included, the Operational Authority will suggest remediation and then follow the procedures detailed in the USPTO PKI Policy and this CPS for amending this CPS.

The USPTO PKI Policy Authority is the final authority to resolve disputes when the CPS procedures do not provide a resolution.

The parties must resolve any disputes arising with respect to this policy or certificates issued under this policy.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

The USPTO Certification Authority is required to comply with applicable law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Not applicable.

9.16.2 Assignment

Not applicable.

9.16.3 Severability

Should it be determined that one section of this CPS is incorrect or invalid, the other sections of this CPS must remain in effect until the CPS is updated. The process for updating this CPS is described in sections 1.5 and 9.12.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

Not applicable.

9.16.5 Force Majeure

Not applicable.

9.17 Other Provisions

Not applicable.

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	1.2	2022
FIPS 140-3	Security Requirements for Cryptographic Modules https://csrc.nist.gov/		03-22-2019
FIPS 186-4	*Digital Signature Standard* http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf		July 2013
FOIAACT	*5 U.S.C. 552, Freedom of Information Act* http://www4.law.cornell.edu/uscode/5/552.html		
FPKI Profiles	Federal Public Key Infrastructure X.509 Certificate and Certificate Revocation List Extensions Profile https://www.idmanagement.gov/topics/fpki/		May 10, 2018
CCP-PROF	Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles https://www.idmanagement.gov/topics/fpki/	2.1	2-1-2021
ISO9594-8	*Information Technology – Open Systems Interconnection – The Directory: Authentication Framework* ftp://ftp.bull.com/pub/OSIdirectotry/ITU/97x509final.doc		2014
ITMRA	*40 U.S.C. 1452, Information Technology Management Reform Act* http://www4.law.cornell.edu/uscode/40/1452.html		
NAG69C	*Information System Security Policy and Certification Practice Statement for Certification Authorities,*	Revision C	November 1999
NSD42	*National Policy for the Security of National Security Telecom and Information Systems* http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)		5 July 1990
RFC8017	*PKCS #1: RSA Cryptography Specifications Version*	2.2	November 2016

Number	Title	Revision	Date
RFC7292	*PKCS #12: Personal Information Exchange Syntax*	1.1	July 2014
RFC4210	*Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)* https://tools.ietf.org/html/rfc4210		September 2005
RFC3647	*Certificate Policy and Certification Practices Framework,* Chokhani and Ford http://www.ietf.org/rfc/rfc3647.txt		November 2003
SP 800-157	*Guidelines for Derived Personal Identity Verification (PIV) Credentials* http://dx.doi.org/10.6028/NIST.SP.800-157		December 2014
SP 800-63-3	Digital Identity Guidelines	3	02 March 2020
RFC5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile		May 2008
SP 800-79-2	Guidelines for the Authorization of PIV Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)		July 2015
PTOI-007-00	DOC USPTO Privacy Impact Assessment for ID-Auth		FY22
EIPL-DS-09-00	DOC USPTO Privacy Threshold Analysis for ID-Auth		FY22
	DOC Privacy Program Plan		Sept 2021
USPTO	HSPD-12 PIV Card Issuers Operations Plan		

11 ACRONYMS AND ABBREVIATIONS

CA	Certification Authority
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Objects Registry
CSS	Certificate Status Service
DN	Distinguished Name
ECDSA	Elliptic Curve Digital Signature Algorithm
FBCA	Federal Bridge Certification Authority
FIPS PUB	(US) Federal Information Processing Standards Publication
FPKI	Federal Public Key Infrastructure
FPKI OA	Federal Public Key Infrastructure Operational Authority
FPKIA	Federal PKI Architecture
FPKIPA	Federal PKI Policy Authority
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
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
S&A	Security Assessment and Authorization
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 (IS) resource. [NS4009]
access control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
accreditation	Formal declaration by a Designated Approving Authority that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
applicant	The Subscriber is sometimes also called an "applicant" after applying to a Certification Authority for a certificate, but before the certificate issuance procedure is completed.
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	An authority trusted by one or more users to create and assign certificates. [ISO9594-8]
Certification Authority facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.

Term	Definition
certificate	A digital representation of information which at least (1) identifies the Certification Authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the Certification Authority issuing it. [ABADSG]
certificate-related information	Information, such as a Subscriber's postal address, that is not included in a certificate, but that may be used by a Certification Authority 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]
Cross-certification	The process undertaken by Certification Authorities to establish a relationship of trust.
cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS 140]
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 DNs 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	Framework established to issue, maintain, and revoke public key certificates.
Registration Authority	Entity responsible for Identification and Authentication of certificate subjects that have automated equipment for the communication of applicant data to Certification Authority and does not sign or directly revoke certificates.

Term	Definition
Root Certification Authority	In a hierarchical Public Key Infrastructure, the Certification Authority 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]. Current subscribers possess valid ECA-issued certificates.
Superior Certification Authority	In a hierarchical Public Key Infrastructure, a Certification Authority who has certified the certificate signing key of another Certification Authority, and who constrains the activities of that Certification Authority. (See subordinate Certification Authority)
Supervised Remote Identity Proofing	A real-time identity proofing event where the RA or Trusted Agent is not in the same physical location as the applicant/subscriber. The RA or 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.

Term	Definition
system equipment configuration	A comprehensive accounting of all system hardware and software types and settings.
technical non-repudiation	The contribution public key mechanisms make to the provision of technical evidence supporting a non-repudiation security service.
threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
trust list	Collection of Trusted Certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	A Trusted Agent is authorized by a CA to act on its behalf and may record information from and verify biometrics (e.g., photographs) on presented credentials on behalf of an RA for Applicants who cannot appear in person. Trusted Agents are not Trusted Roles. Note: At the time of publication, USPTO does not use Trusted Agents in the Identify Proofing process.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure, authenticated delivery. The public keys included in Trusted Certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
two person control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. [NS4009]
update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Virtual Machine Environment	An emulation of a computer system (in this case, a CA) that provides the functionality of a physical machine in a platform-independent environment. They provide functionality needed to execute entire operating systems.
zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS 140]