United States Federal PKI X.509 Certification Practice Statement (CPS) for the Federal Public Key Infrastructure (FPKI) Trust Infrastructure

Federal Bridge Certification Authority (FBCA), Federal Common Policy Certification Authority (FCPCA), SHA-1 Federal Root Certification Authority (SHA1 FRCA)

4 August 2014

Version 4.5

REDACTED

Signature Page

_____ _____

Chair, Federal Public Key Infrastructure Policy Authority DATE

Table of Contents

1 FPKI TRUST INFRASTRUCTURE CPS INTRODUCTION 1

1.1 OVERVIEW 2

1.1.1 Certification Practice Statement 2

1.1.2 Relationship Between the CP and the CPS 2

1.1.3 Scope 2

1.1.4 Interoperation with CAs Issuing under Different Policies 3

1.2 DOCUMENT NAME AND IDENTIFICATION 3

1.3 PKI PARTICIPANTS 5

1.3.1 PKI Authorities 5

1.3.2 Registration Authorities 7

1.3.3 Card Management System (CMS) 8

1.3.4 Subscribers 8

1.3.5 Affiliated Organizations 8

1.3.6 Relying Parties 8

1.3.7 Other Participants 8

1.4 CERTIFICATE USAGE 8

1.4.1 Appropriate Certificate Uses 8

1.4.2 Prohibited Certificate Uses 9

1.5 POLICY ADMINISTRATION 9

1.5.1 Organization administering the document 9

1.5.2 Contact Person 9

1.5.3 Person Determining CPS Statement Suitability for the Policy 10

1.5.4 CPS Approval Procedures 10

1.6 DEFINITIONS AND ACRONYMS 10

1.6.1 Definitions 10

1.6.2 Acronyms 17

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 23

2.1 REPOSITORIES 23

2.2 PUBLICATION OF CERTIFICATION INFORMATION *23*

2.2.1 Publication of Certificates and Certificate Status 23

2.2.2 Publication of CA Information 24

2.2.3 Interoperability 24

2.3 FREQUENCY OF PUBLICATION *24*

2.4 ACCESS CONTROLS ON REPOSITORIES *25*

3 IDENTIFICATION AND AUTHENTICATION **26**

3.1 NAMING *26*

3.1.1 Type of Names 26

3.1.2 Need for Names to Be Meaningful 27

3.1.3 Anonymity or Pseudonymity of Subscribers 27

3.1.4 Rules for Interpreting Various Name Forms 27

3.1.5 Uniqueness of Names 27

3.1.6 Recognition, Authentication, and Role of Trademarks 28

3.2 INITIAL IDENTITY VALIDATION *28*

3.2.1 Method to Prove Possession of Private Key 28

3.2.2 Authentication of Organization Identity 29

3.2.2.1 Authentication of Entity CAs 29

3.2.2.2 Entity CAs are established by the applicant Entity. 29

3.2.3 Authentication of Individual Identity 29

3.2.3.1 Authentication of Human Subscribers 29

3.2.3.2 Authentication of Human Subscribers For Role-based Certificates 29

3.2.3.3 Authentication of Human Subscribers For Group Certificates 29

3.2.3.4 Authentication of Devices 29

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 REQUEST 30
4 CERTIFICATE LIFE-CYCLE 32
4.1 CERTIFICATE APPLICATION 32
4.1.1 Submission of Certificate Application 33
4.1.2 Enrollment Process and Responsibilities 33
4.2 CERTIFICATE APPLICATION PROCESSING 34
4.2.1 Performing Identification and Authentication Functions 34
4.2.2 Approval or Rejection of Certificate Applications 34
4.2.3 Time to Process Certificate Applications 34
4.3 ISSUANCE 34
4.3.1 CA Actions during Certificate Issuance 34
4.3.2 Notification to Entity of Issuance of Certificate 35
4.4 CERTIFICATE ACCEPTANCE 35
4.4.1 Conduct Constituting Certificate Acceptance 35
4.4.2 Publication of the Certificate by the CA 35
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 35
4.5 KEY PAIR AND CERTIFICATE USAGE 36
4.5.1 Subscriber Private Key and Certificate Usage 36
4.5.2 Relying Party Public key and Certificate Usage 36
4.6 CERTIFICATE RENEWAL 36
4.6.1 Circumstance for Certificate Renewal 36
4.6.2 Who May Request Renewal 36
4.6.3 Processing Certificate Renewal Requests 37
4.6.4 Notification of New Certificate Issuance to Subscriber (i.e., Entity CA) 37
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 37
4.6.6 Publication of the Renewal Certificate by the CA 37
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 37
4.7 CERTIFICATE RE-KEY 37

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 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 38
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 39
4.9.2 Who Can Request Revocation 40
4.9.3 Procedure for Revocation Request 40
4.9.4 Revocation Request Grace Period 41
4.9.5 Time Within Which CA must Process the Revocation Request 41
4.9.5.1 Revocation of a Cross-Certificate Issued by the Entity CA 42
4.9.6 Revocation Checking Requirements for Relying Parties 42
4.9.7 CRL Issuance Frequency 42
4.9.8 Maximum Latency of CRLs 42
4.9.9 On-line Revocation/Status Checking Availability 42
4.9.10 On-line Revocation Checking Requirements 42
4.9.11 Other Forms of Revocation Advertisements Available 42
4.9.12 Special Requirements Related To Key Compromise 42
4.9.13 Circumstances for Suspension 43
4.10 CERTIFICATE STATUS SERVICES 43

4.11 END OF SUBSCRIPTION *43*

4.12 KEY ESCROW AND RECOVERY *43*

4.12.1 Key Escrow and Recovery Policy and Practices 43

4.12.2 Session Key Encapsulation and Recovery Policy and Practices 43

5 FACILITY MANAGEMENT AND OPERATIONAL CONTROLS 44

5.1 PHYSICAL CONTROLS *44*

5.1.1 Site Location and Construction 44

5.1.2 Physical Access 45

5.1.2.1 Physical Access for CA Equipment 45

5.1.2.2 Physical Access for RA Equipment 47

5.1.2.3 Physical Access for CSS Equipment 47

5.1.2.4 Physical Access for CMS Equipment 47

5.1.3 Power and Air Conditioning 47

5.1.4 Water Exposures 48

5.1.5 Fire Prevention and Protection 49

5.1.6 Media Storage 49

5.1.7 Waste Disposal 49

5.1.8 Off-Site backup 49

5.2 PROCEDURAL CONTROLS *49*

5.2.1 Trusted Roles 49

5.2.1.1 Administrator 50

5.2.1.2 Officer 50

5.2.1.3 Auditor 50

5.2.1.4 Operator 51

5.2.2 Number of Persons Required per Task 51

5.2.3 Identification and Authentication for Each Role 51

5.2.4 Separation of Roles 51

5.3 PERSONNEL CONTROLS *52*

5.3.1 Qualifications, Experience, and Clearance Requirements 52
5.3.2 Background Check Procedures 52
5.3.3 Training Requirements 52
5.3.4 Retraining Frequency and Requirements 53
5.3.5 Job Rotation Frequency and Sequence 53
5.3.6 Sanctions for Unauthorized Actions 53
5.3.7 Independent Contractor Requirements 53
5.3.8 Documentation Supplied To Personnel 54
5.4 AUDIT LOGGING PROCEDURES 54
5.4.1 Types of Events Recorded 54
5.4.2 Frequency of Processing Log 61
5.4.3 Retention Period for Audit Log 62
5.4.4 Protection of Audit Log 62
5.4.5 Audit Log Backup Procedures 63
5.4.6 Audit Collection System (Internal vs. External) 63
5.4.7 Notification to Event-Causing Subject 63
5.4.8 Vulnerability Assessments 63
5.5 RECORDS ARCHIVAL 64
5.5.1 Types of Records Archived 64
5.5.2 Retention Period for Archive 65
5.5.3 Protection of Archive 65
5.5.4 Archive Backup Procedures 66
5.5.5 Requirements for Time-Stamping of Records 66
5.5.6 Archive Collection System (Internal or External) 66
5.5.7 Procedures to Obtain and Verify Archive Information 66
5.6 KEY CHANGEOVER 66
5.7 COMPROMISE AND DIASTER RECOVERY 67
5.7.1 Incident and Compromise Handling Procedures 67
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 68
5.7.3 Entity (CA) Private Key Compromise Procedures 68
5.7.4 Business Continuity Capabilities After a Disaster 69

5.8 CA OR RA TERMINATION *69*

6 TECHNICAL SECURITY CONTROLS **71**

6.1 KEY PAIR GENERATION AND INSTALLATION *71*

6.1.1 Key Pair Generation 71

6.1.1.1 CA Key Pair Generation 71

6.1.1.2 Subscriber Key Pair Generation 71

6.1.2 Private Key Delivery to Subscriber 71

6.1.3 Public Key Delivery to Certificate Issuer 71

6.1.4 CA Public Key Delivery to Relying Parties 71

6.1.5 Key Sizes 72

6.1.6 Public Key Parameters Generation and Quality Checking 72

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 72

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS *72*

6.2.1 Cryptographic Module Standards and Controls 72

6.2.2 Private Key (n out of m) Multi-Person Control 73

6.2.3 Private Key Escrow 73

6.2.3.1 Escrow of Trust Infrastructure CA and Entity CA Private Signature Key 73

6.2.3.2 Escrow of CA Encryption Keys 73

6.2.4 Private Key Backup 73

6.2.4.1 Backup of Trust Infrastructure CA and Entity CA Private Signature Key 73

6.2.4.2 Backup of Subscriber Private Signature Key 73

6.2.4.3 Backup of Subscriber Key Management Private Keys 73

6.2.4.4 Backup of CSS Private Key 73

6.2.4.5 Backup of PIV-I Content Signing Key 73

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 74

6.2.8 Method of Activating Private Key 74

6.2.9 Methods of Deactivating Private Key 74
6.2.10 Method of Destroying Subscriber (i.e., Officer) Private Signature Key 74
6.2.11 Cryptographic Module Rating 74
6.3 OTHER ASPECTS OF KEY MANAGEMENT 74
6.3.1 Public Key Archival 74
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 75
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 78
6.6.3 Life Cycle Security Ratings 78
6.7 NETWORK SECURITY CONTROLS 78
6.8 TIME-STAMPING 79
7 CERTIFICATE, CRL, AND OCSP PROFILES 80
7.1 CERTIFICATE PROFILE 80
7.1.1 Version Number(s) 80
7.1.2 Certificate Extensions 80
7.1.3 Algorithm Object Identifiers 80
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 83
7.1.8 Policy Qualifiers Syntax and Semantics 83
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 83

7.2 CRL PROFILE *83*

7.2.1 Version Number(s) 83

7.2.2 CRL and CRL Entry Extensions 83

7.3 OCSP PROFILE *84*

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 85

8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT *85*

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR *85*

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY *85*

8.4 TOPICS COVERED BY ASSESSMENT *85*

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY *86*

8.6 COMMUNICATION OF RESULTS *86*

9 OTHER BUSINESS AND LEGAL MATTERS 87

9.1 FEES *87*

9.1.1 Certificate Issuance or Renewal Fees 87

9.1.2 Certificate Access Fees 87

9.1.3 Revocation or Status Information Access Fee 87

9.1.4 Fees for Other Services 87

9.1.5 Refund Policy 87

9.2 FINANCIAL RESPONSIBILITY *87*

9.2.1 Insurance Coverage 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 88

9.4 PRIVACY OF PERSONAL INFORMATION *88*

9.4.1 Privacy Plan 88

9.4.2 Information Treated as Private 88

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 89
9.5 INTELLECTUAL PROPERTY RIGHTS 89
9.6 REPRESENTATIONS AND WARRANTIES 89
9.6.1 CA Representations and Warranties 89
9.6.2 RA Representation and Warranties 89
9.6.3 Subscriber Representations and Warranties 89
9.6.4 Relying Parties Representations and Warranties 90
9.6.5 Representations and Warranties of Other Participants 90
9.7 DISCLAIMERS OF WARRANTIES 90
9.8 LIMITATIONS OF LIABILITY 90
9.9 INDEMNITIES 90
9.10 TERM AND TERMINATION 90
9.10.1 Term 90
9.10.2 Termination 90
9.10.3 Effect of Termination and Survival 90
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 91
9.12 AMENDMENTS 91
9.12.1 Procedure for Amendment 91
9.12.2 Notification Mechanism and Period 91
9.12.3 Circumstances under which OID must be changed 91
9.13 DISPUTE RESOLUTION PROVISIONS 91
9.14 GOVERNING LAW 91
9.15 COMPLIANCE WITH APPLICABLE LAW 91
9.16 MISCELLANEOUS PROVISIONS 91
9.16.1 Entire agreement 91
9.16.2 Assignment 92

9.16.3 Severability 92
9.16.4 Enforcement (Attorney's Fees or Waiver of Rights) 92
9.17 OTHER PROVISIONS 92

List of Tables

Table 1.2-1. id-fpki-certpcy Policy OIDs 3

Table 1.2-2. id-fpki-common Policy OIDs 4

Table 1.2-3. Certificate Policy OIDS Identifying the Use of SHA-1 4

Table 1.3.1-1. FPKI Roles 5

Table 2.2.2-1. FPKIPA Website 24

Table 2.4-1 FPKI Repository Addresses 25

Table 3.1.1-1. Naming Requirements Per Assurance Level 26

Table 5.1.2.1-1. FPKI Trust Infrastructure Multiple Person Control Access Matrix ..... **Error! Bookmark not defined.**

Table 5.4.1-1. Auditable Events 55

Table 7.1.3-1 FBCA Signature Algorithm OIDs 80

Table 7.1.3-2 FBCA Subject Key Algorithm OIDs 80

Table 7.1.3-3 FCPCA Signature Algorithm OIDs 81

Table 7.1.3-4 FCPCA Subject Key Algorithm OIDs 81

Table 7.1.6-1 FBCA Policy OIDs 81

Table 7.1.6-2 FCPCA Policy OIDs 83

Table 7.1.6-3 SHA1 FRCA Policy OIDs 83

RECORD OF CHANGES

CHANGE DESCRIPTION	VERSION NUMBER	DATE OF CHANGE	DATE RECEIVED	DATE ENTERED	SIGNATURE OF PERSON ENTERING CHANGE
Updated CPS to RFC 3647 Format.	2.0	2 February 2008			
Updated CPS to reflect new location of FPKI and changes made for deployment of the Target Architecture (planned deployment in September 2010).	3.0	21 May 2010			
Minor updates to CPS to clarify archiving procedures.	3.1	27 May 2010			
Updated to incorporate changes to the FBCA CP in regards to PIV-I and to enhance the description of CPS activities to meet policy.	3.2	19 July 2010			
Updated to address comments from the Day 0 Audit, September 2010.	3.3	29 September 2010			
Updated to include the SHA1 FRCA.	3.4	15 November 2010			
Combined CPS for FBCA and Common Policy into a single document. Updated to remove information for Legacy CAs and to address findings and recommendations from final Audit of Legacy CAs.	4.0	28 November 2011			

CHANGE DESCRIPTION	VERSION NUMBER	DATE OF CHANGE	DATE RECEIVED	DATE ENTERED	SIGNATURE OF PERSON ENTERING CHANGE
Revisions in response to annual PKI audit findings and recommendations. Audit conducted in January 2012.	4.1	26 March 2012			
Revisions in response to FPKI Systems Compliance Audit Report Triennial Audit Year 1 findings and recommendations. Audit conducted March 2013.	4.2	27 June 2013			
Revisions in response to FPKIPA Chair review	4.3	16 October 2013			
Updated for production site relocation	4.4	22 April 2014			
Revisions in response to FPKI Compliance Audit Report Triennial Audit Year 2 findings and recommendations. Audit conducted May 2014.	4.5	4 August 2014			
Removed sensitive information for security purposes and to allow for public dissemination of CPS	4.5 REDACTED	October 2014			

1 FPKI TRUST INFRASTRUCTURE CPS INTRODUCTION

The Federal Public Key Infrastructure Management Authority (FPKIMA) operates the certification authorities (CAs) that comprise the FPKI Trust Infrastructure. This FPKI Certification Practice Statement (CPS) documents the internal practices and procedures used by the FPKIMA for certificate lifecycle services including issuance, certificate management (including publication and archiving), revocation, and renewal or re-keying. In addition, this CPS covers the operation of systems and the management of facilities, which includes FPKI Repository functionality used to post CA certificates and certificate revocation lists (CRLs) issued by FPKI Trust Infrastructure CAs.

The scope of this CPS is limited to the three FPKI Trust Infrastructure CAs that operate in compliance with *X.509 Certificate Policy for the Federal Bridge Certification Authority* [FBCA CP] and/or *X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework* [FCPF CP]. The three FPKI Trust Infrastructure CAs covered are:

1. **The Federal Bridge Certification Authority (FBCA)** – facilitates interoperability between the PKIs of the U.S. Federal Government and other Entity PKI domains. The FBCA enables interoperability among Entity PKI domains in a peer-to-peer fashion. The FBCA issues certificates only to CAs designated by the Entity operating that PKI. FBCA certificates issued to Entity CAs act as a conduit of trust. The FBCA extends interoperability with non-federal entities only when the FPKIPA has determined it is beneficial to the Federal Government.

2. **The Federal Common Policy Certification Authority (FCPCA)** – acts as the trust anchor for the Federal Government PKI domains. The FCPCA issues certificates to Shared Service Provider (SSP)[1] CAs approved by the FPKI Policy Authority (FPKIPA). The Federal Legacy PKIs mapped to the FBCA at mediumHardware may also be approved to issue certificates in compliance with the FCPF CP. Therefore the Federal Legacy PKIs mapped to the FBCA at mediumHardware may choose to cross-certify in a peer-to-peer fashion directly with the FCPCA rather than with the FBCA. FCPCA certificates issued to Entity CAs act as a conduit of trust

3. **The SHA1 Federal Root Certification Authority (SHA1 FRCA)** – facilitates interoperability between the PKIs of the U.S. Government that were not ready to transition to SHA-256 by January 1, 2011, and other Entity PKI domains still using SHA-1. The SHA1 FRCA enables interoperability among Entity PKI domains in a peer-to-peer fashion. The SHA1 FRCA issues certificates only to Entity CAs. SHA1 FRCA certificates issued to Entity CAs act as a conduit of trust. The SHA1 FRCA was extended in response to Version 2.27 of the [FBCA CP].

[1] The SSP program is designed to facilitate outsourcing of PKI services by federal agencies.

The requirements and operation of the SHA1 FRCA match the requirements for, and operation of the FBCA[2]. The manner in which the distinction is made is via the CP object identifiers (OIDs) asserted in the certificatePolicy and policyMapping certificate extensions of the certificates issued by the SHA1 FRCA.

The internal practices and procedures to operate the FBCA and SHA1 FRCA (when issuing in an FBCA capacity) comply with the requirements, policy, and procedures set forth in [FBCA CP].

Therefore, throughout this CPS, except for Sections 1.2, 1.3.1, 3.1.1 and 6.1.5, FBCA implicitly refers to both the FBCA and SHA1 FRCA. Where the SHA1 FRCA differs from FBCA, this CPS explicitly specifies the difference.

The remaining FPKI Trust Infrastructure CAs, the E-Governance Certification Authorities (EGCA), which issue certificates only to devices, are covered by a separate CPS. Therefore, reference to "FPKI Trust Infrastructure CAs" in this CPS pertains only to FBCA, FCPCA, and SHA1 FRCA.

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

1.1 OVERVIEW

1.1.1 Certification Practice Statement

This CPS documents the practices and procedures used by the FPKIMA to operate the FBCA, FCPCA and SHA1 FRCA. Practices include the operation of systems, the FPKI Repository function, and management of facilities.

1.1.2 Relationship Between the CP and the CPS

[FBCA CP] states what assurance can be placed in certificates issued by the FBCA. [FCPF CP] states what assurance can be placed in a certificate issued by the FCPCA. This CPS states how the FPKIMA establishes that assurance.

1.1.3 Scope

The generic term "Entity" applies equally to federal organizations and other organizations owning or operating PKI domains (e.g., a PKI provided by a commercial service, or a bridge CA serving a community of interest).

An SSP is an Entity that issues Personal Identity Verification (PIV) credentials to federal users in compliance with the [FCPF CP].

This CPS covers cross-certificates issued by the FPKI Trust Infrastructure CAs to Entity CAs including SSPs CAs.

[2] The SHA1 FRCA issues cross-certificates to Entities that would otherwise cross-certify with the FBCA (but cannot because of their SHA-1 limitation).

1.1.4 Interoperation with CAs Issuing under Different Policies

Interoperation between CAs that issue under different policies is achieved through policy mapping with the FBCA CP and cross-certification after formal mapping and approval by the FPKIPA. The FCPCA is cross-certified with the FBCA and SHA1 FRCA. Legacy federal PKI CAs mapped to id-fpki-certpcy-mediumHardware may be directly cross-certified with the FCPCA instead of the FBCA. A legacy federal PKI is a PKI managed by a federal agency who received approval to cross-certify with the FBCA prior to the 12/31/2005 mandate to use SSP services. No matter which FPKI Trust Infrastructure CA issues the cross-certificate to an entity that operates in accordance to its own CP, the entity CP is mapped to the FBCA CP.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is referred to as the FPKI CPS.

The FPKI CPS supports twelve policies specified at six levels of assurance in [FBCA CP]. Each policy has an OID, to be asserted in certificates issued by the FBCA. Entity CAs may assert these OIDs in policyMappings extensions of certificates issued to the FBCA. Table 1.2-1 lists the FBCA policy OIDs registered in the NIST Computer Security Objects Registry.

Table 1.2-1. id-fpki-certpcy Policy OIDs

FBCA Policy	OID
csor-certpolicy OBJECT IDENTIFIER	::= { 2.16.840.1.101.3.2.1 }
fbca-policies OBJECT IDENTIFIER	::= { 2.16.840.1.101.3.2.1.3 }
id-fpki-certpcy-rudimentaryAssurance	::= { 2.16.840.1.101.3.2.1.3.1 }
id-fpki-certpcy-basicAssurance	::= { 2.16.840.1.101.3.2.1.3.2 }
id-fpki-certpcy-mediumAssurance	::= { 2.16.840.1.101.3.2.1.3.3 }
id-fpki-certpcy-mediumHardware	::= { 2.16.840.1.101.3.2.1.3.12 }
id-fpki-certpcy-medium-CBP	::= { 2.16.840.1.101.3.2.1.3.14 }
id-fpki-certpcy-mediumHW-CBP	::= { 2.16.840.1.101.3.2.1.3.15 }
id-fpki-certpcy-mediumDevice	::= { 2.16.840.1.101.3.2.1.3.37}
id-fpki-certpcy-mediumDeviceHardware	::= { 2.16.840.1.101.3.2.1.3.38}
id-fpki-certpcy-highAssurance	::= { 2.16.840.1.101.3.2.1.3.4 }
id-fpki-certpcy-pivi-hardware	::= { 2.16.840.1.101.3.2.1.3.18 }
id-fpki-certpcy-pivi-cardAuth	::= { 2.16.840.1.101.3.2.1.3.19 }
id-fpki-certpcy-pivi-contentSigning	::= { 2.16.840.1.101.3.2.1.3.20 }

The High Assurance policy is reserved for U.S. Federal government entity PKI operation and use.

The requirements associated with the medium-CBP (commercial best practice) policy are identical to those defined for the Medium Assurance policy with the exception of personnel security requirements (see [FBCA CP] Section 5.3.1).

The requirements associated with the Medium Hardware policy are identical to those defined for the Medium Assurance policy with the exception of Subscriber cryptographic module requirements (see [FBCA CP] Section 6.2.1).

