



UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

**OCIO IT SECURITY – PUBLIC KEY INFRASTRUCTURE (PKI) CERTIFICATE
POLICY
OCIO-6004-09**

Date of Issuance: May 27, 2009

Effective Date: May 27, 2009

Review Date:

TABLE OF CONTENTS

Section

- I. REVISION HISTORY
- II. POLICY TABLE OF CONTENTS
- II. PURPOSE
- III. AUTHORITY
- IV. SCOPE
- V. DEFINITIONS
- VI. POLICY
- VII. RESPONSIBILITIES
- VIII. EFFECT ON OTHER POLICIES

I. REVISION HISTORY

Version	Date	Editor	Change Description
1.1-1.3	8/20/04	Darryl Clemons	Version 1.3 was the first signed version.
1.4	12/8/04	Amit Jain	Modified sections 1.4.2, 2.7.1, 3.1.4, 3.2.1, 4.2.1, 4.4.4, 4.5.1, 4.5.5, 4.6.5, 5.3.1, 6.1.5, and 6.4.1 to incorporate necessary modifications identified by FBCA/CPWG.
1.4	12/14/04	Greg McCain	Changed column title from ‘Author’ to ‘Editor’ in the Revision History table.
1.5	03/27/07	Greg McCain	Updated to reflect USPTO organizational changes related to management or operational responsibilities for: <ul style="list-style-type: none"> • Security Policy • Security Operations • User Account Creation and Maintenance
2.0	10/23/07	John Michie	Updated to reflect the new RFC 3647 format
2.1	5/26/09	Steven Bjarnason (Facilitation Services Contract)	Revised to reflect new OCIO policy document template format.

II. POLICY TABLE OF CONTENTS

1	INTRODUCTION.....	11
1.1	Overview	12
1.1.1	Certificate Policy	12
1.1.2	Relationship between the CP and the CPS	12
1.1.3	Scope	13
1.1.4	Interoperation with CAs Issuing under Different Policies	13
1.2	Document Name and Identification	13
1.3	PKI Participants.....	14
1.3.1	PKI Authorities.....	14
1.3.2	Registration Authorities (RA)	16
1.3.3	Local Registration Authority (LRA)	17
1.3.4	Subscribers.....	17
1.3.5	Relying Parties.....	17
1.3.6	Other Participants	18
1.4	Certificate Usage.....	18
1.4.1	Appropriate Certificate Uses	19
1.4.2	Prohibited Certificate Uses.....	20
1.5	Policy Administration	20
1.5.1	Specification Administration Organization.....	20
1.5.2	Contact Person.....	20
1.5.3	Person Determining CPS Suitability for the Policy	21
1.5.4	CPS Approval Procedures	21
1.6	Definitions and Acronyms	21
2	PUBLICATION AND REPOSITORY RESPONSIBILITIES.....	21
2.1	Repositories.....	21
2.2	Publication of Certification Information.....	22
2.2.1	Publication of Certificates and Certificate Status.....	22
2.2.2	Publication of CA Information	22
2.2.3	Interoperability	22
2.3	Time or Frequency of Publication.....	22
2.4	Access Controls on Repositories.....	23
3	IDENTIFICATION AND AUTHENTICATION	23
3.1	Naming.....	23
3.1.1	Types of Names	23
3.1.2	Need for Names to be Meaningful	25
3.1.3	Anonymity or Pseudonymity of Subscribers.....	25
3.1.4	Rules for Interpreting Various Name Forms	26
3.1.5	Uniqueness of Names	26
3.1.6	Recognition, Authentication, and Role of Trademarks	26

3.2	Initial Identity Validation	26
3.2.1	Method to Prove Possession of Private Key.....	26
3.2.2	Authentication of Organization Identity.....	27
3.2.3	Authentication of Individual Identity	27
3.2.4	Non-verified Subscriber Information	29
3.2.5	Validation of Authority	29
3.2.6	Criteria for Interoperation.....	30
3.3	Identification and Authentication for Re-key Requests	30
3.3.1	Identification and Authentication for Routine Re-key	30
3.3.2	Identification and Authentication for Re-key after Revocation	30
3.4	Identification and Authentication for Revocation Requests	30
4	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	32
4.1	Certificate Application	32
4.1.1	Who Can Submit a Certificate Application.....	32
4.1.2	Enrollment Process and Responsibilities.....	32
4.2	Certificate Application Processing.....	33
4.2.1	Performing Identification and Authentication Functions	33
4.2.2	Approval or Rejection of Certificate Applications.....	33
4.2.3	Time to Process Certificate Applications	33
4.3	Certificate Issuance	33
4.3.1	CA Actions during Certificate Issuance	33
4.3.2	Notification to Subscriber by the CA of Issuance of Certificate.....	34
4.4	Certificate Acceptance	34
4.4.1	Conduct Constituting Certificate Acceptance	34
4.4.2	Publication of the Certificate by the CA	34
4.4.3	Notification of Certificate Issuance by the CA to Other Entities	34
4.5	Key Pair and Certificate Usage	35
4.5.1	Subscriber Private Key and Certificate Usage	35
4.5.2	Relying Party Public Key and Certificate Usage.....	35
4.6	Certificate Renewal	35
4.6.1	Circumstance for Certificate Renewal.....	35
4.6.2	Who May Request Renewal	35
4.6.3	Processing Certificate Renewal Requests.....	36
4.6.4	Notification of New Certificate Issuance to Subscriber	36
4.6.5	Conduct Constituting Acceptance of a Renewal Certificate	36
4.6.6	Publication of the Renewal Certificate by the CA	36
4.6.7	Notification of Certificate Issuance by the CA to Other Entities	36
4.7	Certificate Re-key	36
4.7.1	Circumstance for Certificate Re-key	37
4.7.2	Who May Request Certification of a New Public Key	37
4.7.3	Processing Certificate Re-keying Requests.....	38
4.7.4	Notification of New Certificate Issuance to Subscriber	38
4.7.5	Conduct Constituting Acceptance of a Re-keyed Certificate	38
4.7.6	Publication of the Re-keyed Certificate by the CA	38
4.7.7	Notification of Certificate Issuance by the CA to Other Entities	38

4.8	Certificate Modification	38
4.8.1	Circumstance for Certificate Modification.....	38
4.8.2	Who May Request Certificate Modification	38
4.8.3	Processing Certificate Modification Requests.....	39
4.8.4	Notification of New Certificate Issuance to Subscriber	39
4.8.5	Conduct Constituting Acceptance of Modified Certificate	39
4.8.6	Publication of the Modified Certificate by the CA.....	39
4.8.7	Notification of Certificate Issuance by the CA to Other Entities	39
4.9	Certificate Revocation and Suspension.....	39
4.9.1	Circumstances for Revocation.....	40
4.9.2	Who can Request a Revocation	40
4.9.3	Procedure for Revocation Request	40
4.9.4	Revocation Grace Period	42
4.9.5	Time within which CA must Process the Revocation Request	42
4.9.6	Revocation Checking Requirements for Relying Parties	42
4.9.7	CRL/CARL Issuance Frequency	42
4.9.8	Maximum Latency for CRLs.....	43
4.9.9	Online Revocation / Status Checking Availability.....	43
4.9.10	Online Revocation Checking Requirements.....	43
4.9.11	Other Forms of Revocation Advertisements Available.....	43
4.9.12	Special Requirements Related to Key Compromise.....	44
4.9.13	Circumstances for Suspension.....	44
4.9.14	Who Can Request Suspension.....	44
4.9.15	Procedure for Suspension Request	44
4.9.16	Limits on Suspension Period	44
4.10	Certificate Status Services.....	44
4.10.1	Operational Characteristics.....	44
4.10.2	Service Availability	44
4.10.3	Optional Features.....	44
4.11	End of Subscription.....	45
4.12	Key Escrow and Recovery	45
4.12.1	Key Escrow and Recovery Policy and Practices	45
4.12.2	Session Key Encapsulation and Recovery Policy and Practices	45
5	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.....	46
5.1	Physical Controls.....	46
5.1.1	Site Location and Construction	46
5.1.2	Physical Access	46
5.1.3	Power and Air Conditioning.....	47
5.1.4	Water Exposures.....	48
5.1.5	Fire Prevention and Protection	48
5.1.6	Media Storage.....	48
5.1.7	Waste Disposal	48
5.1.8	Off-site Backup.....	48
5.2	Procedural Controls.....	48
5.2.1	Trusted Roles.....	48

OCIO IT SECURITY – PKI CERTIFICATE POLICY

- 5.2.2 Number of Persons Required per Task..... 50
- 5.2.3 Identification and Authentication for Each Role..... 51
 - Roles Requiring..... 51
- 5.2.4 Separation of Duties 51
- 5.2.5 Identification and Authentication for Each Role..... 51
- 5.3 Personnel Controls 51
 - 5.3.1 Qualifications, Experience, and Clearance Requirements..... 51
 - 5.3.2 Background Check Procedures..... 51
 - 5.3.3 Training Requirements 52
 - 5.3.4 Retraining Frequency and Requirements 52
 - 5.3.5 Job Rotation Frequency and Sequence..... 52
 - 5.3.6 Sanctions for Unauthorized Actions..... 52
 - 5.3.7 Contracting Personnel Requirements 53
 - 5.3.8 Documentation Supplied to Personnel 53
- 5.4 Audit Logging Procedures 53
 - 5.4.1 Types of Events Recorded..... 53
 - 5.4.2 Frequency of Processing Data..... 58
 - 5.4.3 Retention Period for Security Audit Data..... 58
 - 5.4.4 Protection of Security Audit Data 59
 - 5.4.5 Security Audit Data Backup Procedures 59
 - 5.4.6 Security Audit Collection System (Internal vs. External)..... 59
 - 5.4.7 Notification to Event-Causing Subject..... 59
 - 5.4.8 Vulnerability Assessments 60
- 5.5 Records Archival..... 60
 - 5.5.1 Types of Events Archived 60
 - 5.5.2 Retention Period for Archive..... 61
 - 5.5.3 Protection of Archive..... 61
 - 5.5.4 Archive Backup Procedures 61
 - 5.5.5 Requirements for Time Stamping of Records 62
 - 5.5.6 Archive Collection System (Internal vs. External)..... 62
 - 5.5.7 Procedures to Obtain Archive Information 62
- 5.6 Key Changeover..... 62
- 5.7 Compromise and Disaster Recovery 62
 - 5.7.1 Incident and Compromise Handling Procedures..... 62
 - 5.7.2 Computing Resources, Software, and/or Data are Corrupted 63
 - 5.7.3 Certification Authority signature Keys are Compromised..... 63
 - 5.7.4 Business Continuity Capabilities after a Disaster..... 64
 - 5.7.5 Notification Related to Compromise or Disaster 64
 - 5.7.6 Certification Authority Cannot Generate Certificate Revocation 64
- 5.8 CA or RA Termination..... 65
- 6 TECHNICAL SECURITY CONTROLS..... 66**
 - 6.1 Key Pair Generation and Installation 66
 - 6.1.1 Key Pair Generation 66
 - 6.1.2 Private Key Delivery to Subscriber..... 66
 - 6.1.3 Public Key Delivery to Certificate Issuer..... 68

6.1.4	Certification Authority Public Key Delivery to Relying Powers	68
6.1.5	Key Sizes and Signature Algorithms	69
6.1.6	Public Key Parameters Generation	70
6.1.7	Key Usage Purposes (as per X.509 V3 Key Usage Field)	70
6.2	Private Key Protection and Cryptographic Module Engineering Controls	71
6.2.1	Cryptographic Module Standards and Controls	71
6.2.2	Private Key (n out of m) Multi-Person Control	72
6.2.3	Private Key Escrow	72
6.2.4	Private Key Backup	72
6.2.5	Private Key Archival	73
6.2.6	Private Key Transfer into or from a Cryptographic Module	73
6.2.7	Private Key Storage on Cryptographic Module	73
6.2.8	Method of Activating Private Keys	73
6.2.9	Method of Deactivating Private Key	74
6.2.10	Method of Destroying Private Key	74
6.2.11	Cryptographic Module Rating	74
6.3	Other Aspects of Key Pair Management	74
6.3.1	Public Key Archival	74
6.3.2	Certificate Operational Periods and Key Usage Periods	74
6.4	Activation Data	75
6.4.1	Activation Data Generation and Installation	75
6.4.2	Activation Data Protection	75
6.4.3	Other Aspects of Activation Data	76
6.5	Computer Security Controls	76
6.5.1	Specific Computer Security Technical Requirements	76
6.5.2	Computer Security Rating	77
6.6	Life Cycle Technical Controls	77
6.6.1	System Development Controls	77
6.6.2	Security Management Controls	77
6.6.3	Life-Cycle Security Ratings	78
6.7	Network Security Controls	78
6.8	Time Stamping	78
7	CERTIFICATE, CRL, AND PROFILES	79
7.1	Certificate Profile	79
7.1.1	Version Numbers	79
7.1.2	Certificate Extensions	79
7.1.3	Algorithm Object Identifiers	79
7.1.4	Name Forms	81
7.1.5	Name Constraints	81
7.1.6	Certificate Policy Object Identifier	81
7.1.7	Usage of Policy Constraints Extension	81
7.1.8	Policy Qualifiers Syntax and Semantics	81
7.1.9	Processing Semantics for the Critical Certificate Policy Extension	82
7.2	CRL Profile	82
7.2.1	Version Numbers	82