The requirements associated with the mediumHW-CBP policy are identical to those defined for the Medium Hardware Assurance policy with the exception of personnel security requirements (see [FBCA CP] Section 5.3.1).

The requirements associated with PIV-Interoperable (PIV-I) Hardware and PIV-I Content Signing are identical to Medium Hardware except where specifically noted in the text and further described in [FBCA CP] Appendix A.

In addition, the PIV-I Content Signing policy is reserved for certificates used by the Card Management System (CMS) to sign the PIV-I card security objects.

This CPS provides substantial assurance concerning identity of certificate subjects.

Subordinate cross-certificates issued from the FCPCA in accordance with this CPS shall assert in the certificate policy extension at least one of the eight OIDs listed in Table 1.2-2.

Table 1.2-2. id-fpki-common Policy OIDs

FCPCA Policy	OID
id-fpki-common-policy	::= {2.16.840.1.101.3.2.1.3.6}
id-fpki-common-hardware	::= {2.16.840.1.101.3.2.1.3.7}
id-fpki-common-devices	::= {2.16.840.1.101.3.2.1.3.8}
id-fpki-common-authentication	::= {2.16.840.1.101.3.2.1.3.13}
id-fpki-common-High id-fpki-common-cardAuth	::= {2.16.840.1.101.3.2.1.3.16}. ::= {2.16.840.1.101.3.2.1.3.17}
id-fpki-common-devicesHardware id-fpki-common-piv-contentSigning	::= {2.16.840.1.101.3.2.1.3.36} ::= {2.16.840.1.101.3.2.1.3.39}

Certificates issued to CAs may contain any or all of these OIDs. Certificates issued to users, other than devices, to support digitally-signed documents or key management may contain id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-High.

This CPS supports the two [FCPF CP] policies specific to the Federal Information Processing Standards (FIPS) 201 PIV Card. Certificates issued to users supporting authentication but not digital signature may contain id-fpki-common-authentication. Certificates issued to users supporting authentication where the private key can be used without user authentication may contain id-fpki-common-cardAuth.

Table 1.2-3 lists the additional SHA-1 certificate policies that are asserted by the SHA1 FRCA.

Table 1.2-3. Certificate Policy OIDS Identifying the Use of SHA-1

SHA1 FRCA Policy	OID	Corresponding id-fpki-common policy

SHA1 FRCA Policy	OID	Corresponding id-fpki-common policy
id-fpki-SHA1-policy	::={2.16.840.1.101.3.2.1.3.23}	id-fpki-certpcy-mediumAssurance
id-fpki-SHA1-hardware	::= {2.16.840.1.101.3.2.1.3.24}	id-fpki-certpcy-mediumHardware
id-fpki-SHA1-devices	::= {2.16.840.1.101.3.2.1.3.25}	id-fpki-certpcy-mediumDevice
id-fpki-SHA1-medium-CBP	::= {2.16.840.1.101.3.2.1.3.21}	id-fpki-certpcy-medium-CBP
id-fpki-SHA1-mediumHW-CBP	::= {2.16.840.1.101.3.2.1.3.22}	id-fpki-certpcy-mediumHW-CBP

1.3 PKI PARTICIPANTS

The following roles are relevant to the administration and operation of the FPKI Trust Infrastructure. The responsibilities of each of the Trusted Roles are further defined in Section 5.2.1.

1.3.1 PKI Authorities

Table 1.3.1-1. FPKI Roles

FPKI Role	Description
Federal Chief Information Officers Council	The Federal CIO Council comprises the Chief Information Officers of all cabinet level departments and other independent agencies. The Federal CIO Council has established the framework for the interoperable federal PKI, and that includes overseeing the operation of the organizations responsible for governing and promoting its use. In particular, the Federal CIO Council delegates policy and practice responsibilities to the Federal PKI Policy Authority.
Federal PKI Policy Authority (FPKIPA)	The FPKIPA is a group of U.S. federal government agencies (including cabinet-level Departments) established pursuant to the Federal CIO Council. The FPKIPA includes representatives of the Agencies that execute a Memorandum of Agreement (MOA) with the FBCA and representatives of agencies that use SSP services for their PIV credentials, but have committed the resources to actively participate in the governance of the FPKI. The FPKIPA is responsible for: • [FBCA CP] and [FCPF CP]; • Approving the FPKI CPS; • Accepting applications from Entities desiring to cross-certify with the FBCA; • Determining the mappings between certificates issued by applicant Entity CAs and the levels of assurance set forth in [FBCA CP], which includes objective and subjective evaluation of the respective CP contents, and any other facts deemed relevant by the FPKIPA; • Approving the CPS for each SSP that issues certificates under [FCPF CP]; • Identifying and authenticating an Entity, as well as identifying individuals authorized to represent that Entity; • Approving the compliance audit report for each Entity CA issuing

FPKI Role	Description
	certificates under either [FCPF CP] or an Entity CP which has been mapped to [FBCA CP]; and • After an Entity is authorized to cross-certify with the FBCA or SHA1 FRCA, ensuring continued conformance of that Entity with applicable requirements as a condition for allowing continued interoperability using the FPKI Trust Infrastructure. The FPKIPA executes an MOA (an FPKIPA MOA Template is available) with an Entity setting forth the respective responsibilities and obligations of both parties, and the mappings between the certificate policy OIDs contained in [FBCA CP] and those in the Entity CP. When the Entity belongs to a sovereign nation, the United States Department of State may execute the MOA or delegate the authority to execute the MOA on its behalf.
FPKI Management Authority (FPKIMA)	The FPKIMA is the organization that operates and maintains the FPKI Trust Infrastructure CAs in accordance with the practices and procedures identified in this CPS on behalf of the U.S. Government under the General Services Administration (GSA). The FPKIMA is subject to the direction of the FPKIPA. In addition, the FPKIMA is responsible for validating that the individuals representing an Entity in the cross-certificate issuance process have been authorized by the FPKIPA.
FPKIMA Program Manager	The Program Manager is the individual within the FPKIMA who has principal responsibility for overseeing the proper operation of the FPKI Trust Infrastructure including the FPKI Repository, and selecting the FPKIMA Staff. The FPKIMA Program Manager must hold a Top Secret security clearance.
FPKIMA Trusted Roles	Individuals within the FPKIMA who operate the FPKI Trust Infrastructure CAs and the FPKI Repository, including executing FPKIPA direction to issue cross-certificates to Entity CAs from the FBCA, FCPCA, and SHA1 FRCA, or taking other action to affect interoperability between the FPKI Trust Infrastructure and Entity CAs.
Entity CA	CA within a PKI that has been designated to cross-certify directly with one of the FPKI Trust Infrastructure CAs. The Entity CA issues either end-entity certificates, or CA certificates to other Entity or external-party CAs, or both. Where the Entity operates a hierarchical PKI, the CA is typically the Entity Root CA. Where the Entity operates a mesh PKI, the CA may be any CA designated by the Entity for cross-certification with one of the FPKI Trust Infrastructure CAs. The FPKIMA issues cross-certificates to Entity CA's as authorized by the FPKIPA. This may include issuing to more than one CA for the same Entity.
Federal Bridge Certification	The FBCA is the entity operated by the FPKIMA that is authorized by the FPKIPA to create, sign, and issue public key certificates to Entity CAs. The FPKIMA is responsible for all operational aspects of the issuance and

FPKI Role	Description
Authority (FBCA)	management of cross-certificates including: • Control over the registration process; • The certificate manufacturing process; • Publication of certificates; • Revocation of certificates, • Re-key of FBCA signing material; and • Ensuring that all aspects of FBCA services and FBCA operations and infrastructure related to certificates issued under [FBCA CP] are performed in accordance with the requirements, representations, and warranties of [FBCA CP].
Federal Common Policy Certification Authority (FCPCA)	The FCPCA is operated by the FPKIMA, and authorized by the FPKIPA. The FCPCA includes the collection of hardware, software, and operating personnel that create, sign, and issue public key certificates to Subscribers. The FCPCA is responsible for the issuing and managing of certificates including: • The certificate manufacturing process; • Publication of certificates; • Revocation of certificates; • Generation and destruction of FCPCA signing keys; and • Ensuring that all aspects of FCPCA services, operations, and infrastructure related to certificates issued under [FCPF CP] are performed in accordance with the requirements, representations, and warranties of [FCPF CP].
Shared Service Provider Certification Authority (SSP CA)	An SSP CA is operated by an SSP authorized by the FPKIPA to operate under the SSP program. The SSP program is designed to facilitate outsourcing of PKI services by federal agencies.
SHA-1 Federal Root CA (SHA1 FRCA)	The SHA1 FRCA is the entity operated by the FPKIMA that is authorized by the FPKIPA to create, sign, and issue public key certificates to Entity CAs that were unable to transition to SHA-256 by January 1, 2011. The FPKIMA operates the SHA1 FRCA in the same manner as the FBCA, except that the SHA1 FRCA generates certificates and CRLs using the SHA-1 signature algorithm. In addition, the SHA1 FRCA asserts the SHA-1 certificate policies listed in Table 1.2-3, Certificate Policy OIDS Identifying the Use of SHA-1.
Certificate Status Servers (CSS)	Certificate Status Servers are not currently supported in the FPKI Trust Infrastructure.

1.3.2 Registration Authorities

The FPKIMA does not operate a Registration Authority. FPKI Trust Infrastructure CAs issue cross-certificates only to Entity CAs. The FPKIPA collects and validates the authenticity of the Entity and the identity information about the Entity organization including Point of Contact

(POC) information for those individuals authorized to act on behalf of the Entity in the cross-certification process. The FPKIMA verifies the information to be included in the cross-certificate, and validates that the individual representing the Entity matches the POC information in the Letter of Authorization (LOA) provided by the FPKIPA.

1.3.3 Card Management System (CMS)

The FPKI Trust Infrastructure has no CMS.

1.3.4 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate, who asserts that it uses its key and certificate in accordance with the CP asserted in the certificate, and who does not use it to issue certificates. CAs are sometimes technically considered "Subscribers" to a PKI. However, the term "Subscriber" as used in this CPS refers only to those who request certificates for uses other than signing and issuing certificates, or certificate status information. Therefore, the FPKIMA does not issue any Subscriber certificates from FPKI Trust Infrastructure CAs.

1.3.5 Affiliated Organizations

FPKI Trust Infrastructure CAs only issue CA certificates.

1.3.6 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. Although [FBCA CP] and [FCPF CP] contain some helpful guidance, which Relying Parties may consider in making their decisions, Relying Parties are outside the scope of this CPS and are not controlled by the FPKIPA or the FPKIMA.

1.3.7 Other Participants

FPKIMA operation of FPKI Trust Infrastructure CAs under the [FBCA CP] and [FCPF CP] requires the services of security, community, and application authorities not specifically mentioned in the CPs. The Government Information Systems Security Manager (ISSM) is assigned in writing by the appropriate GSA Designated Approving Authority (DAA), and serves as the focal point for overseeing the implementation of adequate security within the system, including ways to prevent, detect, and recover from security problems. These functions are performed through the certification and accreditation (C&A) process, and delegation of tasks to the Information Systems Security Officer (ISSO) (e.g., day-to-day monitoring of FPKIMA system security).

The ISSO is assigned in writing by the appropriate GSA DAA on the recommendation of the ISSM, and is the focal point for ensuring implementation of adequate system security in order to prevent, detect, and recover from security breaches.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

As a key critical infrastructure component, the FPKIMA operates the FPKI Trust Infrastructure CAs at a level of assurance appropriate to meet the requirements for assurance level 4

authentication, as defined by the Office of Management and Budget Memorandum M-04-04, *E-Authentication Guidance for federal Agencies* [OMB M-04-04].

The FBCA is operated at the high CP assurance level, which is equivalent to [OMB M-04-04] assurance level 4. As described in [FBCA CP], high assurance level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. This may include very high-value transactions or high levels of fraud risk. Note that the data in such transactions never traverse the FBCA infrastructure.

The FBCA is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to federal statutes and regulations. Each Entity-specific MOA identifies the level(s) of assurance associated with that Entity.

The FBCA only issues cross-certificates to Entity CAs, and issues CRLs and Certification Authority Revocation Lists (CARLs) relating to those certificates.

The FCPCA issues at least one certificate that asserts id-fpki-common-High OID, so the FCPCA is operated at the assurance level that meets the requirements for [OMB M-04-04] assurance level 4. Note that the data in such transactions never traverse the FCPCA infrastructure.

The FCPCA is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to federal statutes and regulations. Each SSP-specific MOA identifies the level(s) of assurance associated with that SSP.

The FCPCA only issues cross-certificates to SSP and legacy federal PKI CAs, and issues CRLs relating to those certificates.

1.4.2 Prohibited Certificate Uses

FPKI Trust Infrastructure CAs do not issue certificates to end-entity Subscribers, and do not restrict the usage of certificates issued by any Entity CAs. Certificates that assert id-fpki-common-cardAuth shall only be used to authenticate the hardware token containing the associated private key, and shall not be interpreted as authenticating the presenter or holder of the token.

1.5 POLICY ADMINISTRATION

1.5.1 Organization administering the document

The FPKIMA is responsible for maintaining this CPS.

1.5.2 Contact Person

Questions regarding this CPS shall be directed to the FPKIMA Program Manager, who can be reached through the e-mail address: FPKIPA-MA@listserv.gsa.gov.

1.5.3 Person Determining CPS Statement Suitability for the Policy

This CPS must conform to [FBCA CP] and [FCPF CP]. The FPKIPA is responsible for asserting whether this CPS conforms to [FBCA CP] and [FCPF CP]. The FPKIPA is also responsible for approving this CPS.

Entities must designate the person or organization that asserts that their CPS(s) conforms to their CP(s).

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.

1.5.4 CPS Approval Procedures

The FPKIMA submits the FPKI CPS and the results of a compliance audit to the FPKIPA for approval. The FPKIPA votes to accept or reject the FPKI CPS and accompanying compliance audit. If rejected, the FPKIMA Program Manager will task the required FPKIMA resources to resolve the identified discrepancies. When the resolutions are documented, a compliance audit will be conducted and the results resubmitted to the FPKIPA for review and approval.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

Access	Opportunity to make use of an information system (IS) resource. [NS4009]
Access Control	Limiting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Accrediting Authority (DAA) that an IS is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. (See security safeguards.) [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Applicant	The Subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.
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/or changes in an event. [NS4009, "audit trail"]
Authenticate	To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an IS, or to establish the validity of a transmission.
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 a specific communications terminal with a specific cryptographic key or associating two related elements of information. [NS4009]
Biometrics	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally-signed by the certification authority issuing it. [ABADSG]. As used in this CPS, the term “Certificate” refers to certificates that expressly reference one or more of the OIDs of this CPS in the “Certificate Policies” field of an X.509 v.3 certificate.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates that have been revoked.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certification Authority Software	Key Management and cryptographic software used to manage certificates.

Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in the corresponding CP, or requirements specified in a contract for services).
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Common Criteria	A set of internationally-accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Component Private Key	Private key associated with a function of the certificate-issuing equipment, as opposed to being associated with an operator or administrator.
Compromise	Type of incident where information is disclosed to unauthorized individuals or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized individuals, processes, or devices. [NS4009]

Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module	The set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation), and is contained within the cryptographic boundary. [FIPS140-2]
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Discretionary Access Control	Means of restricting access to objects based on user identity.
Duration	A field within a certificate which is composed of two subfields; "date of issue" and "date of next issue".
Employee	Any person employed by an Entity as defined below.
End-entity	Relying Parties and Subscribers.
Entity	The generic term "entity" applies equally to federal organizations and other organizations owning or operating PKI domains.
FPKI Management Authority (FPKIMA)	The FPKIMA is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the FBCA.
Federal Public Key Infrastructure Policy Authority (FPKIPA)	The FPKIPA is the federal government body responsible for setting, implementing, and administering policy decisions regarding interEntity PKI interoperability that uses the FBCA.
FPKI Trust Infrastructure	The CAs and supporting Repositories managed by the FPKIMA. In this CPS, the FPKI Trust Infrastructure refers only to the FBCA, FCPCA, and SHA1 FRCA. An additional Trust Infrastructure CA, the EGCA that issues certificates only to devices, is covered by its own CPS.
Firewall	System designed to defend against unauthorized access to or from a private network. [NS4009]

Information System Security Officer (ISSO)	Individual responsible to the ISSM for ensuring the appropriate operational IA posture is maintained for a system, program, or enclave. [NS4009]
Information System Security Manager (ISSM)	Individual responsible for a program, organization, system, or enclave's information assurance program.
Integrity	Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Key Escrow	A deposit of the private key of a Subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the Subscriber, the terms of which require one or more agents to hold the Subscriber's private key for the benefit of the Subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Letter of Authorization	Written instructions signed (manually or digitally) by the FPKIPA Chair to issue a cross-certificate to an Entity.
Memorandum of Agreement (MOA)	Agreement between the FPKIPA and an Entity allowing interoperability between the Entity CA and the FBCA.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
National Security System	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

‘‘(i) the function, operation, or use of which—
‘‘(I) involves intelligence activities;
‘‘(II) involves cryptologic activities related to national security;
‘‘(III) involves command and control of military forces;
‘‘(IV) involves equipment that is an integral part of a weapon or weapons system; or
‘‘(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions;
or
‘‘(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. ‘‘(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [FISMA]

Non-Repudiation	Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the seven policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Privacy	Restricting access to Subscriber or Relying Party information in accordance with Federal law and Entity policy.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.

Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.
Relying Party	A person or entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CPS.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Root CA	In a hierarchical PKI, the Certification Authority whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Secret Key	A “shared secret” used in symmetric cryptography, wherein users are authenticated based on a password, PIN, or other information shared between the user and the remote host or server. A single key is shared between two parties: the sender, to encrypt a transmission, and the recipient, to decrypt the transmission, with the shared key being generated with an algorithm agreed to beforehand by the transacting parties.

Server	A system entity that provides a service in response to requests from clients.
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. [NS4009]
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 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, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data. [FIPS1402]

1.6.2 Acronyms

BMS	Building Management System
CA	Certification Authority
C&A	Certification and Accreditation

[Acronym redacted for security purposes]

CARL	Certificate Authority Revocation List
CD	Compact Disc
CIO	Chief Information Officer
CISA	Certified Information System Auditor
CM	Configuration Management
CMS	Card Management System
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CPWG	Certificate Policy Working Group
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
CSS	Certificate Status Server
DAA	Designated Approving Authority
DISP	Directory Information Shadowing Protocol
DMZ	Demilitarized Zone
DN	Distinguished Name
DNS	Domain Name System
DSA	Directory Service Agent
EDP	Electronic Data Processing
EGCA	E-Governance Certification Authorities
FACP	Fire Alarm Control Panel
FBCA	Federal Bridge Certification Authority
FCPCA	Federal Common Policy Certification Authority

FCPF	Federal Common Policy Framework
FPKIMA	Federal Public Key Infrastructure Management Authority
FIPS	(US) Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOS	Full Operational Site
FPKI	Federal Public Key Infrastructure
FPKIPA	Federal PKI Policy Authority
FRCA	Federal Root Certification Authority
FTS	Federal Technology Service
GSA	General Services Administration
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HVAC	Heating, Ventilation, and Air Conditioning
ICAMSC	Identity Credentialing and Access Management Steering Committee
IETF	Internet Engineering Task Force
IPS	Information Processing System
ISC	Individual Secure Container
ISO	International Organization for Standardization
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
KVM	Keyboard-Video-Mouse
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LOA	Letter of Authorization

MA	Management Authority
MOA	Memorandum of Agreement (as used in the context of this CPS, between an Entity and the FPKIPA allowing interoperation between the FBCA and Entity CA)
N/A	Not Applicable
NARA	National Archives and records Administration
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCSP	Online Certificate Status Protocol
OEP	Occupant Emergency Plan
OID	Object Identifier
OJP	On the Job Training
OMB	Office of Management and Budget
OS	Operating System
PACS	Physical Access Control System
PDF	Portable Document Format

[Acronym redacted for security purposes]

PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Certificate Standard
PKCS#10	Public Key Certificate Standard Certificate Request
PKI	Public Key Infrastructure

POA&M	Plan of Action and Milestones
POC	Point of Contact

[Acronym redacted for security purposes]

RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SBU	Sensitive But Unclassified
SC	Secure Container
SHA	Secure Hash Algorithm
SHA-1	Secure Hash Algorithm, Version 1
SHA-256	Secure Hash Algorithm, 256 bit length
SHA1 FRCA	SHA-1 Federal Root Certification Authority
SFTP	Secure File Transfer Protocol
SIR	Security Incident Report
SKI	Subject Key Identifier
SOP	Standard Operating Procedure
SP	Special Publication
SSP	Shared Service Provider
TCP	Transmission Control Protocol
TOC	Trusted Operations Center
TSEL	Transport Selector

UPS	Uninterrupted Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
U.S.	United States
U.S.C.	United States Code
UUID	Universally Unique IDentifier
WWW	World Wide Web

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The FPKIMA operates and uses a variety of mechanisms for posting information into a Repository as required by [FBCA CP] and [FCPF CP], and further refined in *Shared Service Provider Repository Service Requirements* [SSP-REP]. The mechanisms supported and operated include:

- Maintaining an online X.500 Directory Service System supporting Lightweight Directory Access Protocol (LDAP) v3, as directed by the FPKIPA, which allows anonymous access and retrieval of the certificate information including all cross-certificates issued by and to FPKI Trust Infrastructure CAs, as well as the CRLs issued by the FPKI Trust Infrastructure;
- Maintaining an online web server which allows anonymous access and retrieval of certificate information via HTTP, including all cross-certificates issued by and to the FPKI Trust Infrastructure CAs and the status of all cross-certificates issued by the FPKI Trust Infrastructure; and
- Providing administrative access control mechanisms when needed to protect FPKI Repository information as described in later sections.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 Publication of Certificates and Certificate Status

The FPKIMA publishes information concerning FPKI Trust Infrastructure CAs as necessary to support their use and operation in the repositories described in Section 2.1. This includes

- The cross-certificates they issue and receive;
- The CRLs and CARLs they issue; and
- The certificates for their certificate signing key.

These repositories are available for anonymous access 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year, and scheduled down-time not to exceed 0.5% annually.

The FPKIMA publishes cross-certificates issued by and to the FPKI Trust Infrastructure as cross-certificate pairs in the CA Directory entry of the FPKI X.500/LDAP directories and in p7c files on the FPKI web server.

When issued, CRLs and CARLs are published to both the FPKI X.500/LDAP directories and the FPKI web server.

The availability requirements are met by the FPKIMA operating multiple sites with load balanced network traffic between the sites, and multiple servers at each site available within the local load-balanced pool.

2.2.2 Publication of CA Information

The FPKIMA will deliver this FPKI CPS to the FPKIPA and any relevant authority in the Federal Government. The FPKIMA will make a redacted version of this FPKI CPS publicly available on the FPKIPA web site.

Information, "about critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities"[3] is omitted in the publicly-available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

The FPKIPA utilizes IDManagement.gov to post FPKI-related documentation, including the [FBCA CP], [FCPF CP], the redacted version of this CPS, and FPKIPA procedural documents. The FPKIPA web server is separate from the FPKI Repositories maintained by the FPKIMA.

Table 2.2.2-1 lists the FPKIPA website that hosts the [FBCA CP], [FCPF CP], redacted CPS, and Interoperability Guidelines:

Table 2.2.2-1. FPKIPA Website

Purpose	Network Address
FPKI CPS Website	http://www.idmanagement.gov/documents/certification-practice-statement-cps-federal-bridge-and-common-policy
FBCA CP Website	http://www.idmanagement.gov/documents/certificate-policy-federal-bridge-certificate-authority
FCPF CP Website	http://www.idmanagement.gov/documents/federal-pki-common-policy-framework-certificate-authority
FBCA Interoperability Guidelines	http://www.idmanagement.gov/documents/fbca-product-interoperability-guidelines

Access to the entire CPS is granted only to Entities authorized by the FPKIPA.

2.2.3 Interoperability

The FPKI X.500/LDAP Directory, in the FPKI Repository, uses a standards-based schema for Directory objects and attributes. During the application process for cross-certification with the FBCA, the FPKIMA performs interoperability testing with the applicant Entity to ensure interoperability between the applicant's Directory and the FPKI Directory. Repository details required by the FCPCA are specified in [SSP-REP].

2.3 FREQUENCY OF PUBLICATION

Updates to [FBCA CP] or [FCPF CP] are made by the FPKIPA and published to the FPKIPA web site. Review and updates, if appropriate, are made to this CPS on an annual basis, or as needed, and are provided to the FPKIPA chair for approval. After approval, a redacted version of this CPS is provided to the FPKIPA for publication.

[3] (GSA Order 1800.3b and Draft GSA Order 1800.3c), and in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a)(i), §3544(A)(1)(a)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3545(f), as well as GSA Orders 1800.3C (draft) and PBS 3490.1

2.4 ACCESS CONTROLS ON REPOSITORIES

The FPKI repositories include an online X.500 Directory Service supporting LDAP V3 as well as Directory System Protocol (DSP) for publishing Entity CAs' cross-certificates, and CRLs issued by the FPKI Trust Infrastructure.

The FPKI Repositories include *[Redacted for Security Purposes]* web servers providing HTTP access to CRLs and certificate-only CMS message files with an extension of ".p7c" that contain cross-certificates issued to and by the FPKI Trust Infrastructure CAs.

The FPKI online repositories reside behind a firewall protecting the FPKI from the Internet. Public anonymous read access to the FPKI Directory and web servers is allowed. Only authorized FPKIMA personnel can update the information stored on these servers. Access controls are set by administrative function and assigned roles/responsibilities, and enforced using password-based authenticated subject identity.

The FPKI Trust Infrastructure CAs are enabled to generate periodic CRLs. These CRLs are published to a master X.500 Directory in the internal local area network (LAN). The master Directory pushes the CRLs to the online FPKI Directories through the internal one-way firewall via the X.500 Directory Information Shadowing Protocol (DISP). A cron job running on each public Repository server reads the CRLs from its local Directory, and updates the web server locally. Directories are protected from unauthorized modification, requiring authorized authentication in order to make updates. Anonymous access is provided via LDAP (port TCP/389) and HTTP (port TCP/80) to the public. Cross-certified PKIs are provided additional access via DSP (port TCP/102).

Table 2.4-1 provides network addresses for LDAP and X.500 Directories, as well as the FPKI Repository.

Table 2.4-1 FPKI Repository Addresses

Purpose	Network Address
LDAP v2 or better	LDAP access to repositories is: ldap.fpki.gov (port 389)
X.500 DSP	DSP access to repositories is: dsp.fpki.gov (port 102, TSEL: 1001) (Restricted to the known IP addresses of affiliate directories that use DSP.)
FPKI Repository website	HTTP access to repositories: http://http.fpki.gov/... See the site map at http://www.idmanagement.gov/sites/default/files/documents/fpki_gov_sitemap.pdf for the full URLs for all HTTP access.

3 IDENTIFICATION AND AUTHENTICATION

This Section contains the practices the FPKIMA follows in registering, identifying, and authenticating Entity CAs and sponsors involved in the certification request process.

3.1 NAMING

3.1.1 Type of Names

FPKI Trust Infrastructure CAs only generate and sign certificates that contain a non-null subject Distinguished Name (DN).

Certificates issued by the FBCA will contain the issuer DN of: C=US, O=U.S. Government, OU=FPKI, CN=Federal Bridge CA or C=US, O=U.S. Government, OU=FPKI, CN=Federal Bridge CA 2013.

Certificates issued by the FCPCA will contain the issuer DN of C=US, O=U.S. Government, OU=FPKI, CN=Federal Common Policy CA.

Certificates issued by the SHA1 FRCA will contain the issuer DN of C=US, O=U.S. Government, OU=FPKI, CN=SHA-1 Federal Root CA.

FPKI Trust Infrastructure CAs generate and sign certificates where the subject DN matches the DN of the CA identified in the LOA from the FPKIPA and the subject DN in the certificate request - Public Key Certificate Standard (PKCS)#10 - received from the Entity CA. These DNs contain X.520 naming elements (at least C, O, and OU), the domain component naming element (DC), or a combination of the two. The FPKI Trust Infrastructure CAs do only issue CA certificates.

Table 3.1.1-1summarizes the naming requirements that apply to each level of assurance.

Table 3.1.1-1. Naming Requirements Per Assurance Level

Level of Assurance	Naming Requirements
Test	The Test level of assurance is used by the test FPKI Trust Infrastructure CAs in the Community Interoperability Test Environment (CITE) and Entity test CAs when conducting interoperability testing. Production FPKI Trust Infrastructure CAs do not issue certificates with the Test level of assurance.
Rudimentary	Non-Null Subject Name, or Null Subject Name if Alternative Subject Name is populated and marked critical.
Basic	Non-Null Subject Name, and optional Alternative Subject Name if marked non-critical.
Medium (all policies)	X.500 Distinguished Name, and optional Alternative Subject Name if marked non-critical.
High	X.500 Distinguished Name, and optional Alternative Subject Name if marked non-critical.

The certificates issued to Entity CAs have an assurance level equal to the highest level of assurance contained in the policy mappings as agreed between the FPKIPA and the Entity CA.

3.1.2 Need for Names to Be Meaningful

The FBCA supports the generation and publication of cross-certificates with Entity CAs. Names used in the certificates identify the Entity CA to which they are assigned in a meaningful way. The Entity assigns the name to their CA, and the FPKIPA states that they are in agreement that the name identifies the Entity CA in a meaningful way by including it in the MOA between the Entity and the FPKIPA, and in the LOA issued to the FPKIMA.

The LOA provided by the FPKIPA and the PKCS#10 request received from the Entity CA will contain the name to be used as the subject of the certificate issued by the FPKI Trust Infrastructure CA.

FPKI Trust Infrastructure CAs issue all the Medium or High Assurance level certificates with name constraints asserted, limiting the name space of the Entity CAs to that appropriate for their domains. The appropriate name constraints will be as agreed to in the MOA between the FPKIPA and Entity, and specified in the LOA provided by the FPKIPA. Additionally, the FPKIPA may require that such constraints be implemented for the certificates issued at the Basic or Rudimentary levels if deemed appropriate.

3.1.3 Anonymity or Pseudonymity of Subscribers

The FPKI Trust Infrastructure CAs do not issue anonymous, pseudonymous, or any other Subscriber certificates.

3.1.4 Rules for Interpreting Various Name Forms

[FBCA CP] contains the rules for interpreting name forms. The FBCA certificate profile supports the DN, [RFC 822], and Domain Name System (DNS) name forms. Rules for interpreting PIV-I certificate UUID names are specified in [RFC 4122].

Rules for interpreting DN forms are specified in X.501, *Information Technology – Open Systems Interconnection – The Directory: Models.* Rules for interpreting the pivFASC-N name type are specified in [SCEPACS].

3.1.5 Uniqueness of Names

Entities are responsible for creating meaningful names that uniquely identify their CAs. The FPKIPA manages the name uniqueness for certificates issued by the FPKI Trust Infrastructure CAs by assuring the CA names provided by the Entity appropriately identifies the relationship with the Entity. Names, whether X.500 DNs or other name forms (e.g., an electronic mail address, DNS name), are approved by the FPKIPA and confirmed as being unique. Additionally, the FPKI Trust Infrastructure CAs are configured to require name uniqueness when issuing cross-certificates to Entity CAs. No other name forms other than DN and DNS naming are supported except for [RFC 822] in Subject AltName.

Each SSP CA has its own name space, which is verified for correctness during the SSP application process.

3.1.6 Recognition, Authentication, and Role of Trademarks

The FPKIPA resolves any name collisions or disputes regarding certificates issued by an FPKI Trust Infrastructure CA brought to its attention. Consistent with federal policy, the FPKIMA will not issue a certificate knowing that it infringes upon the trademark of another.

3.2 INITIAL IDENTITY VALIDATION

An Entity registration to the FBCA service is initiated by applying to the FPKIPA to obtain a cross-certificate from the FBCA to the Entity CA. This application is done using the Cross Certification Application template, which must be filled in and signed by an Entity authorized official. The application contains how the Entity proposes to map its CP certificate levels of assurance to the levels expressed in the [FBCA CP], and how the Entity's certificate profile conforms to the [FPKI-Prof], and [PIV-I-Prof] if applicable . The application also describes how the applicant Entity's PKI has been independently audited to ensure conformance by the applicant to its own CP and CPS.

The FPKIPA evaluates the application, and either accepts the policy mapping proposed by the applicant, or proposes an alternative mapping. As part of the application evaluation, the FPKI attorney vets the identity of the Entity organization and the authority of the POCs to participate in the cross-certification process on behalf of the Entity organization. If the applicant accepts the evaluated mapping, the FPKIPA executes an MOA with the applicant that reflects the respective responsibilities of the FPKIPA and the Entity along with the policy mappings. After the MOA is signed by the parties, the FPKIPA notifies the FPKIMA with an LOA to initiate the process for issuing cross-certificates to the Entity CA and establishing interoperability with the FPKI Directory.

An SSP registration to the FCPCA service is initiated by an SSP applicant submitting an application to the Shared Service Provider Working Group. The SSP applicant is evaluated following the guidelines of the *Shared Service Provider Roadmap: Navigating the Process to Acceptance* [SSP NAV]. During this process the FPKI attorney vets the identity of the SSP applicant organization and the authority of the POCs to represent the organization. Upon successful completion of the application process, the organization is added to the Certified PKI SSP List and may be listed on the Group 70 Schedule under Special Item Number (SIN) 132-61, Public Key Infrastructure (PKI) Shared Service Providers (PKI SSP) Program. After the SSP is approved, the FPKIPA notifies the FPKIMA with an LOA to initiate the process for issuing a subordinate cross-certificate to the SSP CA.

3.2.1 Method to Prove Possession of Private Key

The FPKIMA verifies that an Entity CA possesses the private key corresponding to the public key submitted with the application by using the CA application software to verify the signature on the PKCS#10 certificate request received from the Entity. The Entity should supply the subject key identifier (SKI) independently from the email or CD that contains the PKCS#10. The FPKIMA will verify that the SKI in the PKCS#10 and resulting certificate match the SKI provided by the Entity. All transactions involved in cross-certificate issuance are recorded as part of the security audit data, as described in Section 5.4.1. Shared secrets are not used.
The FPKI does not provide hardware tokens to CAs. The FPKIMA generates a certificate based on the PKCS#10, and returns the certificate as described in *FPKIMA Standard Operating Procedures Certificate Issuance*.

3.2.2 Authentication of Organization Identity

The FPKIMA issues cross-certificates to Entity CAs as authorized by the FPKIPA in an LOA. The FPKIPA authenticates the organization identity as part of the application and MOA processes. For non-government Applicants, the FPKIPA Attorney advises the FPKIPA on the legitimacy and authority of the Applicant organization and representation. The legal review may entail online research and verification of the authorization of the individual submitting the application. For non-U.S. Applicant PKIs, the Department of State is involved in the creation of an MOA or equivalent (i.e., advises the FPKIPA on the legitimacy and authority of the Applicant organization and its representation, advises on the need for an international treaty and may provide assistance in that regard).

The FPKIMA will issue certificates to SSPs as directed by the FPKIPA in an LOA. The FPKIPA will authenticate the SSP's organization identity as part of the application processes, as described in [SSP NAV].

3.2.2.1 *Authentication of Entity CAs*

3.2.2.2 Entity CAs are established by the applicant Entity.

The FPKIMA will verify that they are communicating with an Entity's authorized official by verifying that all communications are with points of contacts (POCs) listed in the LOA.

3.2.3 Authentication of Individual Identity

3.2.3.1 Authentication of Human Subscribers

The FPKI Trust Infrastructure CAs do not issue certificates to human subscribers.

3.2.3.2 Authentication of Human Subscribers For Role-based Certificates

The FPKI Trust Infrastructure CAs do not issue role-based certificates.

3.2.3.3 Authentication of Human Subscribers For Group Certificates

The FPKI Trust Infrastructure CAs do not issue group certificates.

3.2.3.4 Authentication of Devices

The FPKI Trust Infrastructure CAs do not issue certificates to devices.

3.2.4 Non-verified Subscriber Information

All information in cross-certificates issued by the FPKI Trust Infrastructure CAs match information in the LOA and the Entity PKCS#10 (an Entity can send additional extensions in the PKCS#10 that are not specified in the LOA). Extension values containing URIs in the resulting certificate are validated by FPKIMA trusted roles to ensure the extension values only include URIs that are accessible, or will be accessible when populated with the resulting certificate.

3.2.5 Validation of Authority

The FPKIMA confirms a person's authorization to act on behalf of the Entity by validating that the person is listed as a POC in the LOA. The FPKIPA validates individuals who are authorized to represent the Entity while authenticating the identity of the organization as detailed in Section 3.2.2.

3.2.6 Criteria for Interoperation

The FPKIPA determines the criteria for cross-certification with the FPKI Trust Infrastructure. See Section 1.3.1 and the *U.S. Government Public Key Infrastructure Cross-Certification Methodology and Criteria* [Crits and Methods].

Where certificates and CRLs are published in directories, standards-based schemas for FPKI Directory objects and attributes are used. Detailed information is available in technical guidance from the FPKIMA. For more information, see the FPKIPA website.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

Re-keying a certificate means that a new certificate is created that has the same characteristics and certificate policies 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 maybe a different validity period. Cross-certificates issued under this CPS to Entity CAs will have a three-year maximum validity period. Subordinate CA certificates issued under this CPS to SSP CAs will have a maximum validity period of ten years.

New cross-certificates are issued to Entity CAs by the FBCA when the FBCA re-keys (every one-half of the FBCA self-signed certificate validity period), and when Entity CAs re-key. Upon Entity CA re-key, the FPKIMA confirms with the FPKIPA that the MOA between the FPKIPA and Entity is still in good standing, and requests authorization to issue a new cross-certificate to the Entity CA. Authorization is received in the form of an LOA from the FPKIPA or a digitally-signed email from the FPKIPA Chair. Prior to issuing the LOA to the FPKIMA, the FPKIPA will verify POC information for individuals authorized to participate in the cross-certification process on behalf of the Entity. This information is verified with the individual(s) who participate in the FPKIPA on behalf of the Entity PKI.

FCPCA requires an initial registration process as defined in Section 3.2 in the event of certificate revocation.

3.3.2 Identification and Authentication for Re-key after Revocation

After a certificate has been revoked other than during a renewal or update action, the initial registration process is repeated as detailed in Section 3.2. The FPKIMA must receive a new LOA before issuing a new cross-certificate to an Entity CA.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests can come from an authorized Entity POC or the FPKIPA. Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised. Authentication of a revocation request from the FPKIPA or Entity is done by validating that the digital signature on the request is from the FPKIPA Chair or an authorized Entity POC, and is subordinate to the Entity CA. Revocation requests can also be authenticated by the FPKIMA contacting the authorized Entity POC using the POC information in the LOA.

If the revocation request comes from the Entity, the FPKIMA will notify the FPKIPA Chair, and obtain approval before performing the revocation, unless the Entity POC states that the revocation request is due to a compromise. In this case, the revocation can take place first, followed by notification to the FPKIPA.

If the revocation request comes from the FPKIPA Chair, the FPKIMA will notify the Entity using the POC information on the corresponding LOA.

4 CERTIFICATE LIFE-CYCLE

4.1 CERTIFICATE APPLICATION

The procedures an Entity should use to apply for one or more Entity CA certificates under [FBCA CP] were developed and approved by the FPKIPA. These procedures are published on the FPKIPA web site and are as follows:

1. The applicant Entity completes a Cross Certification Application template, which is signed by an Entity authorized official. The application describes how the Entity proposes to map the certificate levels of assurance present in the Entity CA CP to the levels expressed in [FBCA CP], and how the Entity certificate profile conforms to [FPKI-Prof], and [PIV-I-Prof] if applicable. The application also describes how the applicant Entity PKI will be independently audited, prior to cross-certification, to ensure conformance by the applicant to its own CP and CPS. The Entity application will include the Entity CP and CPS written in [RFC 3647] format.
2. The FPKIPA acts on the application and determines whether to issue a certificate, and enter into the MOA with the applicant Entity.
3. The FPKIPA instructs the FPKIMA to issue the certificate to the Entity CA via the LOA, signed by the FPKIPA Chair, detailing the certificate contents and entity POCs. The FPKIPA includes a compliance package with each LOA delivered to the FPKIMA for certificate issuance. The compliance package consists of the latest versions of the identity validation documentation as required in Section 3.2.
4. Based on the LOA provided by the FPKIPA, the FPKIMA team inserts the certificate contents (including policy OIDs and policy mappings) into the cross-certificate.
5. Entity CA public keys are delivered to the FPKIMA in a digitally-signed electronic certificate request (i.e., PKCS#10) message from a POC identified in the LOA via one of the following secure means:
    - Email with valid digital signature (certification path must validate up to the FCPCA or the subject CA that has been approved for cross-certification)
    - Secure File Transfer Protocol (SFTP) application
    - In-person: Identity credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License)
    - CD delivered by registered mail or courier, packaged with a memo on Entity CA letterhead identifying the appropriate CA DN and the details of the request, and signed by a POC identified in the LOA (tracking numbers are exchanged via email or telephone)
6. Identity checking and proof of possession of the private key is accomplished as described in Section 3.2.2 and Section 4.3.1.
7. When two-way cross-certification is authorized in the LOA, the Entity authorized official can request that the FPKIMA issue the Entity CA a PKCS#10 from the FPKI Trust Infrastructure CA prior to the Entity authorized official sending the Entity CA PKCS#10 to the FPKIMA.

The application process for an SSP under [FCPF CP] is slightly different. Following successful completion of the application process by an applicant and subsequent approval by the FPKIPA,

upon FPKIPA request, the FPKIMA Administrator requires the following in order to issue a FCPCA cross-certificate to the applicant:

- A completed and signed LOA and compliance package from the FPKIPA Chair indicating the Entity has completed the Identity Proofing requirements in accordance with [SSP NAV];
- A letter requesting issuance of the certificate. The letter is on SSP letterhead, signed by the SSP authorized official;
- Validation that the POCs listed in the Entity letter are the same ones in the LOA issued and signed by the FPKIPA;
- The SSP CA's public key sent in a digitally-signed PKCS#10, whereupon possession of the private key will be verified by the FCPCA via authenticating the signature on the PKCS#10; and
- Verification that the information to be included in the certificate matches the information specified in the LOA from the FPKIPA.

The above, performed in any order convenient for the FPKIMA and FPKI-approved applicants as long that does not defeat security, are completed before any subordinate SSA CA certificate issuance. All communication between the FPKIMA and Affiliate or SSP supporting the certificate application and issuance process is via an out-of-band secure mechanism such as FedEx, secure File Transfer Protocol (SFTP), or digitally-signed email or PDF documents.

After a certificate is issued by the FPKIMA, it is manually checked to ensure each field and extension is populated with the correct information before it is delivered to the Entity CA and before it is posted in the FPKI Repository.

The FPKI Trust Infrastructure CAs operated under this CPS do not issue end-entity certificates.

4.1.1 Submission of Certificate Application

An Entity authorized official submits the certificate application to the FPKIPA, following the instructions found at http://www.idmanagement.gov/criteria-and-methodology.

4.1.2 Enrollment Process and Responsibilities

Entities applying for cross-certification are responsible for providing accurate information on their certificate applications.

All communication among PKI Authorities supporting the certificate application and issuance process are authenticated and protected from modification. Communications may be electronic or out-of-band. Communications may be via digitally-signed email, SFTP, or out-of-band. When electronic communications are used digital signatures are used to authenticate the identity of the signer and detect modifications. When digital signature is not available, POC information supplied in the LOA is used to authenticate Entity officials. When FedEx or other physical means of transit are used, tracking numbers are exchanged via email or telephone. If passwords or shared secrets are used to protect electronic communications, they will be communicated in-person or via other out-of-band mechanisms.

4.2 CERTIFICATE APPLICATION PROCESSING

The FPKIPA verifies that information in certificate applications is accurate before certificates are issued. The process of verifying the information is detailed in the [Crits and Methods]. The process includes mapping CPs, technical testing, and verification of information with the Entity POC for cross-certificates. For subordinate CA certificates, information is verified with the SSP POC. The verified information is provided to the FPKIMA in the form of an LOA.

The FPKIMA Administrator verifies that the information in the LOA is consistent with information contained in the MOA for Entities cross-certifying with the FPKI Trust Infrastructure.

The FPKIMA verifies the information in cross-certificates issued by the FPKI Trust Infrastructure CAs against the information specified in the LOA.

The FPKIMA verifies the information in cross-certificates issued by Entities to the FPKI Trust Infrastructure CAs against the information specified in the MOA.

4.2.1 Performing Identification and Authentication Functions

The FPKIPA performs identification and authentication of the applicant Entity following the procedures detailed in [Crits and Methods] or during the SSP acceptance process, and sends Entity POC information in the form of an LOA to the FPKIMA. The FPKIMA only corresponds with those POCs listed in the LOA, or as directed by the listed POC.

4.2.2 Approval or Rejection of Certificate Applications

The FPKIPA may approve or reject a certificate application.

4.2.3 Time to Process Certificate Applications

The time to process FBCA certificate applications requires completion of the following steps (1) perform Entity CP to [FBCA CP] mapping to determine the appropriate policy mappings, (2) perform technical testing, (3) FPKIPA vote to approve the Entity's application, (3) obtain a signed MOA between the FPKIPA and the Entity, and (4) the FPKIPA provides an LOA to the FPKIMA.

The time to process FCPCA certificate applications requires completion of the following steps (1) the SSPWG approves the SSP application and (2) the FPKIPA votes to approve the SSP, and (3) the FPKIPA provides an LOA to the FPKIMA.

The FPKIMA will process and issue certificates within 30 days of receipt of a signed LOA and the digitally-signed certificate request file from a POC identified in that LOA, via a secure delivery method verifying the identity of that POC.

4.3 ISSUANCE

4.3.1 CA Actions during Certificate Issuance

The FPKIMA issues cross-certificates to the Entity CA by the following procedure:

1. Upon receiving a signed request message (PKCS#10 message) from the Entity CA, the designated FPKI Trust Infrastructure CA software verifies the signature to prove possession of the private key. Then, after all requirements criteria have been satisfied,

the FPKI Trust Infrastructure CA will sign and issue the cross-certificate to the Entity CA.

2. Each certificate issued by the FPKIMA is manually checked to ensure each field and extension is populated with the correct information, before the certificate is delivered to the Entity CA.
3. The certificate issued by the FPKIMA will be delivered to the Entity CA in a p7b file, via secure means (e.g., CD delivered by registered mail or courier or digitally-signed email).
4. If two-way cross-certification is authorized:
    a. The FPKI Trust Infrastructure CA will generate a digitally-signed certificate request message and deliver it to the Entity CA in a PKCS#10 certificate request message, via secure means (e.g., CD delivered by registered mail or courier or digitally-signed email).
    b. The Entity CA will sign and issue a certificate to the FPKI Trust Infrastructure CA and deliver it to the FPKIMA in a p7b file, via secure means (e.g., CD delivered by registered mail or courier or digitally-signed email).

The FPKIMA will post cross-certificates in the FPKI Directory as cross-certificate pairs, and in p7c files on the HTTP web server. In the case of two-way cross-certificates, both cross-certificates are posted in the FPKI Directory as a single cross-certificate pair.