7.2.2	CRL and CRL Entry Extensions	82
7.3	OCSP Profile	82
7.3.1	Version Number(s)	82
7.3.2	OCSP Extensions.....	82
8	COMPLIANCE AUDIT AND OTHER ASSESSMENT	83
8.1	Frequency or Circumstances of Assessment.....	83
8.2	Identity/Qualifications of Compliance Auditor.....	83
8.3	Compliance Auditor’s Relationship to Assessed Entity	84
8.4	Topics Covered by Compliance Audit	84
8.5	Actions Taken as a Result of Deficiency	84
8.6	Communication of Results	85
9	OTHER BUSINESS AND LEGAL MATTERS	86
9.1	Fees.....	86
9.1.1	Certificate Issuance or Renewal Fees.....	86
9.1.2	Certificate Access Fees.....	86
9.1.3	Revocation or Status Information Access Fees	86
9.1.4	Fees for other Services	86
9.1.5	Refund Policy	86
9.2	Financial Responsibility	86
9.2.1	Insurance Coverage	86
9.2.2	Other Assets.....	86
9.2.3	Insurance or Warranty Coverage for End-Entities	87
9.3	Confidentiality of Business Information	87
9.3.1	Scope of Confidential Information	87
9.3.2	Information not within the Scope of Confidential Information.....	87
9.3.3	Responsibility to Protect Confidential Information.....	87
9.4	Privacy of Personal Information	87
9.4.1	Privacy Plan.....	87
9.4.2	Information Treated as Private	87
9.4.3	Information not Deemed Private	88
9.4.4	Responsibility to Protect Private Information	88
9.4.5	Notice and Consent to Use Private Information.....	88
9.4.6	Disclosure Pursuant to Judicial or Administrative Process	88
9.4.7	Other Information Disclosure Circumstances	88
9.5	Intellectual Property Rights.....	88
9.6	Representations and Warranties	88
9.6.1	CA Representations and Warranties.....	88
9.6.2	RA Representations and Warranties.....	89
9.6.3	LRA Representations and Warranties	90
9.6.4	Subscriber Representations and Warranties	90
9.6.5	Relying Party Representations and Warranties	90
9.6.6	Representations and Warranties of Other Participants	91
9.7	Disclaimers of Warranties	91
9.8	Limitations of Liability	91

OCIO IT SECURITY – PKI CERTIFICATE POLICY

9.9	Indemnities	92
9.10	Term and Termination.....	92
9.10.1	Term.....	92
9.10.2	Termination	92
9.10.3	Effect of Termination and Survival.....	92
9.11	Individual Notices and Communications with Participants	92
9.12	Amendments.....	92
9.12.1	Procedure for Amendment.....	92
9.12.2	Notification Mechanism and Period.....	92
9.12.3	Circumstances under Which OID Must Be Changed.....	92
9.13	Dispute Resolutions Provisions.....	93
9.14	Governing Law.....	93
9.15	Compliance with Applicable Law	93
9.16	Miscellaneous Provisions.....	93
9.16.1	Entire Agreement.....	93
9.16.2	Assignment	93
9.16.3	Severability	93
9.16.4	Enforcement (Attorneys’ Fees and Waiver of Rights).....	93
9.16.5	Force Majeure.....	93
9.17	Other Provisions.....	93
10	BIBLIOGRAPHY	95
11	ACRONYMS AND ABBREVIATIONS.....	98
12	GLOSSARY.....	100

LIST OF TABLES

Table 1-1: Certificate Levels of Assurance	19
Table 3-1: Assurance Level Naming Requirements	23
Table 4-1: Re-keying Identity Requirements.....	36
Table 4-2: CRL Issuance Requirements for Certification Authorities	43
Table 6-1: Minimum Requirements for Cryptographic Modules	71

III. AUTHORITY

This policy is issued pursuant to:

- The Federal Information Security Management Act of 2002 (FISMA)
- USPTO IT Security Policy Management Policy

IV. SCOPE

The provisions of this policy apply to all USPTO employees and contractor employees managing the implementation and operations of Public Key Infrastructure (PKI) electronic certificates at the United States Patent and Trademark Office (USPTO).

V. DEFINITIONS

See sections 11 and 12.

VI. POLICY

1 INTRODUCTION

This Certificate Policy (CP) governs the operation of the Public Key Infrastructure (PKI) by the United States Patent and Trademark Office (USPTO) consisting of products and services that provide and manage X.509 certificates for public-key cryptography. Certificates identify the entity or organization named in the certificate, and bind that entity or organization to a particular public/private key pair. This CP addresses the requirements for the USPTO at four assurance levels, basic, medium, medium hardware, and card authentication. The word “assurance” used in this CP means how well a Relying Party can be certain of the identity binding between the public key and the entity whose subject name is cited in the certificate. It also reflects how well the Relying Party can be certain that the entity whose subject name is cited in the certificate is controlling the use of the private key that corresponds to the public key in the certificate, and how securely the system, which was used to produce the certificate and (if appropriate) deliver the private key to the subscriber, performs its task. The USPTO PKI provides certificates for USPTO personnel and their business-related entities.

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

- Key generation, storage, and recovery;
- Certificate generation, update, renewal, re-key, and distribution;
- Certificate Revocation List (CRL) generation and distribution;

- Directory management of certificate related items;
- Certificate token initialization, programming, and management;
- System management functions (e.g., security audit, configuration management, and archive, etc.).

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

1.1 Overview

1.1.1 Certificate Policy

The USPTO CP is the policy under which the USPTO establishes and operates a Certification Authority (CA). This CP defines four distinct assurance levels for use by USPTO CAs, namely basic, medium, medium hardware, and card authentication. The CA that asserts medium assurance issues certificates to USPTO employees and contractor personnel. Certificates issued by USPTO CAs to external entities such as patent attorneys may be issued at either the basic or medium assurance level depending on the intended usage of the certificate.

Certificates issued under this policy contain a registered certificate policy object identifier (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The OID corresponds to a specific level of assurance, associated with a specific CP, which shall be available to relying parties. Each certificate issued by a USPTO CA will assert the specific USPTO policy that the certificate is issued under by inserting the corresponding USPTO policy OID in the *certificatePolicies* extension on the certificate.

Where the USPTO policy under which a certificate is issued meets or exceeds the requirements of other lower assurance level USPTO policies, those lower assurance level USPTO policy OIDs may also be asserted by listing them in the *certificatePolicies* extension on the certificate. The CPS for each USPTO CA shall distinguish between each USPTO policy under which it can issue a certificate, and the lower level of assurance USPTO policy or policies that will also be asserted in the *certificatePolicies* extension on the certificate.

This CP applies only to CAs owned and operated by the USPTO.

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

1.1.2 Relationship between the CP and the CPS

This CP states what level of assurance can be placed in a certificate issued by a USPTO CA. A Certification Practice Statement (CPS) specifies how that CA establishes that assurance level. USPTO will issue a formal CPS for each CA that issues certificates under this CP.

1.1.3 Scope

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

1.1.4 Interoperation with CAs Issuing under Different Policies

Interoperation with CAs that issue under different policies will be achieved through policy mapping and cross-certification through the FBCA.

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

1.2 Document Name and Identification

There are four levels of assurance in this policy, basic and medium, which are defined in subsequent sections of this CP. Each level of assurance has an object identifier (OID), to be asserted in certificates issued by USPTO CAs who comply with the policy stipulations herein. The FBCA that is cross certified with the USPTO Root CA may assert these OIDs in policy Mappings extensions of certificates issued to the USPTO CA, as appropriate. The OIDs are registered under Computer Security Objects Registry (CSOR) maintained by the National Institute of Standards and Technology.

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)}

csor-certpolicy OBJECT IDENTIFIER	::= {2 16 840 1 101 3 2 1}
pto-policies	::= {csor-certpolicy 2}
id-pto-basic-2003	::= pto-policies 7
id-pto-medium-2003	::= pto-policies 8
id-pto-mediumHardware	::= pto-policies <i>n</i>
id-pto-cardAuth	::= pto-policies <i>n</i>

The requirements associated with the medium hardware policy (id-pto-mediumHardware) are identical to those defined for the medium assurance policy (id-pto-medium-2003), with the exception of Subscriber cryptographic module requirements identified in Section 6.2.1.

The card authentication policy (id-pto-cardAuth) is asserted in certificates issued to Personal Identity Verification (PIV) Cards, as defined in Federal Information Processing Standard (FIPS) 201, supporting card authentication where the private key can be used without cardholder

activation of the card with their PIN. The requirements associated with the Card Authentication policy are the same as those defined for the Medium Hardware policy, with the exception that the private key can be used without activation of the card by the Cardholder. Since the private key can be used without Cardholder activation, no assurance can be associated with this policy.

Unless specifically approved by the Federal Public Key Infrastructure Policy Authority (FPKIPA), USPTO shall not assert the FBCA CP object identifiers in any certificates issued by USPTO, except in the *policyMappings* extension establishing an equivalency between a FBCA object identifier and an object identifier in the USPTO CP.

1.3 PKI Participants

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

1.3.1 PKI Authorities

1.3.1.1 USPTO PKI Approval Authority

This CP is established under the authority of and with the approval of the Chief Information Officer of the USPTO.

1.3.1.2 USPTO PKI Policy Authority

The USPTO PKI Policy Authority is a committee established by and responsible to USPTO Chief Information Officer. The Policy Authority is responsible for:

- Overseeing the creation and update of this CP and plans for implementing any accepted changes;
- Approving Certification Practice Statements of all CAs that provide services meeting the stipulations of this CP;
- Reviewing the results of CA compliance audits to determine if the CA is adequately meeting the stipulations of this CP and its associated approved CPS;
- Directing corrective actions, or other measures that might be appropriate, such as revocation of CA certificates or changes to this CP;
- Receiving requests for modifications to USPTO CP or Certification Practice Statements and recommending adoption, rework or rejections of such requests to the USPTO Chief Information Officer; and
- Receive requests for cross-certification from other entities and recommending adoption, rework or rejections of such requests to the Chief Information Officer of the USPTO.

1.3.1.3 USPTO PKI Operational Authority

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

The Operational Authority for the operation of the USPTO PKI shall determine administrative processes pertaining to this CP as detailed in the CPS.

1.3.1.4 USPTO PKI Operational Authority Administrator

The USPTO PKI Operational Authority Administrator is the Director of Network and Telecommunications Services Group (NTSG). This individual has primary responsibility for overseeing the proper operation of the CA including the repository, and who appoints individuals to the role of Operational Authority Officer.

1.3.1.5 USPTO PKI Operational Authority Officers

The Operational Authority Officers are individuals within the Operational Authority, who are selected by the Operational Authority Administrator, to operate the CA and its repository. These personnel will be employees and trusted contractors who work in or for the Information Technology Security Management Group or the Network Engineering Division under NTSG. The responsibilities of these officers include the following:

- Initial installation and configuration of CA components;
- Review and approval of any modifications to the operating baselines of the CA or Directory Repositories;
- Starting and stopping CA components;
- Periodic review of CA audit logs;
- Coordinating, participating in, reviewing and responding to needed changes identified in compliance audits;
- Coordinating and conducting training;
- Review and maintenance of training records; and
- Overall management of the USPTO PKI activities related to the USPTO SDLC process.

An Operational Authority Officer, as described in Section 5.2.1.3, shall perform the Auditor role.

1.3.1.6 Certification Authority

The Certification Authority¹ is the collection of hardware, software, and operating personnel that create, sign, and issue public key certificates to subscribers. The CA is responsible for the issuance and management of certificates, including the:

- Certificate manufacturing process,
- Publication of certificates,
- Revocation of certificates, and
- Re-key of USPTO PKI CA signing material.