FPKI Trust Infrastructure CAs do not generate Subscriber private keys and are never in possession of Entity CA private signature keys.

4.3.2 Notification to Entity of Issuance of Certificate

The FPKIMA sends an email to the Entity POC and FPKIPA-MA@listserv.gsa.gov, providing the tracking number if an issued certificate is being sent via courier. If the issued certificate is sent via signed email, a second email specifying the date, time, sender, and recipient(s) of the signed email is sent to the Entity POC, the FPKIPA Chair, and the FPKIPA-MA@listserv.gsa.gov.

4.4 CERTIFICATE ACCEPTANCE

The MOA specifies responsibilities an Entity and the FPKIPA must perform before the FPKIPA can authorize issuance of an FPKI Trust Infrastructure cross-certificate to the Entity CA. Once a cross-certificate has been issued and accepted by the Entity, interoperability with the FPKI Trust Infrastructure begins when directory chaining between the Entity CA Directory and the FPKI Directory has been configured, as appropriate. This begins the Entity's obligations under the MOA and this CPS.

4.4.1 Conduct Constituting Certificate Acceptance

For the FPKI Trust Infrastructure, failure to object to the requested certificate or its contents constitutes acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

As specified in Section 2.2.1, all cross-certificates are published in FPKI and Entity Repositories.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The FPKIPA is notified of newly-issued cross-certificates on a monthly basis. In addition, the FPKIMA notifies the FPKI community via an email to the FPKIPA@listserv.gsa.gov and

FPKIPA_Customers@listserv.gsa.gov when it learns that an Entity has published newly-issued cross-certificates to the Entity's Repositories.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

FPKI Trust Infrastructure CAs do not issue subscriber certificates.

4.5.2 Relying Party Public key and Certificate Usage

Certificates issued by FPKI Trust Infrastructure CAs specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. The FPKI Trust Infrastructure CAs issue CRLs specifying the current status of all unexpired certificates issued by FPKI Trust Infrastructure CAs. It is recommended that Relying Parties process and comply with this information whenever using FPKI certificates in a transaction. However, enforcement of that recommendation is outside the scope of this CPS.

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the subject name and attributes are unchanged. The new validity period of the renewed certificate will not extend past the maximum lifetime of the original certificate (six years for the FBCA self-signed certificate, three years for an FBCA cross-certificate, twenty years for the FCPCA self-signed certificate, and ten years for an SSP subordinate cross-certificate). Certificates may also be reissued when a CA re-keys.

If the FBCA or FCPCA performs a key rollover, the FPKIMA will issue renewed certificates for all issued cross-certificates.

4.6.2 Who May Request Renewal

For the FBCA, the Entity or FPKIMA may request renewal of an Entity CA's cross-certificate.

An Entity CA may perform renewal of its cross-certificate with the FBCA without a corresponding request, such as when the CA re-keys by signing the previous PKCS#10 and sending the resulting certificate by agreed-upon means to the FPKIMA. Alternatively, the FPKIMA may request a renewal of the FBCA cross-certificate from the Entity CA, by sending a new PKCS#10 by agreed-upon means to the Entity.

For all Entity CAs operating under [FCPF CP], the Entity authorizing official may request renewal of its own certificate. For the FCPCA, the FPKIMA may also request renewal of FPKI Trust Infrastructure CAs certificates. For the FCPCA, certificate renewal for reasons other than re-key of the FCPCA or Entity CA is approved by the FPKIPA issuing a new LOA or confirming authorization by a digitally-signed email from the FPKIPA Chair. The procedures to issue a certificate renewal are the same as for issuing a new certificate (see Section 4.3.1).

For Entities with a cross-certificate from the SHA1 FRCA, the corresponding operating authority may request renewal of its own.

4.6.3 Processing Certificate Renewal Requests

Certificate renewal for reasons other than re-key of the FBCA, FCPCA, or Entity CA is approved by the FPKIPA issuing a new LOA or confirming authorization by a digitally-signed email from the FPKIPA Chair. The procedures to issue a certificate renewal are the same as for issuing a new certificate (see Section 4.3.1).

4.6.4 Notification of New Certificate Issuance to Subscriber (i.e., Entity CA)

Upon issuance of new cross-certificate to an Entity, the FPKIMA notifies Entity POCs using the same procedures as with notification of original certificates (see Section 4.3.2).

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Failure to object to a certificate issued by an FPKI Trust Infrastructure CA constitutes acceptance of the certificate.

4.6.6 Publication of the Renewal Certificate by the CA

All CA cross-certificates are published in the FPKI and Entity Repositories (see Section 2.2.1).

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of certificate issuance is provided to all cross-certified Entities via the Monthly Statistics Report to the FPKIPA.

4.7 CERTIFICATE RE-KEY

Re-keying a certificate means that a new certificate is created that has the same characteristics and certificate policies as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period. FBCA cross-certificates issued under this CPS to Entity CAs have a three-year maximum validity.

After certificate re-key, the old certificate is revoked.

4.7.1 Circumstance for Certificate Re-key

New cross-certificates need to be issued to Entity CAs by the FPKI CA when the FPKI CA re-keys (every one-half of the FPKI CA self-signed certificate validity period), and when Entity CAs re-key.

4.7.2 Who May Request Certification of a New Public Key

After the FBCA or FCPCA performs a re-key, the FPKIMA issues a request for a new cross-certificate (PKCS#10) from each Entity CA currently two-way cross-certified with the FBCA or FCPCA[4].

After an Entity CA performs a re-key, an Entity authorized official issues a request for a new cross-certificate (PKCS#10) from the FPKI Trust Infrastructure CA.

[4] Fed legacies are allowed to directly, two-way cross-certify with FCPCA.

4.7.3 Processing Certificate Re-keying Requests

The Entity CA's authorized officials are authenticated for the purpose of re-keying in the same manner as was used for the initial application. The FPKIMA will verify that the individuals named in the LOA are still current. Additionally, the FPKIMA verifies with the FPKIPA that the MOA between the FPKIPA and the Entity remains in good standing by receiving a new LOA from the FPKIPA or a digitally-signed email from the FPKIPA Chair confirming authorization to issue the certificate to the Entity CA.

4.7.4 Notification of New Certificate Issuance to Subscriber

The FPKIMA notifies designated Entity POCs upon issuance of new certificates following the same procedures as notifying the Entity of issuance of a new certificate (see Section 4.3.2),

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

For the FPKI Trust Infrastructure, failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.7.6 Publication of the Re-keyed Certificate by the CA

As specified in Section 2.2.1, all CA cross-certificates will be published in FPKI and Entity Repositories.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of certificate issuance is provided to all cross-certified Entities via the Monthly Statistics Report to the FPKIPA

4.8 MODIFICATION

Certificate modification consists of creating new certificates with subject or extension information (e.g., a name or email address) that differs from the old certificate. The new certificate may have the same or different subject public key.

After certificate modification, the old certificate is revoked.

4.8.1 Circumstance for Certificate Modification

For cross-certificates issued by the FPKI Trust Infrastructure, certificate modification is performed if an authorized Entity POC requests a new cross-certificate because of a change to the CA name or if there is a need to correct extension information.

4.8.2 Who May Request Certificate Modification

The FPKIMA or authorized POCs for the Entity CA may request certificate modification for currently cross-certified Entity CAs by sending a digitally-signed email or by using POC information from the LOA or MOA. The FPKIPA may request a certificate modification by providing a new LOA to the FPKIMA.

4.8.3 Processing Certificate Modification Requests

The FPKIMA performs certificate modification at the direction of the FPKIPA. The FPKIMA may also perform certificate modification at the request of the Entity CA for the following reasons:

- Modification of the subjectInfoAccess (SIA) extension;

- Minor name changes (e.g., change CA1 to CA2) as part of key rollover procedures; or
- If an error is discovered in a cross-certificate.

If a certificate is modified to make a correction, the new certificate validity period retains the expiration date of the certificate being corrected. If the modification is directed by the FPKIPA, the LOA states any limitation on the validity period; if it does not, the default validity period of 3 years is used. Whenever the FPKIPA approves a new certificate for a currently cross-certified Entity, the FPKIPA and Entity perform a review of the current MOA for necessary corrections.

It is understood that modifying the certificate involves revoking the old certificate prior to issuing the new certificate. If the modification of the certificate is approved, so is the revocation of the old certificate.

Either a new PKCS#10 or the previous PKCS#10 can be used to process a certificate modification request.

4.8.4 Notification of New Certificate Issuance to Subscriber

The FPKIMA notifies designated POCs of the Entity upon issuance of new certificates, following the same procedures as in section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

For the FPKI Trust Infrastructure, failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.8.6 Publication of the Modified Certificate by the CA

As specified in Section 2.2.1, all CA cross-certificates are published in the FPKI and Entity repositories.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of certificate issuance is provided to all PKI entities in the FPKI in a monthly report to the FPKIPA.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

FPKI Trust Infrastructure CAs issue CRLs covering all unexpired certificates. These CRLs are published in publicly-available repositories, accessible both by HTTP and anonymous LDAP. The crlDistributionPoint (CDP) extension in certificates include at least one URI indicating a location to find the current CRLs. In addition, the FPKIPA web site contains a site map that provides the HTTP locations of the latest CRLs. FPKI Trust Infrastructure CAs do not issue OCSP responder certificates. Any [FBCA CP] or [FCPF CP] requirements related to OCSP operations are not applicable to the FPKI Trust Infrastructure CAs.

FPKI Trust Infrastructure CAs authenticate revocation requests. Revocation requests may be authenticated using the private key associated with the certificate to be revoked, regardless of whether or not the private key has been compromised.

4.9.1 Circumstances for Revocation

There are four circumstances where certificates issued by an FPKI Trust Infrastructure CA can be revoked:

1. When the FPKIPA requests that a certificate issued by the FPKI Trust Infrastructure be revoked. This will be the normal mechanism for revocation in cases where the FPKIPA determines that an Entity PKI does not meet the FPKI policy requirements or certification of the Entity PKI is no longer in the best interest of the federal government;
2. When the FPKIMA receives an authenticated request for revocation[5] of a certificate issued by the FPKI Trust Infrastructure to an Entity from a previously-designated Entity authorized official; or
3. When FPKIMA personnel determine that an emergency (such as compromise of the Entity CA private key) has occurred that may impact the integrity of the certificates issued by the FPKI Trust Infrastructure. Under such circumstances, the following entities may authorize immediate certificate revocation:
    - FPKIPA Chair;
    - Identity Credentialing and Access Management Subcommittee (ICAMSC);
    - FPKIMA Program Manager; or
    - As designated by the FPKIPA.
4. When a certificate has been made obsolete. This can occur when a modified certificate has been requested or an error is discovered in a certificate resulting in the FPKIMA issuing a correct certificate and revoking the certificate with the error.

4.9.2 Who Can Request Revocation

A cross-certificate issued by the FPKI Trust Infrastructure to an Entity CA is revoked (1) upon direction of the FPKIPA, (2) upon an authenticated request by a previously designated Entity authorized official (officials are specified in the MOA and/or LOA as authorized to make such a request), or (3) when the FPKIMA personnel determine that an emergency has occurred that may impact the integrity of the certificates issued by the FPKI Trust Infrastructure (see Section 4.9.1).

Requests are verified by validating the digital signature on a digitally-signed email or PDF file, and by contacting an Entity POC using POC information on the associated LOA.

Cross-certificates are also revoked after a modified cross-certificate is issued and accepted by the Entity POC. Permission to issue the modified certificate provides permission to revoke the obsolete cross-certificate (no additional authorization is required).

4.9.3 Procedure for Revocation Request

When the revocation request is not due to a perceived emergency, the revocation can be at a time mutually-agreed upon by the Entity authorized official and the FPKIMA. Revoked certificates are included on all new publications of the certificate status information until one CRL posting period past the expiration date of the cross-certificate.

The FPKIMA posts the CRL to the FPKI Repository (see Section 2.2.1) within 6 hours of the revocation. Certificates are removed from the CRL and/or CARL after the expiration date of the cross-certificate. However, the revoked certificate must appear on at least one published CRL and/or CARL past the expiration date of the cross-certificate.

The FPKIMA will review all revocation requests to ensure that the revocation requests are legitimate and will then revoke the certificate, as follows:

---

[5] The FPKIMA authenticates a request for revocation by verifying the digital signature on the request or using POC information from the LOA to contact authorized officials of the Entity and/or the FPKIPA, as appropriate.

1. An Entity authorized official or the FPKIPA drafts an authenticated request to revoke a certificate. The individual may notify the FPKIMA Administrative Help desk via phone as well as submit the request via signed e-mail to FPKIPA-MA@listserv.gsa.gov identifying the certificate to be revoked, explaining the reason for revocation
2. Upon receipt of a signed revocation request, the FPKIMA authenticates the request by verifying the digital signature and making direct contact (call back or challenge/response telephone conversation) with the Entity POC (or the FPKIPA).
3. In the event the request to revoke originates from the Entity CA, the FPKIMA apprises the FPKIPA of the request for revocation.
4. The FPKIPA evaluates and verifies the need for revocation expressed in the authenticated request. If the revocation request appears to be valid, the FPKIPA will direct the FPKIMA to proceed with revocation.
5. The FPKIMA will revoke the certificate, which automatically generates and adds a CRL entry for that certificate within 6 hours of notification of approval by the FPKIPA, or at a mutually agreed upon time.
6. The FPKIMA ensures the new CRL is posted in the FPKI Repository within 6 hours of certificate revocation.
7. The Entity CA also revokes the certificate issued to the FPKI Trust Infrastructure and generates and posts a new CARL/CRL.

The FPKIMA may affect revocation of a certificate prior to notification and approval of the FPKIPA by following emergency revocation procedures consisting of the following steps:

1. Notify all identified POCs in the emergency list of FPKIMA (i.e., FPKIMA POC, Entity POCs, CPWG POC). This can be done by either:
    - Telephone (using one of call-back or challenge/response protocols);
    - Signed FAX; or
    - Signed e-mail.
2. Revoke the cross-certificate and post the new CRL.

Once the incident has been investigated and documented, issue a new cross-certificate to replace the one that has been revoked, if directed by the FPKIPA.

4.9.4 Revocation Request Grace Period

There is no revocation grace period for the FPKI Trust Infrastructure. The FPKIMA will revoke certificates as quickly as practical upon receipt of a proper revocation request, or at an agreed time as long as the revocation is not due to a compromise. When the revocation request is due to a compromise, the request will be processed before the next CRL is published, except for those requests received within 2 hours of CRL issuance. Revocation requests for compromise received within 2 hours of CRL issuance are processed before the following CRL is published.

4.9.5 Time Within Which CA must Process the Revocation Request

Revocation of an FPKI Trust Infrastructure CA-issued cross-certificate is accomplished by the generation and publication into the FPKI Repository of a CRL citing the cross-certificate as revoked. The updated CRL is posted within 6 hours of notification of approval by the FPKIPA, or at an agreed upon time, or in accordance with emergency procedures provided in Section 4.9.3.

Further, and separate from the publication of the CRL, prompt oral and/or electronic notification is given by the FPKIMA to all Entity POCs.

4.9.5.1 Revocation of a Cross-Certificate Issued by the Entity CA

Revocation takes effect upon the publication of status information for the cross-certificate issued to an FPKI Trust Infrastructure CA. Information about a revoked cross-certificate remains in the status information (CRL) until after the cross-certificate expires.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying parties should never place any assurance in FPKI certificates that have not been validated against valid revocation status data. Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.9.7 CRL Issuance Frequency

To ensure timeliness of information, FPKI Trust Infrastructure CAs issue CRLs upon every revocation update and every 12 hours (with an 18 hour nextUpdate field) even if there are no changes to be made. Certificate status information is posted within 6 hours of revocation or immediately in accordance with emergency revocation procedures provided in Section 4.9.3. The current CRL will be removed and replaced with the updated CRL.

4.9.8 Maximum Latency of CRLs

There are automated processes running to post CRLs when generated to the FPKI repositories. CRLs are posted initially to the Master Directory Service Agent (DSA) at each Full Operational Site (FOS) and then using X.500 Directory Information Shadowing Protocol (DISP) are shadowed to all publicly-available DSAs. On each public DSA server, a cron job pulls current CRLs from its local DSA and updates the web server location for HTTP access as well (see Section 4.9.7). These automated processes ensure CRLs are published well within the required 4 hours of generation.

4.9.9 On-line Revocation/Status Checking Availability

The FPKIMA has no current plans to support the Online Certificate Status Protocol (OCSP) capability for its cross-certificates.

4.9.10 On-line Revocation Checking Requirements

The FPKI Trust Infrastructure does not provide on-line revocation status checking services other than posting CRLs.

4.9.11 Other Forms of Revocation Advertisements Available

The FPKI Trust Infrastructure does not support any other forms of revocation advertisements.

4.9.12 Special Requirements Related To Key Compromise

In the event of an Entity CA private key compromise or loss, a CRL is published by the FPKIMA as soon as possible and always within 6 hours of notification of approval by the FPKIPA for a Entity CA cross-certified at High, 18 hours for an Entity CA cross-certified at Medium, or within 24 hours for an Entity CA cross-certified at Basic, in accordance with procedures described in Section 4.9.3.

If one of the FPKI Trust Infrastructure CA keys is compromised, the FPKIMA will notify the FPKIPA and authorized officials of Entity CAs. The compromised root certificate will be added to the CRL and a CRL either with no nextUpdateTime or a nextUpdateTime of the expiration time of the root certificate will be posted. Additionally, if the FCPCA key is compromised, all vendors with agreements to distribute the FCPCA root certificate in their commercial trust stores will be notified.

If directed by the FPKIPA a replacement CA root certificate and key pair will be generated and all cross-certified or subordinate Entity CAs of the compromised CA will be issued new certificates. The new root certificate and new cross-certificates will be securely distributed to all Entity CAs.

4.9.13 Circumstances for Suspension

Suspension is not used by the FPKI Trust Infrastructure.

4.10 CERTIFICATE STATUS SERVICES

The FPKI Trust Infrastructure does not provide a Certificate Status Service other than posted CRLs.

4.11 END OF SUBSCRIPTION

The FPKIMA will notify Entity POCs of the pending expiration of a cross-certificate thirty (30) days prior to the expiration of that cross-certificate. If an authorized Entity POC does not initiate the process to request a new cross-certificate the relationship terminates when the cross-certificate expires.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

The FPKIMA does not perform any encryption key recovery functions involving Entity CAs, and does not store any information encrypted by the FPKI Trust Infrastructure CAs private keys that may require key recovery capabilities. Therefore, key escrow and recovery is not used by the FPKI Trust Infrastructure.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

The FPKI Trust Infrastructure does not perform any session key encapsulation recovery functions; no subscriber key management keys are issued or used within the FPKI Trust Infrastructure.

5 FACILITY MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

The FPKIMA imposes physical security requirements that provide the protections specified below. All physical control requirements apply to all FPKI Trust Infrastructure CAs.

The FOS-W and FOS-E sites adhere to the [NIST SP 800-53] Physical and Environmental controls commensurate with the impact level of the FPKI Trust Infrastructure, which include control of physical access points to the facility where the information system resides and verifying individual access authorizations before granting access to the facility.

For FOS-E, the facility Network Operations Center (NOC) immediately notifies the FPKIMA team in the event of any incident that could impact facility operations or procedures, or the operation of the FPKI. For FOS-W, the facility management immediately notifies the FPKIMA team in the event of any incident that could impact facility operations or procedures, or the operation of the FPKI.

FPKI Trust Infrastructure CAs are protected from unauthorized access while the cryptographic module is installed and activated. The cryptographic module activation information is stored in the *[Redacted for Security Purposes]* individual security bags. By design, all FPKI Trust Infrastructure CA equipment stays activated, but is stored in the safe when the equipment is not activated (e.g., when equipment is damaged or inoperable). Inoperable or damaged equipment that cannot be stored in the safe will remain in the locked CA IPS security container until it is either restored to operation on site, or sanitized and shipped out for service or disposal.

At FOS-W, FPKI Trust Infrastructure CA equipment is housed in a locked GSA *[Redacted for Security Purposes]*/NSA approved Information Processing System (IPS) security container within a locked cage with multiple additional controlled access points located in a locked room inside a locked data center. At FOS-E, FPKI Trust Infrastructure CA equipment is housed in another locked GSA *[Redacted for Security Purposes]*/NSA approved Information Processing System (IPS) security container within a locked cage with multiple additional controlled access points within a locked data center.

5.1.1 Site Location and Construction

[Redacted for Security Purposes] The FOS-W Site is located at:

[Redacted for Security Purposes]

At all times, all personnel gaining access to the facility must pass through the building's security checkpoint. GSA issues PIV cards that are used for GSA building access to all FPKIMA personnel. The contractor-owned data centers issue contractor-controlled badges to FPKIMA personnel for access to those facilities. *[Redacted for Security Purposes]* are granted authorization for building access through a contractor-owned PACS system. Only *[Redacted for Security Purposes]* are granted cage access through those same PACS systems. All other personnel must be accompanied by *[Redacted for Security Purposes]* and must sign a Visitor or Personnel Sign-in Log.

[Redacted for Security Purposes] The FOS-E Site is located at:

[Redacted for Security Purposes]

At all times, all personnel gaining access to the facility must pass through the building's security checkpoint. FPKIMA personnel receive data center B badges. Only *[Redacted for Security Purposes]* have access to keys for the locked cage housing the FPKI systems.

These sites are consistent with facilities used to house high value, sensitive information consistent with the required physical access controls described in *FPKI Security Controls Profile of Special Publication 800-53, Security Controls in PKI Systems* [FPKI Security Profile].

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

FPKI Trust Infrastructure equipment is always protected from unauthorized access. Physical access controls are implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated.

Physical and environmental protection policies and procedures have been developed and documented, and are reviewed and updated biennially in accordance with the physical and environmental protection security controls outlined in [NIST SP 800-53]. See *FPKI Trust Infrastructure System Security Plan* [FPKI SSP], "Physical and Environmental Protection" security control section for more details.

FPKI Trust Infrastructure CAs are secured in a two-person control manner. A locked CA IPS security container houses the FPKI Trust Infrastructure CA Servers. The two-person control is attained by separation of access responsibilities: *[Redacted for Security Purposes]* has access to the cage, while *[Redacted for Security Purposes]* has access to the CA IPS security container. The combination of the two individuals is required to access the critical system providing two-person control. The *[Redacted for Security Purposes]* present whenever the CA IPS security container is accessed sign Secured Rack Access Log, which is checked by the auditor during the *[Redacted for Security Purposes]* audits and retained as part of the logs available during the annual PKI Compliance audit. The keyboard-video-mouse (KVM) that is used to access the FPKI Trust Infrastructure CA server is also housed in the locked CA IPS security container, which requires the same two-person control. Using a site-to-site VPN between the FOS-W and FOS-E sites, at the FPKI Trust Infrastructure CA subnet level, an equivalent KVM at the other site can be used to access the FPKI Trust Infrastructure CAs at that other site. Both the *[Redacted for Security Purposes]* must remain in the cage while access to FPKI Trust Infrastructure CAs is unlocked. The *[Redacted for Security Purposes]* is never left in the FPKI cage without escort.

The *[Redacted for Security Purposes]* are required to enable the *[Redacted for Security Purposes]* for use with the CAs, thereby providing multi-person control.

All access into and out of the FPKI cage is recorded in the PACS and/or a manual log. The persons accessing the FPKI Trust Infrastructure CAs record the event in both the FPKI cage access log and in the Secured Rack Access Log.

At both locations, every individual gaining access to the facility must pass through the facility's security checkpoint.

At FOS-W, this includes a cage door contact sensor, electronically monitoring the cage housing the CAs for any intrusions (authorized or unauthorized) at all times. The PACS system at FOS-W also logs successful and failed cage access attempts. Contractor-operated cameras are monitored at all server room entry and exit points.

At FOS-E, the facility security guards monitor the entire campus manually and electronically (via video recorders), including the building housing the CAs, for any intrusions (authorized and unauthorized) at all times. The FOS-E cage has the same cage door contact sensor, electronically monitoring the cage housing the CAs for any intrusions (authorized or unauthorized) at all times.

Access to the FPKI Trust Infrastructure CAs and private signing keys requires multi-person access. When not in use, the *[Redacted for Security Purposes]* is stored in a security container. In addition to the CA IPS security containers at each site, there are three security containers (SCs) used for storage of sensitive materials in FPKI operations: *[Redacted for Security Purposes]*. Only *[Redacted for Security Purposes]* have access to SC1 and SC3. The combination to the SC2 *[Redacted for Security Purposes]* is known only to *[Redacted for Security Purposes]*.

[Redacted for Security Purposes]

Only *[Redacted for Security Purposes]* have the combination to SC2. However, it is housed in a room only accessible to *[Redacted for Security Purposes]*.

Designated FPKI roles *[Redacted for Security Purposes]* are the only personnel with unescorted access to the FPKI Trust Infrastructure cage. *[Redacted for Security Purposes]* are the only personnel with access to the FOS security containers. *[Redacted for Security Purposes]* are the only personnel with access to the *[Redacted for Security Purposes]* security bags, but only the *[Redacted for Security Purposes]* have access to the locked CA IPS security container. *[Redacted for Security Purposes]* are the only personnel that have OS accounts. *[Redacted for Security Purposes]* are the only personnel that have CA *[Redacted for Security Purposes]* accounts.

Error! Reference source not found. summarizes the separation of roles and physical allocation.

[Redacted for Security Purposes]

At least two individuals are assigned for each FPKI Trusted Role (Auditor, Officer, Administrator, and Operator). *[Redacted for Security Purposes]* is the only FPKI role that has access to FPKI Trust Infrastructure CA signing functions and must be accompanied by *[Redacted for Security Purposes]*.

Automatic logs are generated each time an FPKI Trust Infrastructure CA is started, an Entity connects (or unsuccessfully attempts to connect) to the CA, or the private signing key is used.

When not in use, the *[Redacted for Security Purposes]* are stored in a security container controlled by *[Redacted for Security Purposes]*.

When not in use, the *[Redacted for Security Purposes]* security bags are stored in an SC that is controlled by the *[Redacted for Security Purposes]*. These two roles have the authority to access the FOS site SCs to allow *[Redacted for Security Purposes]* access to the individual-assigned security bags. The cryptographic module activation information is stored in the *[Redacted for Security Purposes]* security bags. Normally, all FPKI Trust Infrastructure CA equipment stays activated. If FPKI Trust Infrastructure CA equipment must be inactive (e.g., when equipment is damaged, inoperable), it is stored in the safe. Inoperable or damaged equipment that cannot be stored in the safe will remain in the locked CA IPS security container until it is either restored to operation on site or sanitized and shipped out for service or disposal.

FPKI Trust Infrastructure CAs require M of N authentication to start the software user interface that issues or revokes certificates. The activation data is a *[Redacted for Security Purposes]*token split into multiple parts with the number of parts being greater than the number of *[Redacted for Security Purposes]*. Two (2) parts are required for activation. Each *[Redacted for Security Purposes]* is given one part of the *[Redacted for Security Purposes]* that is stored as a file on FIPS 140-2 Level 3 validated USB Flash Drives stored in security bags, which are stored in *[Redacted for Security Purposes]*. The last part is given to the *[Redacted for Security Purposes]*. Per FPKIMA policy, both *[Redacted for Security Purposes]* must provide their piece of the PSE and a password for that file to activate the user interface to an FPKI Trust Infrastructure CA's user interface (i.e., FPKI trust Infrastructure *[Redacted for security purposes]* Graphic User Interface (GUI), known as the *[Redacted for Security Purposes]*).

The *[Redacted for Security Purposes]* are responsible for ensuring that their security bag is locked prior to returning to the *[Redacted for Security Purposes]* for storage in the SC.

[Redacted for Security Purposes] perform a security check of the facility and complete the appropriate logs (Personnel Sign-in Log, Visitors Log, Secured Container Access Log, Secured Rack Access Log), ensuring all systems are operating in the appropriate state, and that all sensitive material has been secured appropriately before the last authorized individual leaves the FPKI Trust Infrastructure cage.

5.1.2.2 Physical Access for RA Equipment

The FPKI Trust Infrastructure does not have an RA application.

5.1.2.3 Physical Access for CSS Equipment

The FPKI Trust Infrastructure does not have any CSS Equipment.

5.1.2.4 Physical Access for CMS Equipment

The FPKI Trust Infrastructure does not have any CMS Equipment.

5.1.3 Power and Air Conditioning

Both facilities have backup power that will allow the FPKI Trust Infrastructure to continue operating in case power to the facility is interrupted. The backup power will keep the FPKI Trust Infrastructure CAs and Repositories functioning until commercial power is restored. If commercial power will be unavailable longer than the backup power capacity, the facility will notify the FPKIMA with enough time to allow *[Redacted for Security Purposes]* to travel to the site and affect an orderly shutdown of the equipment.

FOS-W: *[Redacted for Security Purposes]* data centers utilize uninterruptible power systems and associated flywheel backup for critical electrical delivery to all computer hardware, and to telecommunications systems (routers, switches and applicable phone systems) within the data center. In association with the UPS Systems, Service Provider data centers also utilize stand-by emergency generators and appropriate automatic switching in the event of unplanned utility outages.

The landlord provides backup units for immediate failover for the primary environmental systems such as HVAC and electrical. The data center has the following features in place, as per the lease agreement with the data center landlord, to provide environmental controls:

- The building is outfitted with five 1 megawatt Hitec Rotary UPS generators.
- The data center rotary generators use internal flywheel for UPS and, therefore, do not require battery backup.

[Redacted for Security Purposes]

Within industry acceptable levels, *[Redacted for Security Purposes]* maintains temperature and humidity levels inside the data centers, which are monitored by sensors located throughout the raised floor area and maintained at defined levels (system tolerances).

Environmental systems are monitored 24/7 and are maintained by Building Engineers and/or third parties. Monthly reports are reviewed by *[Redacted for Security Purposes]* Management to ensure that the generators were tested and that environmental monitoring was performed.

FOS-E: The data center is connected to multiple UPS systems that provide temporary backup power in the event of a power failure at the FOS-E site. The UPS systems will keep the servers powered long enough for the local generators to turn on and start supplying power to the server room equipment. There are Service Level Agreements in place to ensure the UPS devices are inspected and maintained quarterly, semi-annually, and annually by a third-party vendor. In addition, there are multiple dedicated fueled electric generators to assist in a power failure. The generators are also inspected weekly by the third party vendor.

The facility has five redundant chilled-water heat exchange systems with 2,000 tons of chilled water to cool the building. Humidity is maintained at 45% - 55%. Temperature and humidity are monitored and maintained at acceptable levels, within the facility where the information system resides. Temperature and humidity is monitored onsite and offsite. The Building Management System (BMS) is used to monitor any alarms.

5.1.4 Water Exposures

FOS-W: All servers are located on a raised platform and away from any water. There are floor drains and below-floor water sensing devices. Master shut-off valves are located in secured areas and can be accessed by key facility members in the event of an emergency.

FOS-E: All production servers are located on a raised platform and away from water. All production servers are protected from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel. Leak detection mechanisms are also located on each of

the HVAC and Chiller units and under the datacenter floor. Water-resistant Type TC cable is used.

5.1.5 Fire Prevention and Protection

FOS-W: *[Redacted for Security Purposes]* data centers are equipped with smoke detectors, fire alarms (visual & audible type), and dry-pipe water suppression. All of these indicators are electronically tied to the building's alarm system for auto-notification to public response facilities.

The facility is protected by a Siemens-based fire monitoring system with detectors located on the ceiling and under the raised floor. The computer room is fire protected by a pre-action, double inter-lock dry pipe suppression system. Environmental systems are monitored 24/7 and are maintained by Building Engineers and/or third parties. Monthly reports are reviewed by *[Redacted for Security Purposes]* Management to ensure that the generators were tested and that environmental monitoring was performed.

FOS-E: Fire suppression and detection devices/systems that can be activated in the event of a fire are installed. The fire suppression system is zone and pre-action. The fire suppression system is a dry pipe system. There are also handheld fire extinguishers and smoke detectors available. The data center facility is equipped with fire alarms that are monitored by third party security personnel. In the event of a fire, the security, facility, and the fire department are automatically notified.

5.1.6 Media Storage

Any media that has been digitally connected to (e.g., inserted in) a system in the FPKI Trust Infrastructure CA zone is stored at the FPKI sites or kept under two-party control when transferred between sites to protect it from unauthorized physical access, in accordance with the SOPs. Media containing data from an FPKI Trust Infrastructure system is stored in the SC to protect it from accidental damage (water, fire, electromagnetic).

5.1.7 Waste Disposal

The disposal of sensitive or classified information is handled in accordance with the GSA Federal Technology Service (FTS) procedures for disposal of such material.

5.1.8 Off-Site backup

Backup information is stored in a security bag and replicated to the other site.

Whenever a certificate is issued or revoked, and other times as needed, the FPKI Trust Infrastructure CA database is backed up and restored at the other FOS site, using standard *[Redacted for Security Purposes]* procedures. The replicated CA and the current backup of the CA database and private keys is sufficient to recover from a system failure.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security or operational incidents if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles are responsible for the integrity of the FPKI Trust Infrastructure CAs.

The functions performed in these roles form the basis of trust for all uses of the FPKI Trust Infrastructure. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The ISSM and ISSO are Information Assurance roles appointed in accordance with applicable legislation and proscribing directives. The DAA appoints the ISSM, and the ISSM appoints the ISSO. The following is the list of Trusted Roles:

- *Administrator* – authorized to install, configure, and maintain the Operating Systems, Applications and Directory Software; establish and maintain Operating System user accounts; configure Operating System profiles and audit parameters; and generate component keys.
- *Officer* – authorized to request or approve certificates or certificate revocations; maintain FPKI Trust Infrastructure CA software *[Redacted for Security Purposes]*; establish and maintain FPKI Trust Infrastructure CA application and database accounts; and configure FPKI Trust Infrastructure CA software profiles and audit parameters.
- *Auditor* – authorized to view and maintain audit logs.
- *Operator* – authorized to perform system backup and recovery.

5.2.1.1 Administrator

The Administrator role is responsible for:

- Installation, configuration, and maintenance of the Operating Systems(OS) and Directory Software;
- Establishing and maintaining OS and FPKI Directory system accounts;
- Configuring audit parameters for the OS and FPKI Directory;
- Assisting in Generating and Backing up FPKI Trust Infrastructure CA keys; and
- Restarting OS and services in case of system failures.

Administrators do not issue certificates.

5.2.1.2 Officer

The Officer role is responsible for issuing certificates, including:

- Registering new Subscribers and requesting the issuance of certificates;
- Verifying the accuracy of information included in certificates;
- Approving and executing the issuance of certificates;
- Requesting, approving and executing the revocation of certificates;
- Configuring certificate profiles or templates and audit parameters for FPKI Trust Infrastructure CA software; and
- Generating and backing up FPKI Trust Infrastructure CA keys.

5.2.1.3 Auditor

The Auditor role is responsible for:

- Reviewing, maintaining, and archiving audit logs; and

- Performing or overseeing internal compliance audits to ensure that the FPKI Trust Infrastructure CAs are operating in accordance with this CPS.

5.2.1.4 Operator

The Operator role may be responsible for some routine operations of the FPKI Trust Infrastructure CAs including system backups and recovery, or changing recording media. The Operator also assists the Administrator as directed by the Administrator.

5.2.2 Number of Persons Required per Task

To best ensure the integrity of FPKI Trust Infrastructure equipment and operation, no individual will be assigned more than one Trusted Role. The separation provides a set of checks and balances over FPKI Trust Infrastructure CA operation. Since *[Redacted for Security Purposes]* is required to gain access to the FPKI facilities, at least one of the participants will always be *[Redacted for Security Purposes]*.

Only *[Redacted for Security Purposes]* has access to the locked CA IPS security container containing FPKI Trust Infrastructure CA equipment. Therefore, both *[Redacted for Security Purposes]* are required for any task associated with FPKI Trust Infrastructure CAs and Hardware Security Module (HSM), including HSM activation and backup and FPKI Trust Infrastructure CA key generation, certificate issuance, and certificate revocation.

Under no circumstances does any FPKI Trusted Role perform its own auditor function.

5.2.3 Identification and Authentication for Each Role

Individuals identify and authenticate themselves before being permitted to perform any actions set forth above for that Trusted Role.

At the operating system level, authentication is done by system logon controlled by account authentication in *[Redacted for Security Purposes]*. Trusted Roles are given role-based access control on the system enforced by security groups in *[Redacted for Security Purposes]*. Administrators have local and domain administrator rights on the systems (with separate accounts providing those rights).

[Redacted for Security Purposes] are both identified and authenticated by the CA application via *[Redacted for Security Purposes]* files (software tokens) assigned to their respective roles, and by the HSM via *[Redacted for Security Purposes]* keys assigned to their respective roles. *[Redacted for Security Purposes]* are also identified and authenticated by the CA database and HSM via accounts assigned to the *[Redacted for Security Purposes]* role.

5.2.4 Separation of Roles

The separation of roles for the FPKI Trust Infrastructure CA, which is operated at the high CP assurance level, is as follows:

- Individual FPKIMA personnel are specifically designated to the four Trusted Roles defined in Section 5.2.1. Individuals may assume only one of the Officer, Administrator, Operator, and Auditor roles. No user identity can:

[Redacted for Security Purposes]

The crypto module for the FPKI Trust Infrastructure CAs is activated by using the *[Redacted for Security Purposes]* and tokens.

Separation of duty is enforced by a combination of practices. Only the *[Redacted for Security Purposes]* has an account to log onto the system. Each *[Redacted for Security Purposes]* logs on using his own account. Once an *[Redacted for Security Purposes]* is logged on to the FPKI Trust Infrastructure CA server, the *[Redacted for Security Purposes]* is given logical access to the *[Redacted for Security Purposes]*interface for the CA access to the functions for certificate issuance and revocation. The *[Redacted for Security Purposes]* interface requires two *[Redacted for Security Purposes]* enter the activation information for a split *[Redacted for Security Purposes]*. One must be *[Redacted for Security Purposes]* and one must be *[Redacted for Security Purposes]*.

Audit log data is generated automatically by FPKI Trust Infrastructure CAs for all access to FPKI Trust Infrastructure CA activities.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

The FPKIPA and the FPKIMA are responsible and accountable for the operation of the FPKI Trust Infrastructure.

All persons filling Trusted Roles are selected on the basis of loyalty, trustworthiness, and integrity, and are U.S. citizens. The FPKIMA PM and program management team are responsible for evaluating the qualification of each individual selected for a trusted role. The ISSO has oversight of the training provided to trusted roles.

All FPKI personnel serving in Trusted Roles hold Top Secret security clearances.

Personnel security procedures are in place, which include separation of duties (in compliance with the CP), least privilege, and individual accountability to mitigate internal security risks due to the actions of personnel as outlined in [NIST SP 800-53]. See [FPKI SSP] “Personnel Security” security control section for more details.

5.3.2 Background Check Procedures

FPKIMA personnel in Trusted Roles hold Top Secret clearances that require extensive background checks by Government Security personnel. Top Secret clearances are further subject to periodic reviews at least every five years.

5.3.3 Training Requirements

All Trusted Roles undergo security awareness training prior to their appointment to a Trusted Role and on a periodic basis. They are also trained on the operations of the system.

All personnel performing duties with respect to the operation of the FPKI Trust Infrastructure receive comprehensive training. Training (including On-The-Job-Training (OJT) and review of procedures) is conducted in the following areas by product engineers:

- CA/RA security principles and mechanisms;
- All PKI software versions in use for the FPKI Trust Infrastructure CAs;

- All PKI duties they are expected to perform; and
- Disaster recovery and business continuity procedures.

Training in the overall security procedures of the FPKI Trust Infrastructure is conducted for all personnel at the initial full-operation capability of the FPKI Trust Infrastructure. When a person is assigned to a new FPKI Trusted Role, they receive training in all the operational duties for that role; including a period of shadowing another in that role and then a period of reverse shadowing. In addition, training and review of security procedures is conducted at the time a change in procedures occurs and/or annually. Personnel are required to sign acknowledgements that they have received this training. All personnel training records are maintained by the ISSO.

5.3.4 Retraining Frequency and Requirements

Any significant change to the operations is documented, and personnel are informed and made aware of changes in accordance with the personnel training procedures defined in the SOPs. All FPKIMA personnel participate in mandatory refresher training annually to ensure all affected personnel are aware of new changes to procedures and configuration changes. In addition, immediate OJT is conducted when any changes occur within FPKI Trust Infrastructure operations. Examples of such changes are FPKI Trust Infrastructure CA software or hardware upgrades, changes in automated security systems, and relocation of equipment. The ISSO maintains a record of the training received by each person assigned to an FPKI Trusted Role.

5.3.5 Job Rotation Frequency and Sequence

Any rotation or termination of FPKIMA personnel shall not impact the continuity and integrity of the FPKI services. Since there are multiple people fulfilling each trusted role, there is time to identify and train a replacement any time one individual rotates or terminates his/her position within the FPKIMA.

5.3.6 Sanctions for Unauthorized Actions

The FPKIPA takes appropriate administrative and disciplinary actions against personnel who have performed unauthorized actions involving the FPKI Trust Infrastructure or its Repository. In the event of an unauthorized action, the ISSO immediately investigates the incident. After the investigation, the ISSO and ISSM determine if the action warrants disciplinary actions based on severity and the recurring frequency of the indiscretion. If the unauthorized action is a significant indiscretion, it is reported to the FPKI Program Manager and the FPKIPA. If the incident is not severe, immediate remedial training is conducted to ensure the offending party is made aware of his/her action and trained on the correct actions as to prevent further indiscretions.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to the FPKI Trust Infrastructure will have the necessary experience, as determined by their supervisor and Program Manager, to be able to fulfill the required functions of their assigned role when given appropriate training on FPKIMA operational procedures. All personnel assigned to the FPKIMA will be U.S citizens. All personnel assigned to FPKIMA Trusted Roles will hold an active U.S. Government Top Secret Clearance. FPKIMA contractors and subcontractors are contractually obligated to perform their duties in accordance with this CPS.

5.3.8 Documentation Supplied To Personnel

The FPKIMA makes available to all of its personnel the [FBCA CP], [FCPF CP], this FPKI CPS, FPKIMA standard operating procedures (SOPs), and any relevant statutes, policies or contracts when an individual is first assigned to an FPKIMA role.

When these documents are revised, FPKIMA personnel are notified of the changes and updated documents are provided in electronic format via secure ftp or a secure file storage site.

5.4 AUDIT LOGGING PROCEDURES

The FPKIMA generates audit log files for all events relating to the security of the FPKI Trust Infrastructure CAs. In addition to the audit logs detailed below, information relevant to certificate issuance and certificate revocation events is captured on certificate issuance and certificate revocation forms. Where possible, the security audit logs are automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism is used, depending on the audited event. All security audit logs, both electronic and non-electronic, are retained and made available during compliance audits.

Formal audit and accountability policies and procedures have been developed and documented, and are periodically updated, in accordance with [NIST SP 800-53]. See [FPKI SSP] "Audit and Accountability" security control section for more details.

5.4.1 Types of Events Recorded

Security auditing capabilities of the FPKI Repository, the FPKI Trust Infrastructure CA operating system, and FPKI Trust Infrastructure CA applications have been enabled for logging the types of events specified in Table 5.4.1-1. The table indicates whether the auditable event is logged automatically by the application/operating system, is logged manually in a logbook as prescribed by applicable procedures, or both. A message from any source requesting an action by any FPKI Trust Infrastructure CA is documented and retained by the Auditors via the FPKIarchive@SRA.com email account, and included in the audit and archive process. The message must include message date and time, source, destination and contents. At a minimum, each audit record includes the following (either recorded automatically or manually for each auditable event):

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

The FPKIMA staff has verified (i.e., obtained vendor statements and conducted direct testing) that the equipment and application software supports capturing audit logs for the events specified in the table below through HTTP access, error logs and system access logs. Firewall logs are also used to audit who is accessing or attempting to access the system. *[Redacted for Security Purposes]*, FPKI Directory Server Agent logs, firewall operating system access logs and external firewall logs are audited.