The CA ensures that all aspects of the CA services, operations, and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.7 Certificate Status Servers

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

1.3.2 Registration Authorities (RA)

An RA is an entity that collects and verifies each subscriber's identity and information that is to be entered into the subscriber's public key certificates, and authorizes the CA to issue certificates to verified subscribers. The RA must perform its functions in accordance with a CPS approved by the Policy Authority. Registration Authorities shall either personally verify subscriber identity information or shall verify that a Local Registration Authority (LRA) has performed the identity verification. Registration Authorities shall be the only entities that approve certificate generation requests. The RA is responsible for:

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

¹ The term 'Certification Authority' has been used to refer to a computer server system that executes software that performs the certificate signing and generation (manufacturing) process. The term 'Certification Authority' is used in this CP to include the broader responsibilities noted in this section.

1.3.3 Local Registration Authority (LRA)

The USPTO PKI organization may choose to use the services of LRAs to assist Registration Authorities in performing identity verification tasks. LRAs do not have privileged access to CA functions, but are considered agents of the RA in verifying a subscriber's identity.

The Division Manager of the Network Engineering Division will specify, authorize and maintain records of which individuals or other identified trusted entities may act as LRAs and what the scope of any particular LRAs may include. Some examples of LRAs may include:

- Designated USPTO employees;
- Licensed Notary Publics and equivalent officials outside the U.S., whose function is the verification of documents establishing identity;
- Security Officers from other governmental organizations; and
- Responsible parties from business affiliates of USPTO.

The criteria and process for qualifying, training, and recognizing LRAs will be detailed in the Certification Practice Statement.

1.3.4 Subscribers

A subscriber is the entity whose name appears as the subject in a certificate, who asserts that they use the assigned key and certificate in accordance with the CP asserted in the certificate. In the context of this CP, a CA is not considered a subscriber. Subscribers to the USPTO PKI include but are not limited to USPTO employees, USPTO contractor employees, and other personnel requiring authenticated access to USPTO sensitive information or services for which PKI authentication is needed, including foreign governments and foreign organization personnel who are part of the intellectual property community, and their contractors and agents.

Subscribers may also include PKI sponsors who receive certificates for devices and other infrastructure components that require certificates in support of USPTO operations. Subscriber obligations for devices and infrastructure components are the responsibility of the PKI sponsors, who request and accept these certificates and who are responsible for the correct protection and use of associated private keys.

1.3.5 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) to determine the suitability of the certificate for a particular use.

1.3.5.1 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 CP.

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. External relying parties will be identified in the CPS or other official document. No other relying parties are authorized under this CP.

1.3.5.2 Non-USPTO Relying Parties

Non-USPTO relying parties should make the decision whether to rely on a certificate issued under this CP by considering all the facts and circumstances of the transaction including the value of the information, the threat environment, and the existing protection of the information environment, as well as the functionality of the Relying Party's application in validating the certificate, and the integrity of the authenticated or secured payload or transaction. The USPTO does not control this determination. Nonetheless, this CP contains some helpful guidance, set forth below, which Relying parties may consider in making their decisions.

Further, Relying parties may desire to review more detailed guidance governing the use of electronic signatures (which include the use of digital certificates) issued by the Office of Management and Budget implementing the Government Paperwork Elimination Act (Federal Register May 2000: Volume 65, Number 85, Page 25508), as well as more detailed subordinate guidance issued by other agencies pursuant to Office of Management and Budget direction (such as National Institute of Standards and Technology Special Publication 800-25 covering the technical elements of using digital signatures), and electronic record retention guidance such as that provided by the National Archives and Records Administration at www.nara.gov/records/policy/gpea and www.cio.gov/docs/NARA_gpea.

Certificates issued by USPTO to external subscribers are intended to be relied upon only by USPTO applications.

1.3.6 Other Participants

CAs and RAs operating under this policy will require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The CPS for the USPTO CA operated under authority of this CP shall identify the services, the parties responsible for providing such services, and the mechanisms used to support these services.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates granted under this CP are for carrying out the business of the USPTO by providing authentication and security services for use in transactions within the USPTO, with USPTO external customers, international partners, particularly the Trilateral Offices (the European Patent Office and the Japan Patent Office) and World Intellectual Property Organization and in internal USPTO systems and transactions.

For USPTO employees, PKI certificates and associated private keys will 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 will be used to authenticate access to sensitive patent and trademark information, which is the intellectual property of USPTO applicants. This information may include electronic examination records of other intellectual property offices and organizations, which may be of great sensitivity. PKI based authentication will 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.

This CP specifies security requirements at four levels of assurance, namely basic, medium, medium hardware, and card authentication. 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.

The certificate levels of assurance contained in this CP are set forth in the table below, as well as a brief and non-binding description of the applicability for applications suited to each level.

Table 1-1: Certificate Levels of Assurance

Assurance Level	Applicability
Basic	<p>This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. These environments may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.</p> <p>Basic assurance level certificates are intended to be issued to external entities to improve authentication of these entities when communicating with the USPTO.</p>

Assurance Level	Applicability
Medium	<p>This level is relevant to environments where risks and consequences of data compromise are moderate. These environments may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.</p> <p>Medium assurance level certificates are intended to be issued to USPTO employees and contractors, as well as devices and components within the operational control of USPTO. Medium assurance level certificates may also be issued to external entities if required for the types of transactions these entities have with the USPTO.</p>
Medium Hardware	<p>This level is relevant to environments where threats to data are high or consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.</p>
Card Authentication	<p>This level provides the level of assurance for use in FIPS 201 Personal Identity Verification (PIV) card certificates where the private key can be used without cardholder activation of the PIV card with a PIN. It is used in conjunction with Medium Hardware to provide the set of policies required for PIV card implementation.</p>

1.4.2 Prohibited Certificate Uses

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

1.5 Policy Administration

1.5.1 Specification Administration Organization

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

1.5.2 Contact Person

Questions regarding this CP shall be directed to the Division Manager of the Network and Infrastructure Projects Support Division.

Correspondence Address:

Division Manager
Network Engineering Division

Office of Chief Information Officer
P.O. Box 1450
Alexandria, VA 22313-1450
Phone: (571) 272-5391
Electronic Mail: Wes.Clark@USPTO.GOV

Location Address:

Network Engineering Division
Office of Chief Information Officer
05A87 Madison Building West
600 Dulaney Street
Alexandria, VA 22314

1.5.3 Person Determining CPS Suitability for the Policy

The USPTO Director of the Information Technology Security Management Group will determine the suitability of any CPS for each CA that issues certificates under this policy. If the CPS is found suitable, the Director will recommend approval to the USPTO Policy Authority.

1.5.4 CPS Approval Procedures

CAs issuing under this policy are required to meet all facets of the policy. The USPTO PKI Policy Authority will not issue waivers.

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

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

1.6 Definitions and Acronyms

See Sections 11 and 12.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

All CAs that issue certificates under this policy are obligated to post all CA certificates issued by or to the CA and CRLs issued by the CA in a directory that is publicly accessible through the Lightweight Directory Access Protocol (LDAP) and Hypertext Transport Protocol (HTTP). The

USPTO CA will publish subscriber certificates in this directory in accordance with USPTO policy, except as noted in section 9.4.3. Certificates are published following subscriber acceptance as specified in Section 4.4 and proof of possession of private key as specified in Section 3.2.1. All information to be published in the repository shall be published promptly after such information becomes available to the CA. The CA shall specify in its CPS time limits within which it will publish various types of information

Repositories that support a CA in posting information as required by this policy shall:

- Maintain availability of the information as required by the certificate information posting and retrieval stipulations of this policy, and
- Provide access control mechanisms sufficient to protect repository information as described in Section 2.4.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

USPTO CAs shall publish all certificates issued by or to the CA and all CRLs issued by the CA to an online repository that is available to subscribers and relying parties and contains:

- Issued encryption certificates that assert one or more of the policy OIDs listed in this CP,
- The most recently issued CRL and CARL,
- Cross-certificates where appropriate,
- The CA’s certificate for its certificate signing key, and
- The CA’s certificate for its CRL and CARL signing key.

2.2.2 Publication of CA Information

The USPTO CP shall be publicly available to subscribers and relying parties on a USPTO website.

The CPS for USPTO CAs will not be published, but will be made available on a need-to-know basis.

2.2.3 Interoperability

Where certificates and CRLs are published in directories, standards-based schemas for directory objects and attributes shall be used.

2.3 Time or Frequency of Publication

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

2.4 Access Controls on Repositories

USPTO CAs shall protect any repository information not intended for public dissemination or modification. CA certificates and CRLs and CARLs in the repository shall be publicly available through the Internet. The USPTO General Counsel under applicable Federal Laws, and Departmental and USPTO regulations shall determine access to other information in the CA repositories. The CPS shall detail what information in the repository shall be exempt from automatic availability to USPTO staff or external parties and to whom, and under what conditions, the restricted information may be made available.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

The USPTO Certificate Authorities shall be able to generate and sign certificates that contain an X.500 Distinguished Name (DN); the X.500 DN may also contain domain component elements. Certificates issued to CAs and Registration Authorities shall use the Distinguished Name form, and have an assurance level equal to, or greater than, the highest level of assurance of the certificates the CA issues to subscribers or other CAs. Where Distinguished Names are required, subscribers shall have them assigned in accordance with section 3.1.2. Certificates may additionally assert an alternate name form subject to requirements set forth below intended to ensure name uniqueness. The table below describes the naming requirements that apply to each level of assurance.

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	Non-null Subject Name, and optional Alternative Subject Name if marked non-critical
Card Authentication	Non-Null Subject Alternative Name that is of the FASC-N name type, and optional Subject Name
Medium	X.500 Distinguished Name as noted above, and optional Alternative Subject Name if marked non-critical

Assurance Level	Naming Requirements
Medium Hardware	Non-null Subject Name, and optional Alternative Subject Name if marked non-critical

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

dc=gov, dc=uspto, ou=users,

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

dc=gov, dc=uspto, ou= users, cn= *lastname, nickname*
 dc=gov, dc=uspto, ou= users, cn= *lastname, firstname initial.*
 dc=gov, dc=uspto, ou= users, cn= *lastname, firstname middlename*

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

dc=gov, dc=uspto, ou=people, cn= *lastname, nickname (affiliate)*
 dc=gov, dc=uspto, ou=people, cn= *lastname, firstname initial. (affiliate)*
 dc=gov, dc=uspto, ou=people, cn= *lastname, firstname middlename (affiliate)*

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

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

dc=gov, dc=uspto, cn=computers, cn=*device name*
 dc=gov, dc=uspto, ou=domain controllers, cn=*device name*

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

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

Internet domain component names are composed of the following attributes: domain component, organizational unit, and common name.

Certificates issued under id-pto-medium-2003 shall include a subject alternative name. At a minimum, the subject alternative name extension may include the pivFASC-N name type [FIPS 201-1]. The value for this name shall be the FASC-N [PACS] of the subject's PIV card.

Certificates issued under id-pto-cardAuth may include a subject alternative name extension that includes the pivFASC-N name type. The value for this name shall be the FASC-N of the subject's PIV card. Certificates issued under id-pto-cardAuth shall not include any other name in the subject alternative name extension but may include a non-NULL name in the subject field. If included, the subject-distinguished name shall take one of the following forms:

dc=gov, dc=uspto, ou=[ou=structural container], serialNumber=*FASC-N*

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

3.1.2 Need for Names to be Meaningful

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

The common name in the Distinguished Name must represent the subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name. For components, this may be a model name and serial number, an application process, or a fully qualified Internet domain name.

While the relying parties do not generally interpret the issuer name in CA certificates, this CP requires the use of meaningful names by CAs issuing under this policy. If included, the common name should describe the issuer. The subject name in CA certificates must match the issuer name in certificates issued by the subject, as required by Request for Comment 3280.

All certificates issued by the USPTO CA at the medium assurance level shall have name constraints asserted that limit the name space of the Principal CA to that appropriate for their Domains. Additionally, the USPTO Policy Authority may require that the USPTO CA include such constraints for the USPTO CA certificates issued at the basic level if it deems appropriate.

3.1.3 Anonymity or Pseudonymity of Subscribers

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

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

Name uniqueness across the USPTO PKI must be enforced. The Policy Authority along with Certificate Authorities and Registration Authorities shall enforce name uniqueness within the X.500 name space that they have been authorized to use (e.g., an electronic mail address or Domain Naming Service name). When name forms other than a Distinguished Name are used, they too must be allocated such that name uniqueness across the USPTO and the Federal PKI is ensured.

The Customer Support Services Group is the naming authority for the 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.

Where possible, each directory information tree shall be assigned to a single CA. Where multiple CAs share a single directory information tree, the Policy Authority shall review and approve procedures for name space control. Each CPS associated with this CP shall document:

- What name forms shall be used,
- How the Certificate Authorities and Registration Authorities will interact with the Policy Authority to ensure name uniqueness is accomplished, and
- How names will be allocated within the subscriber community to guarantee name uniqueness among current and past subscribers.

3.1.6 Recognition, Authentication, and Role of Trademarks

The Policy Authority shall resolve any name collisions brought to its attention.