Table 5.4.1-1. Auditable Events

Auditable Event	FPKI System			CA Enclave		
	Manual	Automatic	Location	Manual	Automatic	Location
SECURITY AUDIT						
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	✓	✓	CM Package *[Redacted for Security Purposes]* *[Redacted for Security Purposes]* OS Logs	✓	✓	CM Package *[Redacted for Security Purposes]*
Any attempt to delete or modify the Audit logs		✓ After a modification following any archive operation	*[Redacted for Security Purposes]* (Security) *[Redacted for Security Purposes]* OS Logs *[Redacted for Security Purposes]*		✓	*[Redacted for Security Purposes]* (Security) Internal *[Redacted for Security Purposes]* Audit Log
IDENTIFICATION AND AUTHENTICATION						
Successful and unsuccessful attempts to assume a role		✓	*[Redacted for Security Purposes]* *[Redacted for Security Purposes]* OS Logs		✓	*[Redacted for Security Purposes]* *[Redacted for Security Purposes]* (Application)
Change in the value of maximum authentication attempts	✓	✓	CM Package *[Redacted for Security Purposes]* *[Redacted for Security Purposes]* OS Logs	✓	✓	CM Package *[Redacted for Security Purposes]*
Maximum number of unsuccessful authentication attempts during user login		✓	*[Redacted for Security Purposes]* (Security) *[Redacted for Security Purposes]* OS Logs		✓	*[Redacted for Security Purposes]* (Security) *[Redacted for Security Purposes]* (Application)
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts		✓	*[Redacted for Security Purposes]* (Security) *[Redacted for Security Purposes]* OS Logs		✓	*[Redacted for Security Purposes]* (Security)
An Administrator changes the type of authenticator, e.g., from password to biometrics	✓		CM Package	✓		CM Package
KEY GENERATION						
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)				✓	✓	Key Signing Ceremony Internal *[Redacted for Security Purposes]* Audit Log
PRIVATE KEY LOAD AND						

Auditable Event	FPKI System			CA Enclave		
	Manual	Automatic	Location	Manual	Automatic	Location
STORAGE						
The loading of Component private keys					✓	HSM Syslog (backup and restore from token)
All access to certificate subject private keys retained within the CA for key recovery purposes					✓	HSM Syslog (backup and restore from token)
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE						
All changes to the trusted public keys, including additions and deletions				✓		Key Signing Ceremony
PRIVATE KEY EXPORT						
The export of private-keys (keys used for a single session or message are excluded)				✓	✓	HSM Syslog (backing up partition to token)
CERTIFICATE REGISTRATION						
All certification requests				✓	✓	Internal *[Redacted for Security Purposes]* Audit Log
CERTIFICATE REVOCATION						
All certificate revocation requests				✓	✓	Internal *[Redacted for Security Purposes]* Audit Log
CERTIFICATE STATUS CHANGE APPROVAL						
The approval or rejection of a certificate status change request				✓		Letter of Authorization MOU
CA CONFIGURATION						
Any security-relevant changes to the configuration of the CA				✓	✓	CM Package *[Redacted for Security Purposes]*
ACCOUNT ADMINISTRATION						
Roles and users are added or deleted	✓	✓	Event Log *[Redacted for Security*	✓	✓	Event Log Training records and access

Auditable Event	FPKI System			CA Enclave		
	Manual	Automatic	Location	Manual	Automatic	Location
			Purposes] OS Logs Training records and access list			list
The access control privileges of a user account or a role are modified	✓	✓	Event Log *[Redacted for Security Purposes]* OS Logs Training records and access list	✓	✓	Event Log Training records and access list
CERTIFICATE PROFILE MANAGEMENT						
All changes to the certificate profile				✓	✓	PA Meeting Minute Internal *[Redacted for Security Purposes]* Audit Log
REVOCATION PROFILE MANAGEMENT						
All changes to the revocation profile				✓	✓	PA Meeting Minutes Internal *[Redacted for Security Purposes]* Audit Log
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT						
All changes to the certificate revocation list profile				✓	✓	PA Meeting Minutes Internal *[Redacted for Security Purposes]* Audit Log
MISCELLANEOUS						
Installation of the Operating System	✓	✓	*[Redacted for Security Purposes]* CM Package *[Redacted for Security Purposes]* *[Redacted for Security Purposes]* *[Redacted for Security Purposes]* OS Logs	✓	✓	*[Redacted for Security Purposes]* CM Package *[Redacted for Security Purposes]* *[Redacted for Security Purposes]*
Installation of the CA				✓	✓	*[Redacted for Security Purposes]* Build Documents CM Package for new or changed baselines *[Redacted for Security Purposes]*

Auditable Event	FPKI System			CA Enclave		
	Manual	Automatic	Location	Manual	Automatic	Location
Installing hardware cryptographic modules				✓	✓	CM Package Build Documents HSM Syslog
Removing hardware cryptographic modules				✓		CM Package
Destruction of cryptographic modules				✓		CM Package or Decommission Package
System Startup		✓	*[Redacted for Security Purposes]* *[Redacted for Security Purposes]* OS Logs	✓	✓	*[Redacted for Security Purposes]* HSM syslog
Logon Attempts to CA Apps					✓	Internal *[Redacted for Security Purposes]* Audit Log *[Redacted for Security Purposes]* (Application)
Receipt of Hardware / Software	✓		Purchase or Receiving Documents	✓		Purchase or Receiving Documents
Attempts to set passwords	✓		*[Redacted for Security Purposes]* (Security) *[Redacted for Security Purposes]* OS Logs (Secure)		✓	*[Redacted for Security Purposes]*
Attempts to modify passwords	✓		*[Redacted for Security Purposes]* (Security) *[Redacted for Security Purposes]* OS Logs (Secure)		✓	*[Redacted for Security Purposes]*
Backing up CA internal database				✓		System Maintenance Log
Restoring CA internal database				✓		System Maintenance Log
File manipulation (e.g., creation, renaming, moving)	✓	✓	CM Package *[Redacted for Security Purposes]* *[Redacted for Security Purposes]* OS Logs	✓	✓	CM Package *[Redacted for Security Purposes]*
Posting of any material to a repository	✓	✓	*[Redacted for Security Purposes]* audit log Community Notifications & Reports			
Access to CA internal database					✓	*[Redacted for Security Purposes]* Internal *[Redacted for*

Auditable Event	FPKI System			CA Enclave		
	Manual	Automatic	Location	Manual	Automatic	Location
						Security Purposes] Audit Log
All certificate compromise notification requests				✓		Certificate Revocation Form
Loading tokens with certificates				✓	✓	CM Package HSM Syslog
Shipment of Tokens				✓		Purchasing and Receiving Document(s)
Zeroizing tokens					✓	HSM Syslog
Rekey of the CA				✓	✓	Key Signing Ceremony Internal *[Redacted for Security Purposes]* Audit Log
Configuration changes to the CA server involving:						
Hardware				✓	✓	CM Package *[Redacted for Security Purposes]*
Software				✓	✓ (Application Specific)	CM Package
Operating System				✓	✓	CM Package *[Redacted for Security Purposes]*
Patches				✓	✓	System Maintenance Log or Patch Cycle Log
Security Profiles				✓	✓	CM Package *[Redacted for Security Purposes]*
PHYSICAL ACCESS / SITE SECURITY						
Personnel Access to room housing CA				✓	✓	Electronic PACS system log for FOS-WEST Facility Sign In Log and Electronic building access log (both maintained by COLO provider) for FOS-EAST Personnel/Visitor Sign In sheets
Access to the CA server				✓	✓	Electronic PACS system log

Auditable Event	FPKI System			CA Enclave		
	Manual	Automatic	Location	Manual	Automatic	Location
						for FOS-WEST Facility Sign In Log and Electronic building access log (both maintained by COLO provider) for FOS-EAST Personnel/Visitor Sign In sheets Secured Rack Access Log sheets
Known or suspected violations of physical security	✓	✓	SIR Electronic PACS system log for FOS-WEST Electronic building access log (maintained by COLO provider) for FOS-EAST	✓	✓	SIR Electronic PACS system log for FOS-WEST Electronic building access log (maintained by COLO provider) for FOS-EAST
ANOMALIES						
Software Error conditions		✓	*[Redacted for Security Purposes]* *[Redacted for Security Purposes]* OS Logs		✓	*[Redacted for Security Purposes]*
Software check integrity failures		✓	*[Redacted for Security Purposes]* *[Redacted for Security Purposes]*		✓	*[Redacted for Security Purposes]*
Receipt of improper messages		✓	Firewall logs		✓	Firewall logs
Misrouted messages		✓	Firewall logs		✓	Firewall logs
Network attacks (suspected or confirmed)	✓	✓	Firewall logs IDS logs *[Redacted for Security Purposes]*		✓	Firewall logs IDS logs *[Redacted for Security Purposes]*
Equipment failure	✓	✓	SIR *[Redacted for Security Purposes]* *[Redacted for Security Purposes]* OS Logs	✓	✓	SIR *[Redacted for Security Purposes]*
Obvious and significant network service or access failures	✓	✓	SIR *[Redacted for Security Purposes]* *[Redacted for Security Purposes]* OS Logs	✓	✓	SIR *[Redacted for Security Purposes]* HSM Syslog

Auditable Event	FPKI System			CA Enclave		
	Manual	Automatic	Location	Manual	Automatic	Location
Violations of Certificate Policy	✓	Some violations are recorded in various electronic logs, as documented in other areas of this table	SIR	✓	Some violations are recorded in various electronic logs, as documented in other areas of this table	SIR
Violations of Certification Practice Statement	✓	Some violations are recorded in various electronic logs, as documented in other areas of this table	SIR	✓	Some violations are recorded in various electronic logs, as documented in other areas of this table	SIR
Resetting Operating System clock		✓	*[Redacted for Security Purposes]* (System) *[Redacted for Security Purposes]* OS Logs (Messages log)		✓	*[Redacted for Security Purposes]* (System)

If the following events occur, they are manually logged:

- Obtaining a third-party time-stamp
- All security-relevant data that is entered in the system
- All security-relevant messages that are received by the system
- All successful and unsuccessful requests for confidential and security-relevant information
- The manual entry of secret keys used for authentication
- Appointment of an individual to a Trusted Role
- Designation of personnel for multiparty control

5.4.2 Frequency of Processing Log

Audit logs from the Administration and DMZ zones are collected and processed, in an automated continuous process, checking for anomalies. The automatic logger creates alarms if anomalies are encountered.

The Auditor reviews the CAs' application audit logs and HSM audit logs at least *[Redacted for Security Purposes]*, and all other audit logs at least *[Redacted for Security Purposes]*.

The Auditor examines all of the electronic audit logs generated at FOS-W and FOS-E, and all of the manual logs generated at FOS-W, according to the frequencies above. Manual logs generated at FOS-E are transferred to FOS-W by *[Redacted for Security Purposes]* at least once per year, and included in the following *[Redacted for Security Purposes]* review. The Auditor examines the security audit data, paying particular attention to anomalies and suspicious entries. All security alerts and irregularities are explained in an audit log summary. The Auditor reviews

include verifying that the log has not been tampered with, and then briefly inspecting log entries with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews are documented.

The Auditor collects and prepares audit logs for transfer.

The manual logs include:

- Personnel Sign-in log
- Visitor Sign-in Log
- Secure container log
- Secure rack log

The electronic logs include logs from the FPKI Trust Infrastructure CA server, the *[Redacted for Security Purposes]* server, and the HSM syslog as well as the consolidated logs from the automatic logger.

5.4.3 Retention Period for Audit Log

Audit logs are stored onsite on servers until the next *[Redacted for Security Purposes]* audit, and then the logs are pulled off for Auditor analysis, put into tamper evident bags, and then stored inside the FOS-W security container. They are moved from the FOS-W security container to the Interim site security container at least *[Redacted for Security Purposes]*. Audit logs are retained offsite at the Interim storage area until they are sent to National Archives and Records Administration (NARA). The *[Redacted for Security Purposes]*, under supervision of the Auditor, removes audit logs from the Trust Infrastructure and gives them to the Auditor. Audit logs written to optical disk are labeled with the name of the program (FPKI), a description (e.g. *[Redacted for Security Purposes]* Audit), today's date or a range of dates, if applicable.

Neither the *[Redacted for Security Purposes]* nor the Auditor can access the FPKI Trust Infrastructure CA signature key(s).

5.4.4 Protection of Audit Log

The Auditor performs routine review of security audit logs. The policies for protecting security audit data are as follows:

1. Security audit logs are automatically time stamped upon creation.
2. The only authorized people having read access to the logs are the *[Redacted for Security Purposes]* and others possibly designated by the FPKIMA to perform security audit processing.
3. Only the Auditor is authorized to archive audit logs.
4. Audit logs are deleted only under procedural multi-person control, one participating individual must be an Auditor *[Redacted for Security Purposes]*.
5. Audit logs are protected under multi-person control, and cannot be modified without detection. One participating individual must be an Auditor *[Redacted for Security Purposes]*.

Daily audit logs are generated on time stamped digital media, and are protected from deletion and modification prior to the end of the audit log retention period. System logs are automatically time stamped. All audit logs are maintained until after the annual audit.

The FPKIMA maintains two internal Network Time Protocol (NTP) servers used to maintain and synchronize system time for all servers, appliances, and applications within the FPKI Trust Infrastructure. The two internal servers will be synchronized to NIST.

5.4.5 Audit Log Backup Procedures

Manual audit logs are collected *[Redacted for Security Purposes]* and stored in a secure container either in the FOS-W security container or in a separate building (Interim storage) from the FPKI facility. A second copy of the audit logs is placed in the security container and kept at FOS-W for a year in case access is needed for analysis. Audit logs written to removable media as part of the *[Redacted for Security Purposes]* audit are placed in sealed envelopes and transported to the interim site under two person control. These audit logs are archived to a NARA archive location annually.

Administration and DMZ *[Redacted for Security Purposes]* and audit summaries are backed up and time stamped automatically and on a continual basis using an automatic logging device. Copies of these and manual paper logs are moved to and stored in a secure container in a separate building (Interim storage) from the FPKI facility. Logs are placed in sealed envelopes and transported under two-person control. Two-person control is achieved by using tamper-evident envelopes with receipt numbers. The material is placed in the envelope and sealed with both people present. One then carries the envelope, while the other keeps the numbered receipt. At the destination, both people confirm there is no evidence of the envelope having been opened or tampered with, and that the number of the envelope matches the receipt number.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system is internal to the FPKI Trust Infrastructure components (see Section 5.4). Audit processes are invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed (as determined during the auditing process and documented in the auditing/trouble handling forms), and the integrity of the system or confidentiality of the information protected by the system is at risk (as determined by the ISSO in conjunction with the ISSM and Program Manager), the FPKIMA will suspend the FPKI Trust Infrastructure CA operation until the problem is remedied. The CA operating system is configured to shut down upon failure of the *[Redacted for Security Purposes]*. Section 5.4 describes the collection procedures (manual or automatic) for the auditable events. Section 5.5 describes the protection procedures for backing up audited data that has been collected.

5.4.7 Notification to Event-Causing Subject

No notice that an event was audited is provided to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

The FPKIMA performs self-assessments of the security controls at the time of initial installation and configuration of the FPKI Trust Infrastructure components. Periodic vulnerability assessments are performed monthly or following a system configuration change with the potential for effecting system security (i.e., hardware, software, or network changes or upgrades).

External penetration assessments are conducted on a quarterly basis.

The FPKIMA provides a report of the analysis of the results of both internal and external vulnerability assessments to the Program Manager and ISSM, specifically indicating security vulnerabilities identified and mitigation procedures of those vulnerabilities.

5.5 RECORDS ARCHIVAL

The FPKIMA moves archive records to NARA on an annual basis. NARA receipts for archived material are filed at the Interim Site.

5.5.1 Types of Records Archived

At initialization, FPKI Trust Infrastructure system equipment configuration files were archived, as well as the CPS and any contractual agreements to which the FPKIMA is bound. During FPKI Trust Infrastructure operation, the following data are recorded for archive:

Archive Requirements	Artifact to be Archived
FPKI Trust Infrastructure Certification and accreditation	ATO Letter and ATO Report / ATO Documentation
Certificate Policy	Certificate Policy
Certification Practice Statement	Certification Practice Statement
Contractual obligations	MOAs
Other agreements concerning operations of the FPKI Trust Infrastructure CAs	Entity Records
FPKI Trust Infrastructure System and Equipment Configuration Documentation	Build Documentation / Change Requests / Maintenance Logs
Modifications and updates to system or configuration	Change Requests / Maintenance Logs
Certificate requests and issuance forms	LOA / P10 File / Certificate Issuance Form
Revocation requests and revocation forms	Certificate Revocation Form
Subscriber agreement and identity authentication data as per Section 3.2	LOA (ID Authentication) /Application / Subscriber Agreement / MOA (as applicable)
Documentation of receipt and acceptance of certificates	Email or other out-of-band notification from Entity (if applicable)
Documentation of receipt of tokens	N/A (Do not issue tokens)
All certificates issued or published	CA Database Backup / Monthly Statistical Report with P7C
Record of FPKI Trust Infrastructure CA Re-key	Key Generation or Rollover Package
All CRLs issued and/or published	CRLs / CA Database Backup
Other data or applications to verify archive contents	SF-135 – NARA Records Transmittal and Receipt
Compliance Auditor reports	Annual PKI Compliance Reports
Any changes to the Audit parameters, e.g. audit frequency, type of event audited	Audit SOP / Change Requests / Change Management Log
Any attempt to delete or modify the Audit logs	Security Incident Report (if applicable)
Whenever the FPKI Trust Infrastructure CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	Key Generation or Rollover Package / CA Audit Log

Archive Requirements	Artifact to be Archived
All access to certificate subject private keys retained within the FPKI Trust Infrastructure CA for key recovery purposes	N/A (The FPKI CAs do not have access to affiliate/subject private keys)
All changes to the trusted public keys, including additions and deletions	Issuance Form / Key Generation Documentation
The export of private and secret keys (keys used for a single session or message are excluded)	HSM Log Contained on the *[Redacted for Security Purposes]* Audit CD Enclosed in Tamper-Evident Envelope
The approval or rejection of a certificate status change request	Email
Appointment of an individual to a Trusted Role	Email or Document Authorization
Destruction of cryptographic modules	Receipt / Certificate of Destruction and Recycling / Decommission Documentation
All certificate compromise notifications	Authenticated Revocation Request
Security Incident Reports (SIRs) with remedial action details	System Incident Report (SIR)
Violations of Certificate Policy	System Incident Report (SIR)
Violations of Certification Practice Statement	System Incident Report (SIR)
Entity Records	Application / MOA / LOA / Interoperability Test Report / Certificate Issuance Form / Certificate Revocation Form / Mapping Report / Audit Review Letter / Compliance Review Report / ATO / PIV-I Card Test Report (as applicable)

See Sections 5.4.6 and 5.5.6 for a description of the audit and archive collection procedures.

5.5.2 Retention Period for Archive

Items that are required to be archived in paper format are transferred to the Interim site, and then to NARA so they can be retained for the required period of 20 years and 6 months. Other items, such as signed certificates and CRLs, are backed up and stored on the servers themselves. This ensures that there is always a copy available.

The Auditor collects electronic log records and paper access log records *[Redacted for Security Purposes]*. The electronic records are recorded on optical disk. Electronic records written to optical disk are also included in the archive cycle.

The Interim site is located at:

[Redacted for Security Purposes]

5.5.3 Protection of Archive

Archive data is clearly labeled as follows:

- Classification Label: CUI
- Name of the Program: FPKI
- Type of item (e.g., FBCA Log Report)

- Start Date through End Date

The archive media is stored in a safe at the Interim facility, which is temperature controlled and behind locked doors.

The FPKIMA Auditor maintains a list of individuals who can access the archive files at the Interim site. Archive data is protected in safes and by using the packaging in the Audit Procedures.

The contents of the archive will not be released except as determined by the FPKIPA or as required by law. Any request for archived information must be made to the FPKIMA Program Manager, who in consultation with the ISSM will determine if the requested information may be provided. If release of such information is authorized, the ISSM and Program Manager inform the ISSO, who will provide the information.

5.5.4 Archive Backup Procedures

Archive records are periodically written to transferable media (e.g., tape or DVD) and transferred to the Interim site, and then to NARA. Transferable media is put in sealed envelopes and transferred under control of a trusted role auditor.

5.5.5 Requirements for Time-Stamping of Records

Records are clearly labeled with date/time period information of the data contained in the record. System clocks are kept synchronized via NTP and system logs are automatically time stamped.

5.5.6 Archive Collection System (Internal or External)

The archive information is collected by the Auditor, who (using a checklist) is responsible for assuring that all records required for archive are correctly filed.

5.5.7 Procedures to Obtain and Verify Archive Information

The FPKIMA Auditor maintains logging information (and receipts) as archived data is transported to short-term and long-term archive facilities.

Archive material retrieved from NARA is verified against the logging information and receipts. Contents of FPKIMA archives are only released upon request of the FPKIPA. Individual records pertaining to a specific Entity can be released to the authorized POC for that Entity upon Entity POC request.

5.6 KEY CHANGEOVER

The FPKI Trust Infrastructure CA key changeover procedures are as follows:

1. The FPKI Trust Infrastructure CA will generate a self-issued certificate signed by the old private key whose *subjectPublicKeyInfo* field contains the new public key.
2. The FPKI Trust Infrastructure CA will generate a self-issued certificate signed by the new private key whose *subjectPublicKeyInfo* field contains the old public key.
3. The FPKI Trust Infrastructure CA will generate a self-signed certificate signed by the new private key whose *subjectPublicKeyInfo* field contains the new public key.
4. The FPKI Trust Infrastructure CAs and all Entity CAs will process new cross-certificates as described in this CPS.

5. All certificates generated as part of the key changeover process will be posted to the FPKI Repository.
6. The old FPKI Trust Infrastructure CA private key is used to sign CRLs that contain certificates signed with that key as long as required. The old key is retained and protected.

The FBCA signing key has a validity period of three years, and its corresponding certificate has a validity period of six years.

The FBCA will support Entity CA key changeovers by issuing and posting new certificates as required.

The FCPCA signing key has a validity period of ten years, and its corresponding certificate has a validity period of twenty years.

The FCPCA will support Entity CA key changeovers by issuing and posting new certificates as required

The SHA1 FRCA will support Entity CA key changeovers by issuing and posting new certificates as required.

The old private key is used to sign CRLs that contain certificates signed with that key as long as required. The old key is retained and protected.

5.7 COMPROMISE AND DIASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

The FPKIMA responds to all incidents and suspected compromise events. Detailed procedures are explained below.

In the event of a disaster, the following steps will be executed to regain system functionality:

1. Coordinate activities with FOS-E and FOS-W facility owners. These individuals along with the FPKIMA will assess the outage and determine whether all or part of the Recovery team needs to be assembled.
2. Activation of the Damage Assessment and Disaster Recovery team.
3. Based on the severity of the event, activate the recovery procedures for that severity type.
4. Interface with the FPKIMA Management Team.
5. The FPKI Repository services are actively supporting traffic at both the FOS-W and FOS-E sites during normal operation. In the case of an outage or disaster at either site, the [*Redacted for Security Purposes*] at the other site will take over and the single remaining site will automatically continue to service FPKI Repository traffic.
6. The FPKI POCs (“hot list”) will be notified of this change, so that any changes required by the Entity CAs can be performed.
7. Manage the recovery process of the affected facility.
8. Submit post recovery logs to FPKIPA.

The FPKIPA will be notified as soon as possible as described in *FPKIMA Incident Management Plan* [FPKIMA IMP], and no later than 36 hours past the lastUpdateTime of the latest CRL

If log analysis or other information provides reason to suspect any of the following may have occurred:

- compromise of the FPKI Trust Infrastructure systems;
- physical or electronic attempts to penetrate FPKI Trust Infrastructure systems;
- denial of service attacks on FPKI Trust Infrastructure repositories,

[FPKIMA IMP] will be followed to investigate and diagnose the suspected incident. The FPKIPA and other appropriate government and non-government organizations will be notified as soon as possible as described in *the* [FPKIMA IMP].

Incident response policies and procedures have been developed and documented, and are reviewed and updated periodically in accordance with [NIST SP 800-53]. See [FPKI SSP] "Incident Response" security control section for more details.

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

In the event FPKI Trust Infrastructure CA equipment is damaged or rendered inoperative, but the FPKI Trust Infrastructure CA signature keys are not destroyed, FPKI Trust Infrastructure CA operation is reestablished as quickly as possible, giving priority to the ability to generate certificate status information.

In order to provide a 6-hour window for FPKI Trust Infrastructure CA service re-activation, the FPKIMA has implemented a synchronized FOS-E site. The FOS-E site includes an identical configuration of the FOS-W site.

During system restoration, the FPKIMA needs to ensure the CRLs of FPKI Trust Infrastructure CAs are current with the latest Entity CA certificates revoked. Additionally, cross-certificates need to be validated, and new public keys/cross-certificates issued in the event anomalies exist.

The following reports are generated:

- Activity log – this log is maintained throughout the disaster recovery process;
- Test plan results;
- Equipment list – Update configuration management; and
- Restoration Expense report.

5.7.3 Entity (CA) Private Key Compromise Procedures

If the FPKI Trust Infrastructure CA signature keys are compromised or lost (such that compromise is possible even though not certain) the following procedure is executed:

1. The FPKIPA and all member Entities will be securely notified (so that entities may issue CARLs revoking any cross-certificates issued to the FPKI Trust Infrastructure CAs) via telephone to the designated POCs.
2. If possible, the self-signed certificate of the compromised key will be revoked. A compromised key can be used to sign the new CRL.
3. The Entity CAs that have issued certificates to the FPKI Trust Infrastructure CAs will publish a CARL revoking the cross-certificate issued to the FPKI Trust Infrastructure CAs as set forth above.

4. The FPKI Trust Infrastructure CA will generate a new CA key pair and self-signed certificate in accordance with procedures set forth in Section 6.1.
5. New CA certificates[6] will be issued to all Entity CAs in accordance with Section 4.3.
6. New FPKI Trust Infrastructure root certificates will be securely distributed along with the new entity CA certificates.

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

5.7.4 Business Continuity Capabilities After a Disaster

The FPKI Trust Infrastructure CA servers operate with back-up power and telecommunications and appropriate infrastructure system redundancies to minimize outages. However, if an outage appears likely to become, or becomes an extended outage, the disaster recovery plan will come into effect. An extended outage is currently defined as one in which the ability of the FPKI Trust Infrastructure CAs to revoke certificates cannot be re-established within 24 hours. However, the FPKI Trust Infrastructure has the ability to respond to an extended outage at one site. FPKI Trust Infrastructure operations are redundant across both sites and will tolerate a complete outage at either site.