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

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys that party shall be required to prove possession of the private key, which corresponds to the public key in the

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

In the case where key generation is performed directly on a storage hardware token, such as a smart card, or in a key generator that benignly transfers the key to the parties' storage module, then the party is deemed to be in possession of the private key at the time of generation or transfer if the owning party performed the action that initiated the key generation.

If the party is not in possession of the token when the key is generated, then the token (e.g., a smart card or a Public Key Cryptographic Standard #12 encoded message) shall be delivered to the subject via a secure and accountable method approved in section 6.1.2. Any such transfer methods will be detailed in the CPS for the CA.

For all assurance levels, when keyed hardware tokens are delivered to certificate subjects, the delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subjects. The CA must maintain a record of validation for receipt of the token by the subject. When any mechanism that includes a shared secret (e.g., a password or PIN) is used, the mechanism shall ensure that the applicant and the CA are the only recipients of this shared secret.

3.2.2 Authentication of Organization Identity

Requests for certificates in the name of an organization shall include the organization name, address, and documentation of the existence of the organization, and shall identify an individual who will serve the role of PKI Sponsor. This individual will normally be a manager responsible for the organizational function supported with the certificate. The Operational Authority or RA shall verify this information, in addition to the authenticity of the requesting representative, and that representative's authorization to act in the name of the organization. Organization certificates shall be issued only at the basic level of assurance in accordance with Section 6.1.3.

3.2.3 Authentication of Individual Identity

3.2.3.1 Authentication of Human Subscribers

The RA or LRA shall ensure that the applicant's identity information is verified no more than 30 days before initial certificate issuance and checked in accordance with this CP and the applicable CPS. USPTO PKI CAs and RAs shall ensure that the applicant's identity information and public key are properly bound. Additionally, Registration Authorities shall record the process that was followed for issuance of each certificate. Process information shall depend on the certificate level of assurance and shall be addressed in the CPS. The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identification;

- A signed declaration by that person that he or she verified the identity of the applicant;
- A unique identifying number from the identity of the verifier, and if in-person identity proofing is done, a unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature. If in-person identity proofing is done, this signing shall be performed in the presence of the person performing the identity authentication.

In-person proofing for medium assurance, the applicant shall provide at least one federal government issued picture identification credential, or two forms of identity source documents in original form. The identity source documents must come from the list of acceptable documents included in *Form I-9, OMB No. 1115-0136, Employment Eligibility Verification*. At least one document shall be a valid State or Federal government-issued picture identification (ID). The applicant's identity must be personally verified prior to the applicant's certificate being enabled. The applicant shall appear personally before an RA or an approved LRA.

For Basic assurance, identity shall be established by one of the following methods:

- In-person proofing as described for medium assurance;
- Comparison with trusted information in a database of user-supplied information, either obtained and checked electronically or through other trusted means such as the U.S. Mail; or
- By attestation of a supervisor, administrative or information security officer, or a person certified by a state or Federal Entity as being authorized to confirm identities.
- If an applicant is unable to perform face-to-face registration alone (e.g., a network device), a trusted person serving as a PKI Sponsor who has already been issued a digital certificate by the Authorized CA shall represent the applicant. The Sponsor will present information sufficient for registration at the level of the certificate being requested, for both him/her and the network device that the Sponsor is representing.

3.2.3.2 Authentication of Component Identities

Some computing and communications components (e.g., routers and firewalls.) will be named as certificate subjects. In such cases, the component must have a human PKI Sponsor as described in Section 5.2.2.2. The PKI Sponsor is responsible for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., Domain Name Service name),
- Equipment public keys,
- Equipment authorizations and attributes (if any are to be included in the certificate), and

- Contact information for the PKI sponsor.

The registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from sponsor (using certificates of equivalent or greater assurance than that being requested); or
- In person registration by the sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 3.2.3.1.

3.2.3.3 Authentication of Human Subscribers for Group Certificates

Normally, a certificate shall be issued to a single subscriber. For cases where there are several entities acting in one capacity or role, as in the case of organizational certificates, and where non-repudiation for transactions is not desired, a certificate may be issued that corresponds to a private key that is shared by multiple subscribers. In these cases:

- An individual shall be designated in writing to be responsible as the PKI Sponsor for ensuring control of the private key, including maintaining a list of subscribers who have access to use of the private key, and accounting for which subscriber had control of the key at what time;
- The list of those holding the shared private key must be provided to, and retained by, the CA and/or RA;
- The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of this CP (e.g., key generation, private key protection, and subscriber obligations),
- The subjectName DN must not imply that the subject is a single individual, e.g. by inclusion of a human name form, and
- Hardware tokens containing USPTO CA private signature keys may be backed-up in accordance with security audit requirements defined Section 4.5.1.

The methods used for public key delivery shall be stipulated in the CPS.

3.2.4 Non-verified Subscriber Information

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

3.2.5 Validation of Authority

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

3.2.6 Criteria for Interoperation

The U.S. Patent and Trademark Office shall determine the interoperability criteria for CAs operating under this policy

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

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

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

Assurance Level	Routine Re-key Identity Requirements for Subscriber Signature and Encryption Certificates
Basic	Identity may be established through use of current signature key, except that identity shall be reestablished through initial registration process at least once every 15 years from the time of initial registration.
Medium	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration.
Medium Hardware	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration.
Card Authentication	Identity may be established in accordance with the requirements specified in FIPS 201.

3.3.2 Identification and Authentication for Re-key after Revocation

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

3.4 Identification and Authentication for Revocation Requests

OCIO IT SECURITY – PKI CERTIFICATE POLICY

Revocation requests must be authenticated in the manner used to establish the subscriber's identity for certificate issuance, or by means of a shared secret. 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.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

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

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

These steps may be performed in any order that is convenient and that does not defeat security, but all must be completed prior to certificate issuance.

4.1.1 Who Can Submit a Certificate Application

4.1.1.1 CA Certificates

An authorized representative of the applicant CA shall submit applications for CA certificates.

4.1.1.2 User Certificates

The applicant or a trusted agent shall submit applications for user (subscriber) certificates.

4.1.1.3 Component Certificates

The PKI Sponsor of the device shall submit applications for component certificates.

4.1.2 Enrollment Process and Responsibilities

All communications among PKI Authorities supporting the certificate application and issuance process among PKI authorities shall be authenticated and protected from modification; any electronic transmission of shared secrets shall be protected. Communications may be electronic or out-of-band. Electronic communication methods shall employ cryptographic mechanisms commensurate with the strength of the key pair of the certificate shall use. Out-of-band communications shall protect the confidentiality and integrity of the data.

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

4.2 Certificate Application Processing

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

4.2.1 Performing Identification and Authentication Functions

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

4.2.2 Approval or Rejection of Certificate Applications

For the USPTO Root CA, the USPTO Policy Authority may approve or reject a certificate application.

For CAs operating under this policy, approval or rejection of certificate applications is at the discretion of the USPTO Operational Authority Officers or their designees.

4.2.3 Time to Process Certificate Applications

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

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

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

- Verify the identity of the requestor;
- Verify the authority of the requestor and the integrity of the information in the certificate request;
- Build and sign a certificate, if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate); and
- Make the certificate available to the subscriber after confirming that the subscriber has formally acknowledged their obligations as described in section 9.6.3.

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

While the subscriber may do most of the data entry, it is the responsibility of the RA to verify that the information is correct and accurate. If databases are used to confirm subscriber information, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance of the certificate being sought.

To the extent practical, certificates once created shall be checked to ensure that all fields and extensions are properly populated. This checking may be done through software that scans the fields and extensions looking for any evidence that a certificate was improperly manufactured.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

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

4.4 Certificate Acceptance

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

For all levels of assurance certificates, the subscriber shall sign a Subscriber Agreement containing the obligations regarding protection of the private key and the use of the certificates prior to being issued any certificates.

The ordering of the activities in this process, and the mechanisms used, will depend on factors such as where the key is generated and how certificates are posted. In the case of non-human components (router, firewalls, etc.), the PKI sponsor (as defined in Section 5.2.1.6) shall perform the functions of the subscriber.

4.4.1 Conduct Constituting Certificate Acceptance

For all CAs operating under this policy, there is no stipulation.

4.4.2 Publication of the Certificate by the CA

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

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

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

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

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

4.5.2 Relying Party Public Key and Certificate Usage

USPTO-issued certificates specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. All CAs operating under this policy shall issue CRLs specifying the current status of all unexpired certificates (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.

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. Subscriber certificates issued under this policy shall not be renewed, except during recovery from a CA compromise (see Section 5.7.3).

Certificate renewal may occur only if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the subscriber name and attributes are unchanged.

4.6.1 Circumstance for Certificate Renewal

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

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

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

4.6.2 Who May Request Renewal

USPTO CAs may perform renewal of its Subscriber certificates without a corresponding request, such as when the CA re-keys.

4.6.3 Processing Certificate Renewal Requests

No stipulation.

4.6.4 Notification of New Certificate Issuance to Subscriber

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

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6 Publication of the Renewal Certificate by the CA

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

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

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 Certificate Re-key

Re-keying a certificate 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.

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

Table 4-1: Re-keying Identity Requirements

Assurance Level	Routine Re-key Identity Requirements
------------------------	---

Assurance Level	Routine Re-key Identity Requirements
Basic	Signature re-key every five years Confidentiality re-key every five years Identity established through use of current signature key Must prove possession of corresponding private key May authenticate to PKI for re-key with current key twice, after which identity shall be reestablished through initial registration process.
Medium	Signature re-key every three years Confidentiality re-key every three years Identity established through use of current signature key Must prove possession of corresponding private key May authenticate to PKI for re-key with current key twice, after which identity shall be established through initial registration process.

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

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. (Sections 5.6 and 6.3.2 establish usage periods for private keys for both CAs and subscribers.) Examples of circumstances requiring certificate re-key include: expiration, loss or compromise, issuance of a new hardware token, and hardware token failure.

4.7.2 Who May Request Certification of a New Public Key

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

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

4.7.3 Processing Certificate Re-keying Requests

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

4.7.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

No stipulation.

4.7.6 Publication of the Re-keyed Certificate by the CA

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

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

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate Modification

Modifying a certificate means creating a new certificate that has the same or a different key, 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.

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

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

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

4.8.3 Processing Certificate Modification Requests

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

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

4.8.4 Notification of New Certificate Issuance to Subscriber

When a CA modifies its private signature key and thus generates a new public key, the CA shall notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed. For self-signed certificates, such certificates shall be conveyed to users in a secure fashion to preclude malicious substitution attacks. CAs that distribute self-signed certificates shall generate key rollover certificates, where the new public key is signed by the old private key, and vice versa. This permits acceptance of newly issued certificates and CRLs without distribution of the new self-signed certificate to current users. Key rollover certificates are optional for CAs that do not distribute self-signed certificates.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

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

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

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

Certificate suspension is not allowed by this policy

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

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

4.9.1 Circumstances for Revocation

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

- The subject's employment, contract or other relationship with the USPTO ends;
- Identifying information or affiliation components of any names in the certificate become invalid;
- Privilege attributes asserted in the subscriber's certificate are reduced;
- The subscriber can be shown to have violated the stipulations of its Subscriber Agreement;
- The private key is suspected of compromise; and
- The subscriber or other authorized party (as defined in the Certificate Authorities CPS) asks that the subscriber's certificate be revoked.

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

4.9.2 Who can Request a Revocation

Within the PKI, a CA may summarily revoke certificates within its domain. A written notice and brief explanation for the revocation may subsequently be provided to the subscriber, unless laws, regulations or operating policies defined by USPTO preclude such notification. The RA can request the revocation of a subscriber's certificate on behalf of any authorized party such as a LRA or PKI Sponsor, as specified in the associated CPS. Subscribers may request revocation of their own certificates, and PKI Sponsors may request revocation of certificates they sponsor.

4.9.3 Procedure for Revocation Request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). In particular, if the revocation is being requested for reason of key compromise or suspected fraudulent use, then the subscriber's or the RA's revocation request must so indicate. The steps involved in the process of requesting a certificate revocation shall be detailed in the CPS.

Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties. The RA shall authenticate and validate the authority of the requester to request the revocation of a certificate; for signed request from the certificate subject or from a LRA, verification of the signature is sufficient.

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

- Revocation request was not for key compromise,
- Hardware token does not permit the user to export the signature private key,
- Subscriber surrendered the token to the PKI,
- Token was zeroized or destroyed promptly upon surrender, and
- Token has been protected from malicious use between surrender and zeroization or destruction.

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

Upon receipt of a revocation request involving a USPTO certificate, the Operational Authority shall authenticate the request and apprise the appropriate USPTO official (e.g., Human Resources director, office manager, Contract Officer Technical Representative, etc.) If the revocation request appears to be valid, the designated official shall direct the Operational Authority to revoke the certificate by placing its serial number and other identifying information on a CRL/CARL and then post the CRL/CARL in the USPTO repository, in addition to any other revocation mechanisms used.

For PKI implementations using hardware tokens, a subscriber ceasing its relationship with USPTO shall, prior to departure, surrender to USPTO (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of USPTO. If a subscriber leaves USPTO and the hardware tokens cannot be obtained from the subscriber, then all subscriber certificates associated with the uncollected token shall be revoked as quickly as practical upon receipt of the token. The token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction.

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

4.9.4 Revocation Grace Period

There is no grace period for revocation under this policy; Certificate Authorities will revoke certificates as quickly as practical upon receipt of a proper revocation request, and shall always revoke certificates within the time constraints described in Section 4.9.7.

4.9.5 Time within which CA must Process the Revocation Request

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

4.9.6 Revocation Checking Requirements for Relying Parties

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

4.9.7 CRL/CARL Issuance Frequency

CRLs and CARLs are periodically issued and posted to a repository, even if there are no changes or updates to be made, to ensure timeliness of information. CRLs may be issued more frequently than required. If there are circumstances under which the CA will post early updates, these circumstances shall be spelled out in its Certification Practice Statement. Certificate Authorities shall ensure that superseded CRLs are removed from the repository upon posting of the latest CRL.

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

CAs shall make public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to subscribers during certificate request or issuance, and shall be readily available to any potential relying party.

CAs that only issue certificates to CAs and that are generally not operated in a continuous, online state, must issue CRLs at least once every 24 hours, and the *nextUpdate* time in the CRL may be no later than 48 hours after issuance time (i.e., the *thisUpdate* time).

CAs that issue certificates to subscribers or operate online must issue CRLs at least once every 24 hours, and the *nextUpdate* time in the CRL may be no later than 48 hours after issuance time (i.e., the *thisUpdate* time).

Table 4-2: CRL Issuance Requirements for Certification Authorities

Assurance Level	Routine CRL Issuance Frequency	CRL Issuance for Loss or Compromise of Private Key
Basic	24 hours	Within 24 hours of notification
Medium	24 hours	Within 18 hours of notification
Medium Hardware	24 hours	Within 18 hours of notification
Card Authentication	24 hours	Within 18 hours of notification

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

4.9.8 Maximum Latency for CRLs

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

4.9.9 Online Revocation / Status Checking Availability

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

USPTO CAs that issue certificate status online or via delegated certificate status responders, should they be utilized, must meet or exceed the requirements for CRL issuance stated in 4.9.12 for distribution of certificate status information.

4.9.10 Online Revocation Checking Requirements

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

4.9.11 Other Forms of Revocation Advertisements Available

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

- The alternative method must be described in the CA's approved CPS,

- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified, and
- The alternative method must meet the issuance and latency requirements for CRLs stated in sections 4.9.7 and 4.9.8.

4.9.12 Special Requirements Related to Key Compromise

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

4.9.13 Circumstances for Suspension

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

4.9.14 Who Can Request Suspension

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

4.9.15 Procedure for Suspension Request

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

4.9.16 Limits on Suspension Period

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

4.10 Certificate Status Services

No stipulation.

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

No stipulation.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

CA private keys are never escrowed.

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

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

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

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

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

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

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

CA equipment shall always be protected from unauthorized access, especially while the cryptographic module is installed and activated. Physical access controls shall be implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated.

Access to cryptographic modules and the CA equipment shall require the presence of two authorized persons.

The security mechanisms shall be commensurate with the level of threat in the equipment environment. The physical security requirements for basic assurance CAs are intended to:

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

In addition to those requirements, medium assurance CAs shall:

- Be manually or electronically monitored for unauthorized intrusion at all times,
- Ensure an access log is maintained and inspected periodically, and
- Require two-person physical access control to both cryptographic module and computer system.

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

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

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open” and secured when not “closed”),
- Any security containers are properly secured,
- Physical security systems (e.g., door locks and vent covers) are functioning properly, and
- The area is secured against unauthorized access.

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

5.1.2.2 Physical Access for RA Equipment

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

5.1.2.3 Physical Access for CSS Equipment

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

5.1.3 Power and Air Conditioning

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

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

5.1.4 Water Exposures

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

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

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

5.1.8 Off-site Backup

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

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

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be diligent and trustworthy as described in the next section. The functions performed in these roles form the basis of trust in the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first approach is to ensure that the

person filling the role is trustworthy and properly trained. The second is to distribute the functions of the role among several people, so that any malicious activity requires collusion.

The primary trusted roles defined by this policy and detailed in this section are the CA, RA, Auditor, and Operator.

Other important roles include LRA, and PKI Sponsor. They are detailed in Section 5.2.2.

5.2.1.1 Certification Authority

Personnel operating the CA shall consist of CA Administrators and CA Security Officers.

5.2.1.1.1 CA Administrator

CA Administrators shall be responsible for:

- Installing, configuring, and maintaining the CA;
- Establishing and maintaining CA system accounts;
- Configuring certificate profiles, templates, and audit parameters; and
- Generating and backing up CA keys.

5.2.1.1.2 CA Security Officer

CA Security Officers shall be responsible for:

- Registering new CA Trusted Role personnel and requesting the issuance of certificates to Trusted Role personnel,
- Verifying the identity of Trusted Role personnel and accuracy of information included in Trusted Role certificates, and
- Controlling the cryptographic modules containing the CA private key.

5.2.1.2 RA

Registration Authorities shall be responsible for:

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

5.2.1.3 Auditor

Auditors shall be responsible for:

- Reviewing, maintaining, and archiving audit logs,
- Performing or overseeing internal compliance audits to ensure that CAs and associated Registration Authorities are operating in accordance with the appropriate Certification Practice Statement, and
- Auditors shall not request or approve certificate issuance.

5.2.1.4 Operator

Operators shall be responsible for:

- Initial configuration of the base computing system, including installation of the operating system and supporting applications on the CA server, initial setup of computing domain membership and required domain accounts for CA components, configuration of initial host and network parameters, and general system security configuration and lockdown activities;
- Performance of system backups; and
- Secure storage and distribution of backups and upgrades to an off-site location.

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

5.2.1.5 LRA

An LRA is a person authorized to act as a representative of an RA in providing subscriber identity verification during the registration process. LRAs do not have automated interfaces with CAs; they act on the behalf of the RA to verify the identity of the subscriber.

5.2.1.6 PKI Sponsor

A PKI Sponsor fills the role of a subscriber for non-human system components and organizations that are named as public key certificate subjects. For device and infrastructure component certificates, a PKI Sponsor works with Registration Authorities and, when appropriate, their LRAs, to register components in accordance with Section 3.2.3.3. For organizational certificates intended to be shared by multiple individuals, a PKI Sponsor requests issuance of certificates and maintains the list of individuals who have access to the private key associated with the certificate. PKI Sponsors may also fill the role of subscriber as appropriate for disabled personnel. PKI Sponsors are responsible for meeting the obligations of subscribers as defined throughout this document.

5.2.2 Number of Persons Required per Task

Two or more persons are required for the following tasks:

- CA key generation,
- CA signing key activation, and
- CA private key backup.

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

5.2.3 Identification and Authentication for Each Role

CA software and hardware shall identify and authenticate its users and shall ensure that no user can assume more than one of these roles. No individual shall be assigned more than one identity.

5.2.4 Roles Requiring Separation of Duties

Individual CA personnel shall be specifically designated to the roles of CA, RA, Auditor, and Operator as defined in Section 5.2.1.1 to 5.2.1.4. Individuals may not serve more than one of the roles of CA, RA, or Auditor. Individuals designated as Auditors may themselves be subscribers to the PKI, but may not serve any additional roles.

5.2.5 Identification and Authentication for Each Role

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

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

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

5.3.2 Background Check Procedures

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

- Employment,

- Education,
- Place of residence,
- Law Enforcement, and
- References.

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

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

5.3.3 Training Requirements

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

- CA or RA security principles and mechanisms;
- All PKI software versions in use on the CA or RA system;
- All PKI duties they are expected to perform;
- Disaster recovery and business continuity procedures; and
- Stipulations of this policy.
- Documentation detailing the following shall be kept:
 - The name and role of the person receiving training,
 - The scope of the training, and
 - The dates of the training.

5.3.4 Retraining Frequency and Requirements

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

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Contracting Personnel Requirements

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

5.3.8 Documentation Supplied to Personnel

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

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

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

5.4 Audit Logging Procedures

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

5.4.1 Types of Events Recorded

All security auditing capabilities of the underlying CA operating system and the PKI CA applications shall be enabled.

At a minimum, each audit record shall including the following:

- The type of event,
- The date and time the event occurred,

OCIO IT SECURITY – PKI CERTIFICATE POLICY

- A success or failure indicator when executing the CA’s signing process,
- A success or failure indicator when performing certificate revocation, and
- The identity of the entity and/or operator of the CA that caused the event.

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

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

Auditable Event	Basic	Medium
SECURITY AUDIT		
Any changes to the Audit parameters, e.g., audit frequency and type of event audited	X	X
Any attempt to delete or modify the Audit logs	X	X
Obtaining a third-party time-stamp	X	X
IDENTIFICATION AND AUTHENTICATION		
Successful and unsuccessful attempts to assume a role	X	X
The value of maximum authentication attempts is changed	X	X
<i>Maximum authentication attempts</i> unsuccessful authentication attempts occur during user login	X	X
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X
An administrator changes the type of authenticator, e.g., from password to biometrics	X	X
LOCAL DATA ENTRY		
All security-relevant data that is entered in the system	X	X
REMOTE DATA ENTRY		
All security-relevant messages that are received by the system	X	X
DATA EXPORT AND OUTPUT		

OCIO IT SECURITY – PKI CERTIFICATE POLICY

Auditable Event	Basic	Medium
All successful and unsuccessful requests for confidential and security-relevant information	X	X
KEY GENERATION		
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X
PRIVATE KEY LOAD AND STORAGE		
The loading of Component private keys	X	X
All access to certificate subject private keys retained within the CA for key recovery purposes	X	X
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE		
All changes to the trusted public keys, including additions and deletions	X	X
SECRET KEY STORAGE		
The manual entry of secret keys used for authentication	X	X
PRIVATE AND SECRET KEY EXPORT		
The export of private and secret keys (keys used for a single session or message are excluded)	X	X
CERTIFICATE REGISTRATION		
All certificate requests	X	X
CERTIFICATE REVOCATION		
All certificate revocation requests	X	X
CERTIFICATE STATUS CHANGE APPROVAL		
The approval or rejection of a certificate status change request	X	X
CA CONFIGURATION		
Any security-relevant changes to the configuration of the CA	X	X

OCIO IT SECURITY – PKI CERTIFICATE POLICY

Auditable Event	Basic	Medium
ACCOUNT ADMINISTRATION		
Roles and users are added or deleted	X	X
The access control privileges of a user account or a role are modified	X	X
CERTIFICATE PROFILE MANAGEMENT		
All changes to the certificate profile	X	X
REVOCATION PROFILE MANAGEMENT		
All changes to the revocation profile	X	X
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT		
All changes to the certificate revocation list profile	X	X
MISCELLANEOUS		
Appointment of an individual to a trusted role	X	X
Designation of personnel for multiparty control	X	X
Installation of the operating system	X	X
Installation of the CA	X	X
Installing hardware cryptographic modules	If applicable	X
Removing hardware cryptographic modules	If applicable	X
Destruction of cryptographic modules	X	X
System Startup	X	X
Logon Attempts to CA Apps	X	X
Receipt of Hardware / Software		X
Attempts to set passwords	X	X
Attempts to modify passwords	X	X

OCIO IT SECURITY – PKI CERTIFICATE POLICY

Auditable Event	Basic	Medium
Backing up CA internal database	X	X
Restoring CA internal database	X	X
File manipulation (e.g., creation, renaming, moving)		X
Posting of any material to a repository		X
Access to CA internal database		X
All certificate compromise notification requests	X	X
Loading tokens with certificates		X
Shipment of tokens		X
Zeroizing tokens	X	X
Re-key of the CA	X	X
Configuration changes to the CA server involving:		
Hardware	X	X
Software	X	X
Operating System	X	X
Patches	X	X
Security Profiles		X
PHYSICAL ACCESS / SITE SECURITY		
Personnel Access to room housing CA		X
Access to the CA server		X
Known or suspected violations of physical security	X	X
ANOMALIES		
Software Error conditions	X	X
Software check integrity failures	X	X

Auditable Event	Basic	Medium
Receipt of improper messages		X
Misrouted messages		X
Network attacks (suspected or confirmed)	X	X
Equipment failure	X	X
Electrical power outages		X
Alternate power supply failure		X
Obvious and significant network service or access failures		X
Violations of Certificate Policy	X	X
Violations of Certification Practice Statement	X	X
Resetting operating system clock	X	X

5.4.2 Frequency of Processing Data

Audit logs shall be reviewed in accordance with the table below. All significant events shall be explained in an audit log summary. A statistically significant sample of security audit data generated by the CA since the last review shall be examined. This amount will be described in the CPS. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

Assurance Level	Review Audit Log
Basic	Required only for cause
Medium	At least once every two months. Audit data generated by Agency CAs since the last review shall be examined as well as a reasonable search for any evidence of malicious activity

5.4.3 Retention Period for Security Audit Data

Audit logs shall be retained on site for at least two months as well as being retained in the manner described in Section 5.5. The individual who removes audit logs from the CA or system shall be an official different from the individuals who, in combination, control the CA signature key.