In the case of a disaster whereby both the FOS-W and FOS-E installations are physically damaged, the FPKIPA and all of its member entities will be securely notified, and the procedures described in Section 5.7.3 will be followed. FPKI Trust Infrastructure CA installation will then be completely rebuilt by reestablishing the FPKI Trust Infrastructure CA equipment, generating new private and public keys, being re-certified, and re-issuing all cross-certificates.

5.8 CA OR RA TERMINATION

In the event operation of an FPKI Trust Infrastructure CA terminates, certificates signed by that FPKI Trust Infrastructure CA will be revoked, following the standard procedures for revoking cross-certificates (see Section 4.9.3). Using secure communication (callback and challenge-response), the FPKIMA will advise all cross-certified Entity CAs to which that FPKI Trust Infrastructure CA has issued cross-certificates of its termination. All documentation and data will be archived using the archival procedures in section 5.5.3. The FPKI Trust Infrastructure CA to be terminated will either continue issuing CRLs until the latest expiration date of any issued cross-certificates, or will issue a long-term CRL valid until the expiration date of the root certificate. Once the last CRL has been issued, the private signing key(s) of the CA to be terminated will be destroyed. If the FPKIMA ceases operations, any remaining FPKI Trust Infrastructure CA signing keys will be turned over to the FPKIPA.

The FPKIMA will coordinate scheduled termination with cross-certified Entity CAs when authorized by the FPKIPA.

Entities will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought in the event an FPKI Trust Infrastructure CA is terminated.

Cross-certified Entity CAs are registered on the FPKI Trust Infrastructure CA system. Therefore, the RA cannot be terminated independently of an FPKI Trust Infrastructure CA termination.

[6] CA certificates include both subordinate cross-certificates and peer-to-peer cross-certificates.

6 TECHNICAL SECURITY CONTROLS

The FPKI Trust Infrastructure implements an array of technical security controls in accordance with [NIST SP 800-53] that pertain to this section. See [FPKI SSP] "Access Control," "Audit and Accountability," Identification and Authentication," and "System and Communication Planning" security control sections for more details.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

The FPKI Trust Infrastructure CAs were established with a *[Redacted for Security Purposes]* CA. The key pair for each FPKI Trust Infrastructure CA was generated on the *[Redacted for Security Purposes]* cryptographic module. The key pair generation is RSA for digital signature in compliance with PKCS-10 (FIPS 140-2, level 3). The private key is never exposed outside the module in unencrypted form. After the key pair generation process, the *[Redacted for Security Purposes]* partition was backed up onto a secure token and restored to a second *[Redacted for Security Purposes]* at the FOS-E site. Backup copies of the *[Redacted for Security Purposes]* private keys were also created and stored in secure containers at *[Redacted for Security Purposes]*.

Private keys of FPKI Trust Infrastructure CAs are generated using the FPKI Trust Infrastructure CAs Key Signing Ceremony procedures. These procedures document the role separation and provide an auditable trail. The Key Signing Ceremony procedures are completed with a witness present. Each step is verified and the document is signed off on at the end of the procedure.

6.1.1.2 Subscriber Key Pair Generation

FPKI Trust Infrastructure CAs do not issue Subscriber keys.

6.1.2 Private Key Delivery to Subscriber

The Entity CA generates its own key pair, and therefore does not need private key delivery.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys are electronically delivered to the certificate issuer via PKCS#10 messages to the FPKIMA by secure means (e.g., CD delivered by registered mail or courier, or digitally-signed email), as described in Section 4.3.2. Identity checking and proof of possession of the private key will be accomplished as described in Section 4.2.1.

6.1.4 CA Public Key Delivery to Relying Parties

The FPKIMA posts all cross-certificates it issues to the FPKI Repository. The FPKIMA also posts all cross-certificates issued by Entity CAs to the FPKI Trust Infrastructure CAs. FPKI Trust Infrastructure CA and Entity CA public keys are transported in a secure, out-of-band mechanism using PKCS#10 messages via digitally-signed e-mail, SFTP, or CD delivered by registered mail or courier.

FPKI Trust Infrastructure CA root certificates are securely distributed to Entity CAs along with cross certificates issued to Entity CAs using PKCS#7 files via digitally-signed e-mail, SFTP, or CD delivered by registered mail or courier.

The FCPCA root certificate may also be distributed via commercial product trust stores when the FPKIMA is able to reach agreement with vendors as directed by the FPKIPA.

6.1.5 Key Sizes

After December 31, 2010, all FBCA and FCPCA certificates are issued by a *[Redacted for Security Purposes]* CA that signs certificates and CRLs using SHA-256. FPKI Trust Infrastructure CAs key are 2048 bit RSA keys.

All certificates and CRLs issued by the SHA1 FRCA are signed using SHA-1. The SHA1 FRCA's key is a 2048 bit RSA key.

The FBCA will not issue a cross-certificate to any Entity CA that does not adhere to the [FBCA CP] requirements regarding key size on the certificates they issue. Determination of Entity CA adherence to [FBCA CP] is determined by the FPKIPA and documented in the MOA between the FPKIPA and the Entity.

The FCPCA will not issue a cross-certificate to any Entity CA that does not adhere to [FCPF CP] requirements regarding key size on the certificates they issue. Determination of Entity CA adherence to [FCPF CP] is determined by the FPKIPA. Public Key Parameters Generation and Quality Checking

6.1.6 Public Key Parameters Generation and Quality Checking

There are no public key parameters for RSA, and the FPKI Trust Infrastructure CAs use RSA signatures.

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

Four key usage bits may be set in cross-certificates issued by FPKI Trust Infrastructure CAs. cRLSign, CertSign are always set. Digital Signature and Non-Repudiation may be set if specified in the LOA. The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits shall not be asserted in certificates issued by the FPKI Trust Infrastructure CAs.

The use of a specific key is determined by the key usage extension in the X.509 certificate. Section 7 contains further details on key usage.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

FPKI Trust Infrastructure CA private keys are protected using a FIPS 140-2 Level 3 validated cryptographic module: *[Redacted for Security Purposes]* HSM.

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

Activation of the HSM requires the *[Redacted for Security Purposes]* and tokens. Physical access to the HSM requires two-party control (see Section 5.1.2).

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

FPKI Trust Infrastructure CA private keys are under 2 out of N control, where N≥2. N is the total number of *[Redacted for Security Purposes]* plus one. See Section 5.2 and Section 5.2.4 for details on how this is achieved. The *[Redacted for Security Purposes]* present whenever the CA IPS secure container is accessed sign the Secured Rack Access Log which is checked by the auditor during the *[Redacted for Security Purposes]* audits and retained as part of the logs available during the annual PKI Compliance audit.

6.2.3 Private Key Escrow

6.2.3.1 Escrow of Trust Infrastructure CA and Entity CA Private Signature Key

FPKI Trust Infrastructure CA signature keys are not escrowed.

6.2.3.2 Escrow of CA Encryption Keys

FPKI Trust Infrastructure CA encryption keys are not escrowed.

6.2.4 Private Key Backup

6.2.4.1 Backup of Trust Infrastructure CA and Entity CA Private Signature Key

FPKI Trust Infrastructure CA private keys are stored in the *[Redacted for Security Purposes]* at both the FOS-W and FOS-E sites. In addition, the private key is backed up on *[Redacted for Security Purposes]* backup tokens. A backup token is stored in *[Redacted for Security Purposes]* security bag in the SC *[Redacted for Security Purposes]*. The backups of the private keys are made following procedures described in the *[Redacted for Security Purposes]* operations manuals and the FPKIMA HSM manual.

The FPKIMA is never in possession of Entity CA private signature keys.

6.2.4.2 Backup of Subscriber Private Signature Key

The FPKIMA does not issue any Subscriber certificates.

6.2.4.3 Backup of Subscriber Key Management Private Keys

The FPKIMA does not issue any Subscriber key management certificates.

6.2.4.4 Backup of CSS Private Key

The FPKIMA does not support a CSS.

6.2.4.5 Backup of PIV-I Content Signing Key

The FPKIMA does not issue any PIV-I Content Signing certificates.

6.2.5 Private Key Archival

No private keys of FPKI Trust Infrastructure CAs are archived or escrowed (see Section 6.2.3).

6.2.6 Private Key Transfer Into or From a Cryptographic Module

FPKI Trust Infrastructure CAs private keys are generated by and remain in a cryptographic module. The *[Redacted for Security Purposes]* product uses proprietary secure means for transferring keys from one cryptographic module to another to back up the CA keys.

6.2.7 Private Key Storage on Cryptographic Module

FPKI Trust Infrastructure CA private keys are only stored in the *[Redacted for Security Purposes]*, FIPs-140 Level-3 evaluated cryptographic module and on *[Redacted for Security Purposes]* proprietary backup tokens.

6.2.8 Method of Activating Private Key

The *[Redacted for Security Purposes]* cryptographic module requires that two *[Redacted for Security Purposes]* tokens be inserted into the *[Redacted for Security Purposes]*. The *[Redacted for Security Purposes]* must be present.

Procedures for activating and using the private keys, as well as the physical protections procedures for the hardware tokens are provided in Section 5.1.2.

6.2.9 Methods of Deactivating Private Key

The *[Redacted for Security Purposes]* cryptographic module is always in use and activated. The *[Redacted for Security Purposes]* cryptographic module is protected from unauthorized use by the physical access mechanisms described in Section 5.1.2.1.

The *[Redacted for Security Purposes]* cryptographic module is protected from unauthorized logical access by being on the protected FPKI Trust Infrastructure CA sub network as described in Section 6.5.1.

Additionally, the *[Redacted for Security Purposes]* and hardware tokens are required to obtain direct logical access to the *[Redacted for Security Purposes]*. The *[Redacted for Security Purposes]* and hardware tokens are stored as described in Section 5.1.2.1.

6.2.10 Method of Destroying Subscriber *[Redacted for Security Purposes]* Private Signature Key

When *[Redacted for Security Purposes]* leaves, the *[Redacted for Security Purposes]* to access the *[Redacted for Security Purposes]* application are regenerated to remove the piece associated with the terminating individual, or its password is changed by the individual taking the place of the terminating individual.

When a CA private signature key is no longer needed, the key will be deleted from the *[Redacted for Security Purposes]* HSM partition. If the FPKI Trust Infrastructure CA is being decommissioned, the corresponding partition on the *[Redacted for Security Purposes]* will be deleted and all backup tokens will be zeroized.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 OTHER ASPECTS OF KEY MANAGEMENT

6.3.1 Public Key Archival

All certificates issued by FPKI Trust Infrastructure CAs, and their associated public keys, are included in the archival of the CA database backups.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

FBCA private signing keys are used to sign certificates for one-half of the certificate lifetime (e.g. for 3 years with a certificate lifetime of 6 years). Rekeying will be performed at 3 years.

FCPCA private signing keys are used to sign certificates for one-half of the certificate lifetime (e.g. for 10 years with a certificate lifetime of 20 years). Rekeying will be performed at 10 years.

SHA1 FRCA private signing keys are used to sign certificates for the certificate lifetime.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

Activation data for the *[Redacted for Security Purposes]* partition is generated by the HSM during partition creation. The *[Redacted for Security Purposes]* authentication device *[Redacted for Security Purposes]* USB tokens and PINs are used to activate a partition on the *[Redacted for Security Purposes]* to enable use of the FPKI Trust Infrastructure CA private signing keys. These tokens satisfy the policy enforced by the *[Redacted for Security Purposes]*. Once the use of the FPKI Trust Infrastructure CA private signing keys is enabled, actual use of the private signing keys is under multi-person control of the CA software.

Activation data is not transmitted during routine operations. If transmission of activation data is necessary for replication of newly-generated data to the other site, it's transmitted by the trusted role it's assigned to using the associated security bag and a two-party control method (with *[Redacted for Security Purposes]*).

FPKI Trust Infrastructure CAs are installed using a *[Redacted for Security Purposes]* CA. Multi-party control of the *[Redacted for Security Purposes]* CA is enforced through physical means. *[Redacted for Security Purposes]* is required to gain access to the room, and *[Redacted for Security Purposes]* has to unlock the CA IPS Security Container. Access to the operating system requires *[Redacted for Security Purposes]* credentials. In addition, access to the CA software requires authentication of M of N individuals, where M is two, *[Redacted for Security Purposes]*, and N is the total number of *[Redacted for Security Purposes]* plus one. This M of N authentication makes use of split *[Redacted for Security Purposes]* in the *[Redacted for Security Purposes]* CA. Each piece of the split *[Redacted for Security Purposes]* is a file stored on a FIPS 140-2 Level 3 Encrypted USB Flash Drive, which requires the Trusted Role to enter a password to access the Flash Drive and a Password to unencrypt the *[Redacted for Security Purposes]* file. The split *[Redacted for Security Purposes]* are updated whenever there is a change in Trusted Role personnel. In addition, new *[Redacted for Security Purposes]* will be generated when an FPKI Trust Infrastructure CA performs a rekey.

6.4.2 Activation Data Protection

Activation information for the *[Redacted for Security Purposes]* CA will be stored on FIPS 140-2 Level 3 Encrypted USB Flash Drives stored in the *[Redacted for Security Purposes]* security bag, which are stored in *[Redacted for Security Purposes]* when not in use.

Note that on the *[Redacted for Security Purposes]* unit, the activation data is on physical tokens. These tokens are locked in SCs. The M of N keys are stored in security bags locked using devices for which no one person has access to both combinations and keys.

FPKI Trust Infrastructure CAs are configured to temporarily lock out access following three unsuccessful login attempts.

See Sections 5.1.2 and 5.2.2 for descriptions of the procedures for distribution and protection of activation data contained on the hardware tokens.

6.4.3 Other Aspects of Activation Data

Passwords are changed periodically, as described in the SOPs, to decrease the likelihood of discovery. According to FPKIMA policy, the cryptographic module activation data will be changed not less than once per year or when *[Redacted for Security Purposes]* leaves.

6.5 COMPUTER SECURITY CONTROLS

The FPKI Trust Infrastructure implements an array of technical security controls in accordance with [NIST SP 800-53] that pertain to this section. See [FPKI SSP] "Access Control," "Audit and Accountability," Identification and Authentication," and "System and Communication Planning" security control sections for more details.

6.5.1 Specific Computer Security Technical Requirements

The FPKI Trust Infrastructure CA server is dedicated to providing FPKI Trust Infrastructure CA services. The FPKI Trust Infrastructure CA server is accessed only via KVM in the locked CA IPS security container. This server publishes all information to an internal FPKI Directory that connects through a one-way firewall to the online FPKI Repository systems in order to post validation information.

The FPKI Repository servers only run those services necessary to operate and maintain the FPKI Repository and to support online certificate validations by Entity CA Subscribers (e.g., LDAP, DSP, HTTP, DNS, NTP).

All FPKI Trust Infrastructure component systems are configured with appropriate security features turned on as recommended by the host operating system vendor, in accordance with any associated security validation rating.

The FPKI Trust Infrastructure CA server has the following security features and functions:

- Requires authenticated logins;
- Provides Discretionary Access Control via permissions and policies defined in the CA software;
- Provides security audit capability via automatic logging of all FPKI Trust Infrastructure CA activity;
- Restricts access control to FPKI Trust Infrastructure CA services and PKI roles as described in Sections 5.1.2 and 5.2.2;
- Enforces separation of duties for PKI roles as described in Sections 5.1.2 and 5.2.2;
- Requires identification and authentication of PKI roles and associated identities as described in Sections 5.1.2 and 5.2.2;
- Prohibit object re-use or require separation for CA random access memory. This requirement is met by the configuring the *[Redacted for Security Purposes]* operating system to the Vendor Standard *[Redacted for Security Purposes]*. *[Redacted for Security*

Purposes] enforces the required prohibition/separation. *[Redacted for Security Purposes]*.

- Requires use of cryptography for session communication and database security;
- Archives history and audit data from FPKI Trust Infrastructure CA through data collection and archive procedures described in Sections 5.4 and 5.5;
- Requires self-test security related FPKI Trust Infrastructure CA services. FPKI Trust Infrastructure CA security audit logs are signed objects and the software verifies those objects at startup and each time the logs are accessed. If the verification changes, the software provides a message through the user interface and logs the event;
- Uses FIPS 140-2 certified hardware to protect activation data (*[Redacted for Security Purposes]*) required to access the FPKI Trust Infrastructure CA key for certificate issuance and revocation;
- Requires a recovery mechanism for keys and the FPKI Trust Infrastructure CAs through backup and protection procedures described in Section 5.5; and
- Enforces domain integrity boundaries for security critical processes through self-test procedures described in an earlier bullet.

6.5.2 Computer Security Rating

The *[Redacted for Security Purposes]* CA resides on a *[Redacted for Security Purposes]* that has been configured in accordance with NSA hardening guidance.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

The FPKI Trust Infrastructure implements an array of technical security controls in accordance with [NIST SP 800-53] that pertain to this section. See [FPKI SSP] “Access Control,” “Audit and Accountability,” Identification and Authentication,” and “System and Communication Planning” security control sections for more details.

6.6.1 System Development Controls

The FBCA system development controls are as follows:

- FPKI Trust Infrastructure CA software is *[Redacted for Security Purposes]* software that has been developed under a formal development process that is well documented;
- Hardware procured to operate the FPKI Trust Infrastructure CAs has been purchased in a fashion whereby the provider does not know that it is intended for FPKI Trust Infrastructure CA operations. The FPKI Trust Infrastructure CA software has been installed under the direction and control of authorized FPKI operations personnel. Hardware and software updates will be purchased or developed in the same manner as the original equipment, and will be installed by trusted and trained personnel;
- All software and hardware installed in, or run on the FPKI Trust Infrastructure CA server is purchased using *[Redacted for Security Purposes]*. Hardware and non-CA software are purchased through standard procurement procedures provided by the FPKIMA. *[Redacted for Security Purposes]*. An accountable method of packaging and delivery is used to provide a continuous chain of accountability from the vendor to the facility (e.g., UPS, Fedex, USPS Express Mail). The FPKIMA established a relationship with the CA software vendor prior to acquisition that gives assurance that the software has not been tampered with. Installation is performed under multi-person control with only authorized FPKIMA personnel; and

- Proper care is taken to prevent malicious software from being loaded onto FPKI Trust Infrastructure equipment. From the time software is received, software remains under continuous control. All shrink-wrapped packaging is opened and installed inside the secure FPKI facility under multi-person control**.** Antivirus software is used to scan all applications and files for malicious code – initially, periodically, and any time a new file is introduced to the system. Vulnerability assessments are conducted periodically, and any time a system configuration change occurs (e.g., adding a new CA to the FPKI).
- Continuous monitoring of all FPKI systems is performed through Intrusion Detection Systems, vulnerability testing and scanning, external penetrations tests, log analysis, and procedural monitoring as required in operating procedures.
- FPKI Trust Infrastructure CA software and hardware are dedicated to performing FPKI Trust Infrastructure CA functions only.

6.6.2 Security Management Controls

The initial configuration of the FPKI software (i.e., CA software, Repository software) as well as any modifications and upgrades is documented and controlled in accordance with the *Configuration Management (CM) Plan for the FPKI Trust Infrastructure*. System and application level logging is enabled and reviewed *[Redacted for Security Purposes]* to maintain ongoing integrity of the software and configuration. The source for the software is described in Section 6.6.1. Audit procedures are used to ensure software integrity. These procedures are performed on a *[Redacted for Security Purposes]* basis.

6.6.3 Life Cycle Security Ratings

The FPKI Trust Infrastructure operates under standard maintenance. U.S. CERT Technical Alerts (TA) and Security Bulletins (SB), upgrades, , and patches to the software and hardware are applied as necessary under FPKI configuration management procedures.

6.7 NETWORK SECURITY CONTROLS

The FPKI Trust Infrastructure implements an array of technical security controls in accordance with [NIST SP 800-53] that pertain to this section. See [FPKI SSP] “Access Control,” “Audit and Accountability,” Identification and Authentication,” and “System and Communication Planning” security control sections for more details.

FPKI Trust Infrastructure contains a private management network between the secure FPKI Trust Infrastructure CA subnet and the Demilitarized Zone (DMZ). The CRLs, certificates, and cross-certificates will be published first to a Master Directory in the private management network before being pushed out to the public Repositories in the DMZ. The FPKI system includes *[Redacted for Security Purposes]* server supporting the FPKI Trust Infrastructure CAs in the CA enclave. The servers in the CA private network can only be accessed via a KVM in the CA IPS security container.

The *[Redacted for Security Purposes]* HSM is protected in the CA IPS security container that *[Redacted for Security Purposes]* have the combination for (located inside the locked system room to which only *[Redacted for Security Purposes]* have unescorted access).

The FPKI Online Repositories in the DMZ are protected by a Firewall that is configured to only allow access to necessary services on the FPKI Repository systems (DSP, LDAP, and HTTP) and specific machines. All other activity is blocked and recorded.

The FPKI Directories support DSP and LDAP V3 protocols for operation and interoperability of the FPKI Directories with Entity CA directories, including support for X.500 directory chaining, referrals, and cross-referencing mechanisms. The FPKI Repository also includes web servers supporting HTTP access.

The FPKIMA uses a commercial service to provide external performance monitoring of FPKI Trust Infrastructure Repository performance. In addition FPKIMA manages *[Redacted for Security Purposes]* monitoring of the content of the FPKI Trust Infrastructure Repository. The combination of the commercial and FPKIMA monitoring provide a countermeasure for Denial of Service attacks. All unused network ports and services are turned off.

The FOS-W and FOS-E sites are [*Redacted for Security Purposes*].

6.8 TIME-STAMPING

System time is maintained using Network Time Protocol (NTP) and a local timeserver synchronized with a time server synchronized with NIST. Clock adjustments are auditable events (see Section 5.4.1).

System time will be accurate to within three minutes by being automatically synchronized using NTP.

7 CERTIFICATE, CRL, AND OCSP PROFILES

The FPKIPA has defined the Certificate and CRL profiles used by the FPKI. For ease of reference, this CPS includes a selective description in the following Sections.

7.1 CERTIFICATE PROFILE

The FBCA issues cross-certificates in accordance with the FBCA certificate profile contained in the *Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile* [FPKI-Prof], and *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards* [PIV-I-Prof] if applicable.

Certificates issued by the FCPCA conform to the *X.509 Certificate and CRL Extensions Profile for the Common Policy* [CCP-Prof].

7.1.1 Version Number(s)

FPKI Trust Infrastructure CAs issue X.509 v3 certificates (populate version field with integer "2").

7.1.2 Certificate Extensions

Certificates issued by the FBCA shall comply with [FPKI-Prof], and [PIV-I-Prof] if applicable, using standard certificate extensions that comply with [RFC 5280].

Certificates issued by the FCPCA shall comply with [CCP-Prof] using standard certificate extensions that comply with [RFC 5280].

The only private extensions included in cross-certificates issued by FPKI Trust Infrastructure CAs are obtained from the PKCS#10 received from the Entity CA. The FPKIMA will verify that no private extension in the cross-certificate is marked critical.

7.1.3 Algorithm Object Identifiers

In compliance with [FPKI-Prof], and [PIV-I-Prof] if applicable, cross-certificates issued by the FBCA use the signature OIDs listed in Table 7.1.3-1:

Table 7.1.3-1 FBCA Signature Algorithm OIDs

Algorithm	OID
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 }

In compliance with [FPKI-Prof], and [PIV-I-Prof] if applicable, cross-certificates issued by the FBCA use the OIDs listed in Table 7.1.3-2 for identifying the algorithm for which the subject key was generated:

Table 7.1.3-2 FBCA Subject Key Algorithm OIDs

Algorithm	OID
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}

Private extensions are not used.