5.4.4 Protection of Security Audit Data

The security audit data shall not be open for reading or modification by any human, or by any automated process other than those that perform security audit processing. CA system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data. The entity performing security audit data archive need not have modify access, but procedures must be implemented to protect archived data from deletion or destruction prior to the end of the security audit data retention period (note that deletion requires modification access). Security audit data shall be moved to a safe, secure storage location separate from the CA equipment.

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

Only authorized people have read access to the logs,

Only authorized people may archive audit logs, and

Audit logs are not modified.

5.4.5 Security Audit Data Backup Procedures

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

5.4.6 Security Audit Collection System (Internal vs. External)

The security audit process shall run independently and shall not in any way be under the control of the CA. Security audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated security audit system has failed and the integrity of the system or confidentiality of the information protected by the system is at risk, the Operational Authority Administrator shall determine whether to suspend CA operation until the problem is corrected.

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

The entity operating the Operational Authority shall perform routine self-assessment of security controls.

5.5 Records Archival

Any software applications that would be required to process archival data shall also be archived to ensure that data can be viewed or examined at a later point in time².

5.5.1 Types of Events Archived

CA archive records shall be sufficiently detailed to establish the proper operation of the CA or the validity of any certificate (including those revoked or expired) issued by the CA.

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

- CA accreditation (if applicable),
- Certificate policy,
- Certification Practice Statement,
- Contractual obligations and other agreements concerning operations of the CA,
- System and equipment configuration,
- Modifications and updates to system or configuration,
- Certificate requests,
- Revocation requests,
- Subscriber identity Authentication data as per Section 3.2.3,
- Documentation of receipt and acceptance of certificates,
- Subscriber agreements,

² In this Certificate Policy “archival”, “archived” and “archive” should be understood to refer to the body of records generated by a the PKI 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 PKI-Unique Administrative Records, as well as, USPTO Records Management Policy.

- Documentation of receipt of tokens,
- All certificates issued or published,
- Record of CA Re-key,
- All CRLs and CARLs issued and/or published,
- All audit logs (in accordance with section 5.4.1,
- Other data or applications to verify archive contents, and
- Documentation required by compliance auditors.

5.5.2 Retention Period for Archive

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

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

5.5.3 Protection of Archive

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

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

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

5.5.4 Archive Backup Procedures

No stipulation.

5.5.5 Requirements for Time Stamping of Records

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

5.5.6 Archive Collection System (Internal vs. External)

Archive data may be collected in any expedient manner.

5.5.7 Procedures to Obtain Archive Information

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

5.6 Key Changeover

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

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

When a CA updates its private signature key and thus generates a new public key, the CA shall notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed. CAs that distribute self-signed certificates shall generate key rollover certificates, where the new public key is signed by the old private key, and vice versa. This permits acceptance of newly issued certificates and CRLs without distribution of the new self-signed certificate to current users. Key rollover certificates are optional for CAs that do not distribute self-signed certificates.

5.7 Compromise and Disaster Recovery

The CA and repository shall be deployed to provide availability 24 hours a day, 365 days a year. The CA shall implement features to provide high levels of reliability. The following subsections outline the policy for instances that may prevent such maintenance of reliability.

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

5.7.1 Incident and Compromise Handling Procedures

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

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

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

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

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

If Certification Authority equipment, software, and/or data are corrupted, is damaged or rendered inoperative, CAs operating under this policy shall respond as follows:

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

The USPTO PKI Operational Authority Officers shall be notified as soon as possible.

5.7.3 Certification Authority signature Keys are Compromised

If the CA signature key is compromised or lost (such that compromise is possible) the following shall occur:

- The USPTO PKI Policy Authority shall be immediately and securely notified, as well as any cross-certified CAs and any entities known to be distributing the CA certificate (e.g., in a root store).
- Any CAs that have issued certificates to the CA shall be notified so that they can revoke those certificates.
- The CA shall generate a new CA key pair in accordance with procedures set forth in CPS and section 6.1.1.1.

- If the CA distributed their private key in a trusted certificate for use as a trust anchor, the new self-signed certificate must be distributed via secure out-of-band mechanisms.
- Execute procedures to notify subscribers of the compromise.

The CA under the new key pair may renew subscriber certificates automatically, or the CA may require subscribers to repeat the initial certificate application process.

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

5.7.4 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the Policy Authority shall be immediately and securely notified, and the Policy Authority shall take whatever action it deems appropriate. The CA installation shall then be completely rebuilt, by reestablishing the CA equipment, generating new private and public keys, being re-certified, and re-issuing all cross certificates.

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

5.7.5 Notification Related to Compromise or Disaster

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

5.7.6 Certification Authority Cannot Generate Certificate Revocation

If a CA cannot issue a CRL or CARL prior to the time specified in the next update field of its currently valid CRL/CARL, then the Policy Authority shall be immediately and securely notified. This notification will allow relying parties to protect their interests. The CA shall reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS.

The CA shall immediately and securely advise the Policy Authority 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 of termination of the CA operation, certificates signed by the CA shall be revoked. Prior to CA termination, the CA shall provide archived data to the Policy Authorities' approved archival facility, and the Policy Authority shall securely notify all appropriate authorities (e.g., the FBCA and cross-certified CAs.) of the situation at the earliest feasible time in accordance with applicable Memoranda of Agreement and any other contractual agreements.

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

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

Cryptographic keying material for certificates shall be generated in a FIPS 140 validated cryptographic module. A private key must not appear outside of the module in which it was generated unless it is encrypted for local transmission or for processing or storage by a key recovery mechanism.

CA certificate-signing keys shall be generated in FIPS 140, Security Level 2 or higher validated cryptographic hardware modules. CA key generations procedures shall be documented in the CPS and shall generate auditable evidence that the documented procedures were followed. This documentation must be detailed enough to show that appropriate role separation was used. An independent third party shall validate the process for medium assurance Certificate Authorities.

6.1.1.2 Subscriber Key Pair Generation

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

Key generation shall be performed using a FIPS approved method.

Subscriber key pairs shall be generated in FIPS 140 Level 2 hardware cryptographic modules. Any pseudo-random numbers used for key generation material shall be generated by a FIPS-approved method. Symmetric keys may be generated by means of either software or hardware mechanisms.

6.1.1.3 CSS Key Pair Generation

Cryptographic keying material used by CSSs to sign status information shall be generated in FIPS 140 validated cryptographic modules. The cryptographic module(s) shall meet or exceed FIPS 140 Level 2.

6.1.2 Private Key Delivery to Subscriber

In most cases, private keys will be generated and remain within the cryptographic boundary of the cryptographic module. If the Subscriber generates the key, then there is no need to deliver the private key.

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

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

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

6.1.3 Public Key Delivery to Certificate Issuer

For CAs operating at the Basic, Medium, or Medium Hardware level of assurance, the following requirements apply:

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

For encryption keys only, the USPTO Policy Authority shall retain in secured escrow, copies of entities private keys generated for the purpose of obtaining certificates to be used for the encryption of data (encryption keys). The USPTO Policy Authority shall be responsible for directing the retrieval of encryption keys from escrow and only for the purpose of meeting legal and regulatory responsibilities. The methods used to escrow and retrieve encryption keys shall be detailed in the CA's CPS. Retrieval shall include at a minimum:

- Written direction from the Director of the Information Technology Security Policy Division, and
- Actions to be taken on the part of at least two human entities to cause the keys to be un-escrowed.

When keyed hardware tokens are delivered to subscribers, the delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subscribers. The RA must maintain a record of validation for receipt of the token by the subscriber. When any mechanism that includes a shared secret (e.g., a password or pin) is used, the mechanism shall ensure that the applicant and the RA are the only recipients of this shared secret.

6.1.4 Certification Authority Public Key Delivery to Relying Powers

The public key of the CA must be available for certification trust paths to be created and verified. In general, CA certificates are published in the repository (see Section 2.1.7) operated by the Policy Authority, and the verification of public keys is performed using X.509 path validation.

Where users rely on the CA's public key as a trust anchor, publication in the repository does not permit verification of the public key. To extract the key from a certificate with confidence that it has not been altered, the CA must ensure that its users have obtained a self-signed CA certificate through trusted procedural mechanisms. Such a self-signed CA certificate is sometimes called a self-signed root certificate or a trusted certificate. This document will use the term-trusted certificate for such self-signed certificates.

Acceptable methods for trusted certificate delivery include but are not limited to:

- Registration Authorities loading trusted certificates onto tokens delivered to relying parties via secure mechanisms, such as loading the trusted certificate onto the token during the subscriber's appearance at the RA or when the RA generates the subscriber's key pair and loads the private key onto the token;
- Distribution of trusted certificates through secure out-of-band mechanisms;
- Comparison of certificate hashes or fingerprints against trusted certificate hashes or fingerprints made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and
- Loading trusted certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.

CAs that distribute self-signed certificates shall create key rollover certificates as a consequence of CA re-key. The new CA keys may be used securely (through the X.509 path validation algorithm) without explicit delivery of the public key to subscribers.

The FBCA posts the cross-certificates it issues in the FBCA repository. The USPTO CA shall issue a certificate to the FBCA for posting to the FBCA repository concurrent with the issuance of a FBCA certificate to the USPTO CA. The USPTO CA will then make a copy of the FBCA public key available in the USPTO CA certificate, which facilitates trust path validation. For the USPTO CA to issue cross-certificates to the FBCA, the FBCA shall transport its public key to the USPTO CA in a secure, out-of-band fashion to achieve 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 shall 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 CP requires use of RSA PKCS #1, RSASSA-PSS, or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy shall contain RSA or elliptic curve public keys.

Future versions of this policy may specify additional FIPS-approved signature algorithms.

Trusted Certificates shall contain subject public keys of at least 2048 bits for RSA or 224 bits for elliptic curve, and be signed with the corresponding private key.

CAs that generate certificates and CRLs under this policy shall use signature keys of at least 1024 bits for RSA and 163 bits for elliptic curve algorithms. Certificates that expire on or after

December 31, 2010 shall be generated with at least 2048 bit keys for RSA and 224 bit keys for elliptic curve algorithms.

CAs that generate certificates and CRLs under this policy shall use the SHA-1, SHA-224, SHA-256, or SHA-384 hash algorithm when generating digital signatures. RSA signatures on certificates and CRLs that expire on or after December 31, 2010 shall be generated using SHA-256. ECDSA signatures on certificates and CRLs that expire on or after December 31, 2010 shall be generated using SHA-224, SHA-256, or SHA-384, as appropriate for the key length.

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

End entity certificates issued under id-pto-medium-2003, id-pto-cardAuth, and id-pto-mediumHardware that expire before December 31, 2010 shall contain RSA public keys that are at least 1024 bits in length or elliptic curve keys that are at least 163 bits. End entity certificates issued under id-pto-medium-2003, id-pto-cardAuth, and id-pto-mediumHardware that expire on or after December 31, 2010 shall contain RSA public keys that are at least 2048 bits or elliptic curve keys that are at least 224 bits.

Practice Note: Where certificates are issued to satisfy FIPS 201 requirements, implementations are limited to SHA-256 and SHA-384 for ECDSA.

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require (1) triple-DES or AES for the symmetric key through 12/31/10 and AES for the symmetric key after 12/31/10 and (2) at least 1024 bit RSA or 163 bit elliptic curve keys through 12/31/08 and at least 2048 bit RSA or 224 bit elliptic curve keys after 12/31/08.

6.1.6 Public Key Parameters Generation

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

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

The use of a specific key is constrained by the key usage extension in the X.509 certificate.

Public keys that are bound into subscriber certificates shall be used only for signing or encrypting, but not both, except as specified below. Certificates to be used for digital signatures (including authentication) shall assert the digitalSignature and nonRepudiation bits. Certificates to be used for key transport shall assert the keyEncipherment bit for Rivest, Shamir, and Adleman keys. Certificates to be used for key agreement shall 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 shall be generated and managed in accordance with their respective signature certificate requirements,

except where otherwise noted in this CP. Such "dual-use" certificates shall never assert the nonRepudiation bit, and shall not be used for authenticating data that will be verified on the basis of the dual-use certificate at a future time. USPTO will normally issue each subscriber two key pairs, one for data encryption and one for digital signature and authentication.

Public keys that are bound into CA certificates shall be used only for signing certificates and CRLs. CA certificates whose subject public key is to be used to verify other certificates shall assert the keyCertSign bit. CA certificates whose subject public key is to be used to verify CRLs shall assert the cRLSign bit. If the CA certificate is to be used to verify both certificate and CRLs, both the keyCertSign and cRLSign bits shall be 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 shall assert the digitalSignature bit. Device certificates that contain RSA public keys that are to be used for key transport shall assert the keyEncipherment bit. Device certificates that contain elliptic curve public keys that are to be used for key agreement shall assert the keyAgreement bit. Device certificates to be used for both digital signatures and key management shall assert the digitalSignature bit and either the keyEncipherment (for RSA) or keyAgreement (for elliptic curve) bit. Device certificates shall not assert the nonRepudiation bit.

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [current version of FIPS 140]. Cryptographic modules shall be validated to the FIPS 140 level identified in this section.

The table below summarizes the minimum requirements for cryptographic modules.

Table 6-1: Minimum Requirements for Cryptographic Modules

Assurance Level	Latest Version of FIPS 140 series	Certification Authority & Certificate Status Service	RA	Subscriber
Basic	Required	Level 2 (Hardware or Software)	Level 1 (Hardware or Software)	Level 1 (Hardware or Software)
Medium	Required	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

Assurance Level	Latest Version of FIPS 140 series	Certification Authority & Certificate Status Service	RA	Subscriber
Medium Hardware	Required	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
Card Authentication	Required	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

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

A single person shall not be permitted to activate the CA signature key or access any cryptographic module containing the complete CA private signing key. Access to CA signing keys backed up for disaster recovery shall be under the same multi-person control as the original CA signing key. The names of the parties used for two-person control shall be maintained on a list that shall be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

Under no circumstances shall a third party escrow the USPTO CA signature keys used to support non-repudiation services.

Subscriber key management keys may be escrowed to provide key recovery. The method for key escrow and recovery shall be described in the CA’s CPS or Key Recovery Policy.

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

Subscriber private signature keys should not be held by anyone other than the subscriber, except for the situations noted in Section 6.1.2.

6.2.4 Private Key Backup

6.2.4.1 Backup of Certification Authority Private Signature Key

If backed up, the CA private signature keys shall be backed up under the same multi-person control as the original signature key. A single copy of the signature key may be stored at the CA location. A second copy may be kept at the CA backup location. Backup procedures shall be included in the CA’s Certification Practice Statement.

6.2.4.2 Backup of Subscriber Private Keys

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

6.2.4.3 Backup of Subscriber Private Key Management Key

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

6.2.4.4 Backup of CSS Private Key

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

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

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

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

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS 140.

6.2.8 Method of Activating Private Keys

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

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

6.2.9 Method of Deactivating Private Key

Cryptographic modules, which have been activated, must not be left unattended or otherwise open to unauthorized access. After use, they must be deactivated, e.g. via a manual logout procedure, or by a passive timeout. CA cryptographic modules shall be removed and stored in accordance with Section 5.1.2, when not in use.

6.2.10 Method of Destroying Private Key

Individuals in trusted roles shall destroy CA, RA, and CSS (e.g., OCSP server) private signature keys when they are no longer needed. Subscribers shall either surrender their cryptographic module to CA/RA personnel for destruction or destroy their private signature keys, when they are no longer needed or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a “zeroize” command. Physical destruction of hardware is not required.

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

6.2.11 Cryptographic Module Rating

See section 6.2.1.

6.3 Other Aspects of Key Pair Management

It is technically possible to use the same key-pair for both digital signature and confidentiality. However, this Certification Policy discourages that condition for Basic and Medium, except to support legacy applications as defined in Section 6.1.7.

6.3.1 Public Key Archival

The public key is archived as part of the administrative records of the CA.

6.3.2 Certificate Operational Periods and Key Usage Periods

The USPTO shall limit the use of its private keys to a maximum of three years for certificate signing and six years for CRL signing. CAs that distribute their self-signed certificates for use as trust anchors shall limit the use of the associated private key to a maximum of 20 years; the self-signed certificates shall have a lifetime not to exceed 37 years. For all other CAs, the CA shall limit the use of its private keys to a maximum of four years for subscriber certificates and ten

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

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

PIV authentication certificates, card authentication certificates, and optional digital signature certificates must expire no later than the PIV card expiration date. PIV content signing certificates should not expire before the PIV card expires.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

6.4.2 Activation Data Protection

Activation data for cryptographic modules should be memorized, biometric in nature, or if written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module.

Activation data for private keys associated with certificates asserting individual identities shall never be shared. PKI Sponsors shall ensure that activation data for private keys associated with certificates asserting organizational identities is restricted to those in the organization authorized to use the private keys.

Any data that is used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should either be biometric in nature or memorized, not written down. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module. The protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the CPS.

The activation data protection mechanism for CA equipment or applications shall include a facility to temporarily lock out further access attempts, after a predetermined number of failed login attempts as set forth in the CA's CPS.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The USPTO CA and its ancillary parts shall include the following functionality:

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

When CA equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (e.g., hardware, software, and operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as that which received the evaluation rating.

For Certificate Status Servers operating under this policy, the computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the system or applications,

- Manage privileges of users to limit users to their assigned roles,
- Enforce domain integrity boundaries for security critical processes, and
- Support recovery from key or system failure.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The System Development Controls for the CA are as follows:

- The CA shall use software that has been designed and developed under a formal, documented development methodology;
- Hardware and software procured to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with;
- Hardware and software developed specifically for the CA shall be developed in a controlled environment, and the development process shall be defined and documented (this requirement does not apply to commercial off-the-shelf hardware or software);
- The CA hardware and software shall be dedicated to performing one task: the CA, there shall be no other applications, hardware devices, network connections, or component software installed that are not parts of the CA operation;
- Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment, only applications required to perform the operation of the CA shall be obtained from sources authorized by local policy, RA hardware and software shall be scanned for malicious code on first use and periodically thereafter;
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and shall be installed by trusted and trained personnel in a defined manner; and
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the CA physical location.

6.6.2 Security Management Controls

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

Operational Authority shall periodically verify the integrity of the software as specified in the Certification Practice Statement.

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

6.6.3 Life-Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

CA equipment shall be located on internal networks behind boundary/perimeter network defenses and afforded protections consistent with commercial electronic commerce practices for network security. Services allowed to and from the CA equipment shall be limited to those required to perform CA functions. Other CA equipment may enable additional services consistent with local policy.

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

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

Directories and certificate status servers shall employ appropriate network security controls. Networking equipment shall turn off unused network ports and services. Any network software present shall be necessary to the functioning of the equipment.

6.8 Time Stamping

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

7 CERTIFICATE, CRL, AND PROFILES

7.1 Certificate Profile

Certificates issued by a CA under this policy shall conform to the Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile.

7.1.1 Version Numbers

The CA shall issue X.509 Version 3 certificates (populate version field with integer “2”).

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles. These profiles are written to prescribe an appropriate amount of control over an infrastructure, yet be flexible enough to meet the needs of the various CAs and communities. CAs issuing certificates under this CP shall comply with both the Request for Comment 3280 and the Federal PKI X.509 Certificate and Certificate Revocation List Extension Profile. Whenever private extensions are used, they shall be identified in the CPS. Critical private extensions shall be interoperable in their intended community of use.

7.1.3 Algorithm Object Identifiers

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

id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
Sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
RSA with PSS padding	Id-RSASSA-PSS ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}
ecdsa-with-SHA1	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) 1}
ecdsa-with-Sha224	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1}
ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2}

OCIO IT SECURITY – PKI CERTIFICATE POLICY

ecdsa-with-Sha384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3}
ecdsa-with-Sha512	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4}

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

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

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

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1}

Where non-CA certificates contains an elliptic curve public key, the parameters shall be specified as one of the following named curves:

ansip192r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 1}
ansit163k1	{iso(1) identified-organization(3) certicom(132) curve(0) 1}
ansit163r2	{iso(1) identified-organization(3) certicom(132) curve(0) 15}
ansip224r1	{iso(1) identified-organization(3) certicom(132) curve(0) 33}
ansit233k1	{iso(1) identified-organization(3) certicom(132) curve(0) 26}
ansit233r1	{iso(1) identified-organization(3) certicom(132) curve(0) 27}

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

7.1.4 Name Forms

Where required as set forth in Section 3.1.1, the subject and issuer fields of the base certificate shall be populated with an X.500 Distinguished Name, with standard attribute types such as those defined in RFC 3280.

The subject alternative name extension may be present and include the pivFASC-N name type in certificates issued under id-ptocardAuth.

7.1.5 Name Constraints

CAs shall assert name constraints in CA certificates as required.

7.1.6 Certificate Policy Object Identifier

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

7.1.7 Usage of Policy Constraints Extension

CAs shall assert policy constraints in CA certificates as required.

7.1.8 Policy Qualifiers Syntax and Semantics

USPTO CAs shall avoid issuing certificates containing policy qualifiers. If a requirement for a USPTO CA is identified that requires the issuance of certificates containing policy qualifiers, they must be identified in the applicable CPS and are constrained to the policy qualifiers identified in RFC 3280.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

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

7.2 CRL Profile

CRLs and CARLs issued by a CA under this policy shall conform to the Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile.

7.2.1 Version Numbers

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

7.2.2 CRL and CRL Entry Extensions

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

7.3 OCSP Profile

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

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

7.3.1 Version Number(s)

CSSs operated under this policy shall use OCSP version 1.

7.3.2 OCSP Extensions

Critical OCSP extensions shall not be used.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENT

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

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

8.1 Frequency or Circumstances of Assessment

All CAs and RAs shall be subject to a periodic compliance audit. All medium assurance CAs and RAs shall be subject to yearly compliance audits. All basic assurance CAs and RAs shall be subject to a compliance audit at least once every two years. The USPTO PKI Policy Authority and the FBCA Policy Authority has the right to require periodic and a-periodic compliance audits or inspections of any or all CA or RA operations to validate that the entities are operating in accordance with the security practices and procedures described in their applicable CPS.

Alternative reviews may be substituted for full compliance audits under exceptional circumstances. The conditions that permit an alternative review are as follows:

1. If no changes to policies, procedures, or operations have occurred during the previous year, an assertion to that effect, signed by the cognizant executive (CIO or equivalent), is acceptable in lieu of a full compliance audit.
2. If no significant changes to policies, procedures, or operations have occurred during the previous year, a delta compliance audit is acceptable in lieu of a full compliance audit.
3. However, a full compliance audit (see section 8.4) must be completed every third year regardless.

There is no audit requirement for CAs and RAs operating at the Rudimentary level of assurance.

Examples of significant changes include but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to CA and or RA operating procedures; (iii) installation of a new or upgraded hardware platform or firmware component; and (iv) modifications to the CP. This is consistent with the requirements that trigger a full C&A in NIST SP 800-37.

The USPTO PKI Policy Authority has the right to require periodic and aperiodic compliance audits or inspections of CA, RA, or CSS operations to validate that the subordinate entities are operating in accordance with the security practices and procedures described in their respective CPS. The USPTO PKI Policy Authority shall state the reason for any aperiodic compliance audit.

8.2 Identity/Qualifications of Compliance Auditor

The auditor shall demonstrate competence in the field of compliance audit of PKIs to the USPTO Policy Authority. The auditor must be thoroughly familiar with the Certificate Authorities CPS and this CP and FBCA Policy Authority policies imposes on the issuance and management of their certificates and requirements for cross certification. The compliance auditor must perform such compliance audits as a primary responsibility.

8.3 Compliance Auditor’s Relationship to Assessed Entity

The compliance auditor either shall be a private firm, which is independent from the entities being audited, or it shall be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. If a private firm, the compliance auditor and the USPTO CA shall have a contractual relationship for the performance of the compliance audit. An example of the latter situation may be an Agency inspector general or internal auditor. The Policy Authority shall determine whether a compliance auditor meets this requirement.

8.4 Topics Covered by Compliance Audit

The purpose of a compliance audit shall be to verify that the CA and its recognized RAs comply with all the requirements of this CP, the USPTO CPS and the FBCA CP. All aspects of the CA and RA operation shall be subject to compliance and inspection. LRAs other than Notaries Public and equivalent foreign officers may also be subject to compliance audit.