Certificates issued by the FCPCA will use the OIDs listed in Table 7.1.3-3 for signatures:

Table 7.1.3-3 FCPCA Signature Algorithm OIDs

Algorithm	OID
sha1WithRSAEncryption	{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}

Certificates issued by the FCPCA will use the OID listed in Table 7.1.3-4 to identify the algorithm associated with the subject key:

Table 7.1.3-4 FCPCA Subject Key Algorithm OIDs

Algorithm	OID
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

7.1.4 Name Forms

The subject and issuer fields of the cross-certificate are populated with an X.500 DN, with the attribute type as further constrained by [RFC 5280].

7.1.5 Name Constraints

FPKI Trust Infrastructure CAs assert name constraints in certificates issued to Entity CAs appropriate for the PKI being certified, as specified in the LOA issued by the FPKIPA.

7.1.6 Certificate Policy Object Identifier

All certificates issued by FPKI Trust Infrastructure CAs include a certificate policies extension asserting the OID(s) appropriate to the level of assurance with which it was issued.

A certificate issued by the FBCA will assert (as directed in the applicable LOA) in the certificate policies extension one or more of the OIDs listed in Table 7.1.6-1.

Table 7.1.6-1 FBCA Policy OIDs

FBCA Policy	OID
id-fpki-certpcy-rudimentaryAssurance	::= { 2.16.840.1.101.3.2.1.3.1 }
id-fpki-certpcy-basicAssurance	::= { 2.16.840.1.101.3.2.1.3.2 }
id-fpki-certpcy-mediumAssurance	::= { 2.16.840.1.101.3.2.1.3.3 }
id-fpki-certpcy-mediumHardware	::= { 2.16.840.1.101.3.2.1.3.12 }
id-fpki-certpcy-medium-CBP	::={ 2.16.840.1.101.3.2.1.3.14 }
id-fpki-certpcy-mediumHW-CBP	::={ 2.16.840.1.101.3.2.1.3.15 }
id-fpki-certpcy-mediumDevice	::= { 2.16.840.1.101.3.2.1.3.37}
id-fpki-certpcy-mediumDeviceHardware	::= { 2.16.840.1.101.3.2.1.3.38}
id-fpki-certpcy-highAssurance	::= { 2.16.840.1.101.3.2.1.3.4 }
id-fpki-certpcy-pivi-hardware	::={ 2.16.840.1.101.3.2.1.3.18 }
id-fpki-certpcy-pivi-cardAuth	::={ 2.16.840.1.101.3.2.1.3.19 }

id-fpki-certpcy-pivi-contentSigning	::= { 2.16.840.1.101.3.2.1.3.20 }

A certificate issued by the FCPCA will assert (as directed by the applicable LOA) in the certificate policies extension one or more of the OIDs listed in Table 7.1.6-1.

Table 7.1.6-2 FCPCA Policy OIDs

FCPCA	OID
id-fpki-common-policy	::= {2.16.840.1.101.3.2.1.3.6}
id-fpki-common-hardware	::= {2.16.840.1.101.3.2.1.3.7}
id-fpki-common-devices	::= {2.16.840.1.101.3.2.1.3.8}
id-fpki-common-authentication	::= {2.16.840.1.101.3.2.1.3.13}
id-fpki-common-High	::= {2.16.840.1.101.3.2.1.3.16}
id-fpki-common-cardAuth	::= {2.16.840.1.101.3.2.1.3.17}
id-fpki-common-devicesHardware	::= {2.16.840.1.101.3.2.1.3.36}
id-fpki-common-piv-contentSigning	::= {2.16.840.1.101.3.2.1.3.39}

A certificate issued by the SHA1 FRCA will assert (as directed by the applicable LOA) in the certificate policies extension one or more of the OIDs listed in Table 7.1.6-3.

Table 7.1.6-3 SHA1 FRCA Policy OIDs

SHA1 FRCA Policy	OID
id-fpki-SHA1-policy	::= {2.16.840.1.101.3.2.1.3.23}
id-fpki-SHA1-hardware	::= {2.16.840.1.101.3.2.1.3.24}
id-fpki-SHA1-devices	::= {2.16.840.1.101.3.2.1.3.25}

The FPKIMA will verify that the certificate policies extension asserts the OID(s) as specified in the LOA.

7.1.7 Usage of Policy Constraints Extension

Policy constraints appear in certificates only when the FPKIPA directs the FPKIMA to inhibit policy mapping as specified in the LOA.

7.1.8 Policy Qualifiers Syntax and Semantics

The cross-certificates issued by FPKI Trust Infrastructure CAs do not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificates issued by FPKI Trust Infrastructure CAs do not contain a critical certificate policy extension.

7.2 CRL PROFILE

FPKI Trust Infrastructure CAs issue CRLs in accordance with [FPKI-Prof], [PIV-I-Prof], and [CCP-Prof], as applicable.

7.2.1 Version Number(s)

FPKI Trust Infrastructure CAs issue X.509 version two (2) CRLs.

7.2.2 CRL and CRL Entry Extensions

FPKI Trust Infrastructure CAs generate CRLs in conformance with [FPKI-Prof], [PIV-I-Prof], and [CCP-Prof] at least every 12 hours with an 18 hour nextUpdate time.

7.3 OCSP PROFILE

The FPKIMA does not plan to support the Online Certificate Status checking Protocol (OCSP) capability for its cross-certificates.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT

The FPKIMA will arrange, initially and annually, for independent inspections and compliance audits to validate that the FPKI Trust Infrastructure CAs are operating in accordance with the security practices and procedures described in this CPS. Results of the compliance audit will be provided to the FPKIPA in the form of an Auditor Letter of Compliance that follows the FPKIPA Audit Letter Guidelines.

As an alternative to a full annual compliance audit against the entire CPS, the compliance audit of CAs and RAs may be carried out in accordance with the requirements as specified in the FPKI Compliance Audit Requirements document which state after an initial compliance audit, subsequent compliance audits require review of previous year's discrepancies, evaluation of modifications and changes made over the last year, core criteria and triennial criteria.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The FPKI compliance audits will be provided by an independent Auditor as agreed between the FPKIPA and FPKIMA. The Auditor selected will be a Certified Information System Auditor (CISA), IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices. The Auditor must perform such compliance audits as a regular ongoing business activity. The Auditor selected will have a demonstrated proven track record in one or more of the following areas:

- Specialization in Electronic Data Processing (EDP) security audit;
- Knowledge and experience with Compliance Audits and PKI;
- Independence from the organization being audited; or
- Understanding of the federal certification and accreditation process required by OMB A-130 and the Federal Information Security Management Act (FISMA) of 2002 (Public Law 107-347).

The selected Auditor will verify and validate, through document reviews and demonstrations, that the FPKIMA complies with [FBCA CP] and [FCPF CP].

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

As required by FISMA, the selected FPKI Compliance Auditor is a contractor that is independent from the FPKIMA, FPKIPA, and ICAMSC. This contractor provides an unbiased, independent evaluation and is one whose primary responsibility is the performance of EDP Compliance Audits.

To insure independence and objectivity, the FPKI Compliance Auditor may not have served the FPKIMA in developing or maintaining the FPKI's Facility or CPS.

8.4 TOPICS COVERED BY ASSESSMENT

The compliance audit will address all aspects of FPKI Trust Infrastructure operation, or that portion specified for a given year in accordance with the FPKI Compliance Audit Requirements document. The compliance audit will verify that FPKI Trust Infrastructure CAs are operated in compliance with all the requirements of the current versions of the applicable CPs and this CPS. The audit shall also verify that the FPKIMA is implementing the relevant provisions of the MOAs between the FPKI Policy Authority and each Entity PKI.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Within 24 hours after the conclusion of the compliance audit, the FPKI Compliance Auditor will notify the FPKIMA of the results of the compliance audit by e-mail and/or out-of-band writing.

The FPKIMA will provide the audit results to the FPKIPA chair, and in consultation with the FPKIPA chair, will have 10 business days to review the results and the recommendations from the compliance audit to determine the action to be taken.

Based on the findings of the FPKI Compliance Auditor, a Plan of Action and Milestones (POA&M) will document what steps must be taken. Possible steps include:

- Correction of deficiencies prior to implementing full operation of the FPKI Trust Infrastructure or within another time period as determined by the FPKIPA and FPKIMA;
- Suspension of full operation of one or more of the FPKI Trust Infrastructure CAs (this alternative will execute the emergency procedure described in Section 4.9.1 for revocation of certificates);
- The FPKIMA shall determine what further notifications or actions are necessary to meet the requirements of [FBCA CP], [FCPF CP], and the MOAs, and then proceed to make such notifications and take such actions without delay;
- Execute other corrective actions through procedures developed and published by the FPKIPA; and
- Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the FPKIPA may direct the FPKIMA to take additional actions as appropriate, including temporarily halting operation of one or more of the FPKI Trust Infrastructure CAs.

If the FPKIPA receives a report of audit deficiency from an Entity, the FPKIPA may direct the FPKIMA to take additional actions to protect the FPKI Trust Infrastructure's level of trust by revoking cross-certificates issued to that Entity (this alternative will execute the revocation procedure described in Section 4.9.1), or take other actions it deems appropriate.

8.6 COMMUNICATION OF RESULTS

The Compliance Auditor will submit a compliance audit written report (via signed e-mail and/or in writing) to the FPKIMA 24 hours after audit conclusion. The report will contain a summary table of topics covered, areas in which one or more of the FPKI Trust Infrastructure CAs were found to be non-compliant, a brief description of the problem(s) for each area of non-compliance, and possible remedies for each area. A more comprehensive report may be provided later.

Within 30 days of receipt of the written audit report, the FPKIMA will provide the audit results and corrective actions to the FPKIPA.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

The FPKIPA reserves the right to charge a fee to each Entity in order to support operations of the FPKI Trust Infrastructure.

9.1.1 Certificate Issuance or Renewal Fees

At this time, the FPKIMA does not charge a fee for certificate issuance or renewal.

9.1.2 Certificate Access Fees

At this time, the FPKIMA does not charge a fee for certificate access.

9.1.3 Revocation or Status Information Access Fee

At this time, the FPKIMA does not charge a fee for access to certificate revocation or status information.

9.1.4 Fees for Other Services

At this time, the FPKIMA does not charge a fee for any other services.

9.1.5 Refund Policy

At this time, since there are no fees associated with FPKIMA services, there is no refund policy in place.

9.2 FINANCIAL RESPONSIBILITY

This CPS contains no limits on the use of any certificates issued by the FPKI Trust Infrastructure CAs or by Entity CAs. Rather, entities acting as Relying Parties shall determine what financial limits, if any, they wish to impose for certificates used to complete a transaction.

9.2.1 Insurance Coverage

The FPKIMA does not provide any insurance or warranty coverage for the use of any certificates issued either by the FPKI Trust Infrastructure CAs or any cross-certified Entity CA.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

FPKI Trust Infrastructure information not requiring protection is publicly available in either the FPKI Repositories, the FPKIPA web site, or the FPKIMA web site. FPKIPA access to Entity information is addressed in the MOA with that Entity. Public access to Entity information is determined by the respective Entity.

9.3.1 Scope of Confidential Information

The FPKIMA does not maintain any confidential information about Entity CAs.

9.3.2 Information Not Within the Scope of Confidential Information

[FBCA CP] does not stipulate requirements for this Section.

9.3.3 Responsibility to Protect Confidential Information

Any information about Entity CAs that is not publicly available will be treated as confidential by FPKIMA personnel.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

The initial FPKIMA Privacy Impact Assessment determined there was no requirement for a Privacy Plan as no personal data/information is collected on the general public or government employees.

9.4.2 Information Treated as Private

All archive records will be treated as Controlled Unclassified Information (CUI) and will only be released as requested by the FPKIPA or as required by law. This includes any identity authentication and registration information collected from the Entity CAs.

The certificate issuance paper files are stored in the server room, leveraging the physical security requirements detailed in Section 5.1, until they are processed for audit review and archival by the Auditor. A copy of each certificate issuance paper file remains in binders secured inside the server room after the originals are processed for audit review and archival.

Information stored on FPKI Trust Infrastructure systems, including the FPKI Trust Infrastructure workstations, leverage the physical security requirements of the server room as detailed in Section 5.1. Access to the FPKI Trust Infrastructure systems is protected by password, limited to those in Trusted Roles, and security and access control settings are applied through group policies.

9.4.3 Information Not Deemed Private

FPKI Trust Infrastructure certificates are public certificates. Information about entities cross-certified with the FPKI Trust Infrastructure is maintained on the FPKIPA web site. Therefore, information included in FPKI Trust Infrastructure certificates and about what PKIs are cross-certified is not subject to protections outlined in Section 9.4.1.

9.4.4 Responsibility to Protect Private Information

Sensitive information is stored securely and released only in accordance with the provisions of Section 9.4.

9.4.5 Notice and Consent to Use Private Information

The FPKIMA does not issue certificates to subscribers or Entity personnel, and is not required to provide any notice or obtain the consent of the Subscriber or Entity personnel in order to release private information in accordance with the stipulations of Section 9.4.6.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The FPKIMA will disclose confidential information to any third party when required by this CPS, [FBCA CP], [FCPF CP], law, government rule or regulation, or order of a court of competent jurisdiction. Any request for release of information will be authenticated. The authentication will consist of validating the identity of the requester using two forms of photo

identifications. The individual's authority to obtain the information will be validated using at least one of the following means:

- The individual has the duly-executed court order from a Federal court;
- The individual has duly-executed request from the respective Agency Office of Inspector General;
- The individual is the Subscriber itself; or
- The individual has a duly-signed request from the Subscriber requesting the release of the information from the Subscriber.

In compliance with 41 CFR 105-60.605, the FPKIMA Program Manager will be notified of any validated requests for disclosure of confidential information. The FPKIMA Program Manager will notify the Appropriate Authority.

9.4.7 Other Information Disclosure Circumstances

There are no other disclosure circumstances.

9.5 INTELLECTUAL PROPERTY RIGHTS

While executing the certificate management and operational practices of this CPS, the FPKIMA will not knowingly violate intellectual property rights held by others.

The U.S. Government retains exclusive rights to any products or information developed under or pursuant to this FPKI CPS.

9.6 REPRESENTATIONS AND WARRANTIES

The obligations described below pertain to the FPKI Trust Infrastructure CAs (and, by implication, the FPKIMA, and Entity CAs that either interoperate with the FPKI Trust Infrastructure CAs or are in a trust chain up to an Entity CA that interoperates with the FPKI Trust Infrastructure). The obligations applying to Entity CAs pertain to their activities as issuers of certificates. Further, the obligations focus on Entity CA obligations affecting interoperability with the FPKI Trust Infrastructure. Thus, where the obligations include, for example, a review (or audit) by the FPKIPA or some other body of an Entity's CA operation, the purpose of that review pertains to interoperability using the FPKI Trust Infrastructure CAs, and whether the Entity is complying with the MOA.

9.6.1 CA Representations and Warranties

FPKI Trust Infrastructure CA cross-certificates are issued and revoked at the sole discretion of the FPKIPA. The FPKIMA warrants that FBCA and FCPCA operational procedures comply with this CPS, as well as [FBCA CP] and [FCPF CP] respectively.

9.6.2 RA Representation and Warranties

The FPKIMA makes no representation or warranty that the information in a cross-certificate is accurate, other than it matches the information specified in the LOA authorizing the issuance of that certificate.

9.6.3 Subscriber Representations and Warranties

The FPKI Trust Infrastructure CAs do not issue subscriber certificates.

9.6.4 Relying Parties Representations and Warranties

The FPKIMA makes no representation or warranty about the use of certificates issued by Entity PKIs for Relying Parties.

9.6.5 Representations and Warranties of Other Participants

The FPKIMA makes no representation or warranty for other participants.

9.7 DISCLAIMERS OF WARRANTIES

The FPKIMA does not disclaim any responsibilities described in [FBCA CP] and [FCPF CP].

9.8 LIMITATIONS OF LIABILITY

Certificates are issued and revoked at the sole discretion of the FPKIPA. When the FBCA or SHA1 FRCA issues a cross-certificate to a non-federal Entity, it does so for the convenience of the Federal Government. Any review by the FPKIPA of a non-federal Entity's certificate policy is for the use of the FPKIPA in determining whether or not interoperability is possible, and if possible, to what extent the non-federal Entity's certificate policy maps to [FBCA CP]. A non-federal Entity must determine whether that Entity's certificate policy meets its legal and policy requirements. Review of a non-federal Entity's certificate policy by the FPKIPA is not a substitute for due care and mapping of certificate policies by the non-federal Entity.

Entities acting as Relying Parties are responsible for determining what financial limits, if any, they wish to impose for certificates used to consummate a transaction. This is entirely at the discretion of the Entity as Relying Party and is likely to depend upon several factors in addition to the certificate assurance level (e.g., likelihood of fraud, other procedural controls, Entity-specific policy or statutorily imposed constraints).

As an example, one Entity may be willing to accept a FBCA Basic assurance level certificate for transactions of a specific financial value for which another Entity would require a FBCA High assurance level certificate.

Neither the FPKIPA nor the FPKIMA is financially responsible for any losses incurred from using its services.

9.9 INDEMNITIES

This FPKI CPS does not include any claims of indemnity.

9.10 TERM AND TERMINATION

9.10.1 Term

This CPS becomes effective when approved by the FPKIPA. This CPS has no specified term.

9.10.2 Termination

Termination of this CPS is at the discretion of the FPKIPA.

9.10.3 Effect of Termination and Survival

The requirements of [FBCA CP] and [FCPF CP] remain in effect through the end of the archive period for the last certificate issued.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

The FPKIMA use the POC information provided by the FPKIPA in LOAs and MOAs, and as updated by Entity authorized officials, when communicating with Entities . The FPKIPA listservs maintained by the FPKIMA on behalf of the FPKIPA will also be used for communications to Entities.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The FPKIMA shall review the FPKI CPS at least once every year, or when a change is made to [FBCA CP] or [FCPF CP]. If the FPKIMA determines modifications to this CPS are required, the change, a change justification, and contact information for the person requesting the change will be presented to the FPKIPA for review and acceptance.

9.12.2 Notification Mechanism and Period

[FBCA CP] and [FCPF CP], and any subsequent changes shall be made publicly available. The redacted FPKI CPS and any subsequent changes shall be made publicly available.

9.12.3 Circumstances under which OID must be changed

If the FPKIPA determines that there is a requirement to change the OIDs defined in [FBCA CP], the FPKIPA will vote to amend [FBCA CP].

If the FPKIPA determines that there is a requirement to change the OIDs defined in [FCPF CP], the FPKIPA will vote to amend [FCPF CP].

9.13 DISPUTE RESOLUTION PROVISIONS

The FPKIPA will resolve any disputes associated with the use of the FPKI Trust Infrastructure or certificates issued by the FPKI Trust Infrastructure CAs.

9.14 GOVERNING LAW

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

Where an inter-governmental dispute occurs, resolution will be according to the terms of the MOA.

9.15 COMPLIANCE WITH APPLICABLE LAW

The FPKIMA will comply with applicable law.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire agreement

There are no additional miscellaneous provisions on this CPS.

9.16.2 Assignment

This FPKI CPS does not assign rights or responsibilities other than what is specified in this CPS, [FBCA CP], [FCPF CP], and MOAs with cross-certified Entities.

9.16.3 Severability

Should it be determined that one Section of this CPS is incorrect or invalid, the other Sections of this CPS shall remain in effect until the CPS is updated. The process for updating this CPS is described in Section 9.12.1.

9.16.4 Enforcement (Attorney's Fees or Waiver of Rights)

Failure by any person to enforce a provision of this CPS will not be deemed a waiver of future enforcement of that or any other provision.

9.17 OTHER PROVISIONS

This CPS does not stipulate any additional provisions.

Appendix A References

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

ABADSG	Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html
BCCP	FPKI Business Continuity and Contingency Plan, 8 January 2001
CCP-Prof	X.509 Certificate and CRL Extensions Profile for the Common Policy, December 8, 2003.
CITE	Community Interoperability Test Environment (CITE) http://www.idmanagement.gov/documents/community-interoperability-test-environment-cite-participation-guidance
Crits and Methods	Criteria and Methodology For Cross-Certification with the U.S. Federal Bridge Certification Authority (FBCA) http://www.idmanagement.gov/documents/cross-certification-methodology-and-criteria
Cross Certificate Application Template	Cross Certificate Application Template http://www.idmanagement.gov/criteria-and-methodology
DR	FPKI Contingency Plan, v0.1.2, December 6, 2010
FBCA CP	X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) http://www.idmanagement.gov/documents/certificate-policy-federal-bridge-certificate-authority
FCPF CP	X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework http://www.idmanagement.gov/documents/federal-pki-common-policy-framework-certificate-authority
FIPS 140-2	Security Requirements for Cryptographic Modules May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 186-3	Digital Signature Standard, June 2003. http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf
FISMA	Federal Information Security Management Act of 2002 (44 U.S.C. § 3541) http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
FOIACT	5 U.S.C. 552, Freedom of Information Act. http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm

FPKI Compliance Audit Requirements	FPKI Compliance Audit Requirements, April 10, 2012, Version 2.0.0 http://www.idmanagement.gov/documents/fpki-compliance-audit-requirements
FPKI-Prof	Federal PKI X.509 Certificate and CRL Extensions Profile http://www.idmanagement.gov/documents/fpki-x509-certificate-and-crl-extensions-profile
FPKI Security Profile	FPKI Security Controls Profile of Special Publication 800-53, Security Controls for PKI Systems http://www.idmanagement.gov/documents/fpki-security-controls-profile-special-publication-800-53-security-controls-pki-systems
FPKI SSP	Federal Public Key Infrastructure (FPKI) Trust Infrastructure System Security Plan
FPKIMA IMP	FPKIMA Incident Management Plan
ISO9594-8	Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate Framework, 2008 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53372
NAG69C	Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.
NIST SP 800-53	Recommended Security Controls for Federal Information Systems and Organizations http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
NSD42	National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. http://www.fas.org/irp/offdocs/nsd/nsd_42.htm
CNSSP-1	CNSS Policy No.1, National Policy for Safeguarding and Control of COMSEC Materials, September 2004 http://www.cnss.gov/Assets/pdf/cnssp_1.pdf
NS4009	NSTISSI 4009, National Information Assurance (IA) Glossary http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
OMB M-04-04	Office of Management and Budget (OMB) Memorandum, E-Authentication Guidance for Federal Agencies http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

PIV-I-Prof	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards http://www.idmanagement.gov/documents/piv-i-x509-certificate-and-certificate-revocation-list-crl-extensions-profile
PKCS#7	Cryptographic Message Syntax Standard http://www.rsa.com/rsalabs/node.asp?id=2129
PKCS#10	Certification Request Syntax Standard http://www.rsa.com/rsalabs/node.asp?id=2132
RFC 2510	Certificate Management Protocol, Adams and Farrell, March 1999 http://www.ietf.org/rfc/rfc2510.txt
RFC 5280	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Housley et al., April 2008. http://www.ietf.org/rfc/rfc5280.txt
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003 http://www.ietf.org/rfc/rfc3647.txt
RFC 4122	A Universally Unique IDentifier (UUID) URN Namespace http://www.ietf.org/rfc/rfc4122.txt
SCEPACS	Technical Implementation Guidance: Smart Card Enabled Physical Access Control http://fips201ep.cio.gov/documents/TIG_SCEPACS_v2.2.pdf
SSP NAV	Shared Service Provider Roadmap: Navigating the Process to Acceptance http://www.idmanagement.gov/documents/shared-service-provider-roadmap-navigating-process-acceptance
SSP-REP	Shared Service Provider Repository Requirements http://www.idmanagement.gov/documents/shared-service-provider-repository-service-requirements