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

Where permitted by section 8.1, the FBCA or Entity PKI may perform a delta compliance audit in lieu of the full compliance audit. A delta compliance audit covers all changes to policies, procedures, or operations that have occurred during the previous year. The following topics must be addressed in a delta compliance audit even if no changes have occurred since the last full compliance audit:

- Personnel controls,
- Separation of Duties,
- Audit review frequency and scope,
- Types of events recorded in physical and electronic audit logs,
- Protection of physical and electronic audit data,
- Physical security controls, and
- Backup and Archive generation and storage.

8.5 Actions Taken as a Result of Deficiency

The USPTO Policy Authority determines whether the USPTO CA is complying with its obligations as set forth in this CP.

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

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

8.6 Communication of Results

The compliance auditor shall provide the Policy Authority an Audit Compliance Report letter within 20 calendar days of the completion of any Compliance Audit. The report will include identification of corrective measures that are recommended, that have been completed or that are planned for implementation by the CA, RA or LRA. The report shall identify the versions of the CP and CPS used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in Section 8.5 above.

The results will be reported to the audited CA, RA or LRA. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy. If warranted, notice of implementation of required remedies shall be provided to appropriate entities in accordance with established Memoranda of Agreement, Memoranda of Understanding, and contractual agreements.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

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

9.1.1 Certificate Issuance or Renewal Fees

No Stipulation.

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for other Services

No Stipulation.

9.1.5 Refund Policy

No Stipulation.

9.2 Financial Responsibility

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

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

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

9.3.1 Scope of Confidential Information

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

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

9.3.2 Information not within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The USPTO PKI Operational Authority or USPTO PKI Operational Authority Officers shall conduct a Privacy Impact Assessment. If deemed necessary, USPTO PKI Operational Authority or USPTO PKI Operational Authority Officers shall have a Privacy Plan to protect personally identifying information from unauthorized disclosure. The USPTO PKI Policy Authority shall approve the Privacy Plan. Privacy plans will be implemented in accordance with the requirements of the Privacy Act of 1974, as amended.

9.4.2 Information Treated as Private

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

9.4.3 Information not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

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

9.4.5 Notice and Consent to Use Private Information

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

9.4.7 Other Information Disclosure Circumstances

No stipulation

9.5 Intellectual Property Rights

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

9.6 Representations and Warranties

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

9.6.1 CA Representations and Warranties

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

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

- Providing to the Policy Authority a CPS, as well as notice of any subsequent changes, for conformance assessment;
- Conforming to the stipulations of the approved CPS;
- Ensuring that registration information is accepted only from Registration Authorities who understand and are obligated to comply with this policy and the associated CPS;
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating that information contained in the certificates;
- Revoking the certificates of subscribers found to have acted in a manner counter to subscriber obligations in accordance with section 9.6.3 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 this policy shall comply with the stipulations of this policy and comply with a CPS approved by the Policy Authority for use with this policy. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities. An RA supporting this policy shall conform to the stipulations of this document, including:

- 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 or LRA; and

- 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 LRA Representations and Warranties

An LRA shall perform subscriber identity verification in accordance with this CP and in accordance with the CAs approved CPS. LRAs will not directly approve or generate certificate issuance requests. Those activities will be the responsibility of duly authorized RA staff.

9.6.4 Subscriber Representations and Warranties

Subscribers shall:

- Accurately represent themselves in all communications with the PKI authorities and other subscribers;
- Protect their private keys at all times, in accordance with this policy, as stipulated in their subscriber agreements, certificate acceptance agreements and local procedures;
- Notify, in a timely manner, the CA that issued their certificates upon suspicion that their private keys are compromised or lost. Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS;
- Use certificates provided by the USPTO PKI only for transactions related to USPTO business;
- Execute a USPTO Subscriber Agreement as detailed in the CPS acknowledging their obligations, terms, conditions and restrictions upon their private keys and certificates use; and
- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates.

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

9.6.5 Relying Party Representations and Warranties

Parties who rely upon the certificates issued under a policy defined in this document shall:

- Perform a risk analysis to decide whether the level of assurance provided by the certificate is adequate to protect the Relying Party based upon the intended use;
- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- 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

9.6.6 Representations and Warranties of Other Participants

The USPTO may issue certificates to subscribers other than employees of the U.S. Government, such as contractors 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 shall 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 of the Information Technology Security Management Group, in consultation with the USPTO PKI Sponsor, may impose additional conditions and qualifications for such subscribers.

9.7 Disclaimers of Warranties

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

9.8 Limitations of Liability

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

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.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

The Policy Authority shall review this policy at least once every year. The Policy Authority shall maintain and publish a Certificate Policy Plan that describes anticipated changes to this CP. Errors, updates, or suggested changes to this document shall be publicly available. Suggested changes to this CP shall be communicated to the contact in section 1.5.2; such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.2 Notification Mechanism and Period

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

9.12.3 Circumstances under Which OID Must Be Changed

OIDS will be changed if the USPTO PKI Policy Authority determines that a change in the CP reduces the level of assurance provided.

9.13 Dispute Resolutions Provisions

Procedures to resolve disputes with a CA's operations shall be documented in the CA's CPS. The USPTO PKI PA is the final authority to resolve disputes when the CPS procedures do not provide a resolution.

The parties shall 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) shall govern the construction, validity, performance and effect of certificates issued under this CP for all purposes.

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

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

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.

10 BIBLIOGRAPHY

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

Number	Title	Revision	Date
ABADSG	<i>Digital Signature Guidelines</i> , American Bar Association http://www.abanet.org/scitech/ec/isc/dsgfree.html		1 August 1996
ABAPAG	<i>PKI Assessment Guidelines</i> , American Bar Association http://www.abanet.org/scitech/ec/isc		18 June 2001
Common Policy Framework CP	<i>X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework</i> , Version 3647 – 1.0		8 May 2007
DHS CP	<i>X.509 Certificate Policy for the U.S. Department of Homeland Security Public Key Infrastructure (PKI)</i>	V 3.0	28 September 2006
FBCA CP	<i>X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)</i> http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC_3647.pdf	V 2.5	12 July 2007
FIPS 140-2	<i>Security Requirements for Cryptographic Modules</i> http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf		25 May 2001
FIPS 112	<i>Password Usage</i> http://www.itl.nist.gov/fipspubs/fip112.htm		30 May 1985
FIPS 186-2	<i>Digital Signature Standard</i> http://csrc.nist.gov/fips/fips186-2.pdf		27 January 2000
FIPS 201-1	<i>Personal Identity Verification (PIV) of Federal Employees and Contractors</i> http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf		March 2006
FOIAACT	<i>5 U.S.C. 552, Freedom of Information Act</i> http://www.usdoj.gov/oip/foiastat.htm		
FPKI-Prof	<i>Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile</i> http://www.cio.gov/fpkipa/documents/fpki_certificate_profile.pdf		12 October 2005

OCIO IT SECURITY – PKI CERTIFICATE POLICY

Number	Title	Revision	Date
ISO9594-8	<i>Information Technology – Open Systems Interconnection – The Directory: Authentication Framework</i> ftp://ftp.bull.com/pub/OSIdirectotry/ITU/97x509final.doc		1997
ITMRA	<i>40 U.S.C. 1452, Information Technology Management Reform Act</i> http://www4.law.cornell.edu/uscode/40/1452.html		
NAG69C	<i>Information System Security Policy and Certification Practice Statement for Certification Authorities,</i>	Rev. C	November 1999
NARARM P	<i>Records Management Guidance for PKI-Unique Administrative Records,</i> http://www.archives.gov/records-mgmt/policy/final-pki-guidance		14 March 2002
NS4009	<i>NSTISSI 4009, National Information Systems Security Glossary</i>		January 1999
NSD42	<i>National Policy for the Security of National Security Telecom and Information Systems</i> http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)		5 July 1990
Public Key Certificate Standard-1	<i>Public Key Cryptographic Standard #1 v2.0: Rivest, Shamir, and Adleman Cryptography Standard</i> http://www.rsa.com		1 October 1998
Public Key Certificate Standard-12	<i>Personal Information Exchange Syntax Standard</i> http://www.rsa.com/rsalabs/pubs/Public Key Certificate Standard/html/pkes-12.html		April 1997
ECAKRP	<i>Key Recovery Policy for External Certification Authorities</i>	Ver. 1.0	4 June 2002
RFC2510	<i>Certificate Management Protocol, Adams and Farrell</i> http://www.ietf.org/rfc/rfc2510.txt		March 1999
RFC3647	<i>Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Housley, Polk, Ford and Solo.</i> http://www.ietf.org/rfc/rfc3280.txt		November 2003

OCIO IT SECURITY – PKI CERTIFICATE POLICY

Number	Title	Revision	Date
RFC3647	<i>Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework</i> , Chokhani, Ford, Sabett, and Wu. http://www.ietf.org/rfc/rfc3647.txt		November 2003
SP800-78	<i>Cryptographic Algorithms and Key Sizes for Personal Identity Verification</i> http://www.csrc.nist.gov/publications/nistpubs		April 2005

11 ACRONYMS AND ABBREVIATIONS

CA	Certification Authority
CARL	Certification Authority Revocation List
C&A	Certification and Accreditation
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

OCIO IT SECURITY – PKI CERTIFICATE POLICY

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
SDLC	System Development Life Cycle
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
WWW	World Wide Web

12 GLOSSARY

The primary source is *NSTISSI 4009, National Information Systems Security Glossary*; other sources were used if NSTISSI 4009 had no entry for the term, or if another source gave a definition more appropriate to PKI. If no reference is given, the definition is ad hoc.

Term	Definition
access	Ability to make use of any information system resource. [NS4009]
access control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
applicant	The subscriber is sometimes also called an "applicant" after applying to a CA for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
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.

OCIO IT SECURITY – PKI CERTIFICATE POLICY

Term	Definition
Certification Authority (CA)	An authority trusted by one or more users to create and assign certificates. [ISO9594-8]
CA facility	The collection of equipment, personnel, procedures and structures that are used by a CA to perform certificate issuance and revocation.
Certificate	A digital representation of information which at least (1) identifies the CA issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the CA issuing it. [ABADSG]
certificate-related information	Information, such as a subscriber's postal address, that is not included in a certificate, but that may be used by a CA in certificate management.
client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [Federal Information Processing Standard 140]
dual use certificate	A certificate that is intended for use with both digital signature and data encryption services.
e-commerce	The use of network technology (especially the Internet) to buy or sell goods and services
encryption certificate	A certificate containing a public key that is used to encrypt or decrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. The process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate is sometimes referred to as key management.

OCIO IT SECURITY – PKI CERTIFICATE POLICY

Term	Definition
firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
inside threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
integrity	Protection against unauthorized modification or destruction of information. [NS4009]
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.
LRA	Entity authorized to act as a representative of a Certificate Management Authority in providing subscriber identification during the registration process. LRAs do not have automated interfaces with CAs.
naming authority	An organizational entity responsible for assigning distinguished names and for assuring that each distinguished name is meaningful and unique within its domain.
non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009]
outside threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
PKI Sponsor	Fills the role of a subscriber for non-human system components or organizations that are named as public key certificate subjects, and is responsible for meeting the obligations of subscribers as defined throughout this document.

OCIO IT SECURITY – PKI CERTIFICATE POLICY

Term	Definition
privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates.
RA (RA)	Entity responsible for verification of subscriber identity and generation and issuance of subscriber certificates.
Root Certification Authority	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application.
Relying Party	A person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them. [ABADSG]
renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates. [ABADSG]
risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
risk tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
server	A system entity that provides a service in response to requests from clients.
signature certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate. [ABADSG].

Term	Definition
superior Certification Authority	In a hierarchical PKI, a CA who has certified the certificate signing key of another CA, and who constrains the activities of that CA. (see subordinate Certification Authority)
system equipment configuration	A comprehensive accounting of all system hardware and software types and settings.
technical non-repudiation	The contribution public key mechanisms make to the provision of technical evidence supporting a non-repudiation security service.
threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
trust list	Collection of Trusted Certificates used by relying parties to authenticate other certificates.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure, authenticated delivery. The public keys included in Trusted Certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
two person control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. [NS4009]
update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [Federal Information Processing Standard 140]

VII. RESPONSIBILITIES

See paragraphs 1.3.1 through 1.3.6 (PKI Participants)

VIII. EFFECT ON OTHER POLICIES

This policy affects all new, revised, or retired policies issued in Fiscal Year 2009.

ISSUED BY:

Issued By: John B. Owens II, CIO, USPTO
(signature)

John B. Owens II
Chief Information Officer
United States Patent and Trademark Office

OFFICE OF PRIMARY INTEREST: IT Security Management Group