FBCA Certificate Policy Change Proposal Number: 2022-04

To: Federal PKI Policy Authority (FPKIPA)
From: Federal PKI Certificate Policy Working Group (CPWG)
Subject: Proposed modifications to the Federal Bridge Certification Authority Certificate Policy and certificate profile specification
Date: July 12, 2022

Title: Consolidated update to the Federal Bridge Certification Authority Certificate Policy and associated profiles

Version and Date of Certificate Policy Requested to be changed:

- *X.509 Certificate Policy For The Federal Bridge Certificate Authority (FBCA) Version 2.36, May 6, 2022*

Change Advocate's Contact Information:
Organization: FPKI Policy Authority
E-mail address: fpki@gsa.gov

Organization requesting change: FPKI Certificate Policy Working Group

Change summary: This is a comprehensive update to the FBCA CP and the associated certificate profile specification (formerly titled "Federal Public Key Infrastrucure (PKI) X.509 Certificate and CRL Extensions Profile"). High-level update summary:

- Standardized terminology
- Realigned requirements with appropriate policy sections
- Increased use of tables to improve readability
- Aligned requirements with observed practices
- Clarified definitions of certificate types
- Streamlined certificate naming
- Updated certificate re-key, renewal, and modification definitions for clarity
- Removed SHA-1 references
- Updated permitted key sizes and algorithms
- Converted sections after Section 9 to appendices
- Updated format and content of certificate profiles
    - Aligned profiles with proposed updates to Common Policy
    - Consolidated relevant "PIV-I" profiles
    - Split Cross Certificate profile into two profiles (Cross certificate and Intermediate CA) to help clarify requirements and reduce confusion

- Numerous worksheet updates (see Appendix B)

Background: This update consolidates CPWG policy recommendations dating back to 2018. It also cleans-up outdated references and requirements, clarifies existing requirements, aligns policy with observed agency practices (e.g., certificate naming), and improves readability.

Updates related to the following topics were discussed with CPWG members to minimize adverse impact:

- Allowance of code signing certificates
- Bridge partner certificate policy public posting
- Device naming and issuance guidance
- Allowance of wildcard certificates
- Allowance of electronic authentication for "derived" certificates
- PIV-I biometric retention update
- UUID publication restriction
- Personnel training requirements updates
- Log processing frequency updates
- Archive retention periods updates
- Business continuity after disaster allowances
- CA cryptographic module requirement updates
- Certificate profile changes
    - Consolidation with PIV-I profiles
    - Specification of PIV-I-hardware OID usage only for authentication certificate

Specific Changes: Due to format changes and the number of edits, updates were highlighted to CPWG and FPKIPA members in separate, redlined versions of Common Policy.

Change Impact:

- Potential impacts resulting from the proposed updates to the FBCA Certificate Policy are included in Appendix A.
- Potential impacts resulting from the proposed updates to the certificate profiles are included in Appendix B.

Estimated Cost: TBD

Implementation Date: September 1, 2023

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:
Date presented to CPWG: December 7, 2021
Date change released for comment: May 3, 2022
Date comment adjudication published: June 24, 2022

APPENDIX A: IMPACT OF POLICY UPDATES

Policy Change Summary	Impact
Overall • Standardized terminology ("Human Subscriber", "Device", "must", "publicly accessible", etc.) • Clarified and streamlined language • Standardized formatting of "Practice Notes" and external references • Deprecated algorithms (e.g., SHA-1), and removed unused references • Relocated requirements to more applicable policy sections	No negative impact
Section 1 • Introduction streamlined and CP OIDs tabularized for more efficient reading/reference • Certification Authorities was expanded to define system software layers in alignment with Common v2.2 • PKI authorities expanded to align with recent Common versions to include definitions of Key Recovery Authorities; correlates CA requirements to KED/DDS, RA requirements apply to KRA/KRO systems	No negative impact Allows CA use of virtualization/containers provided security requirements are met None - all Key Recovery requirements were already active in the KRP
Section 2 • Modified to align to Common v2.0: o now allows for AIA bundles to include .cer DER encoded certificates, o now requires Entity CPs to be publicly posted, o now explicitly requires PIV-I issuing CAs to support OCSP o Now explicitly allows for certificates and statuses to be replicated	No negative impact: • .cer allowance accounts for known practices, • all Entity CPs are already publicly posted, • all known PIV-I issuers already maintain OCSP • replication accounts for practices
Section 3 Created sub-sections for Subject Names and Subject Alternative names (aligns with Common v2.0) • Device certificate names are now addressed and must not take the same name form as a human subject	No negative impact: • device name guidance is very broad

• PIV-I SAN details are included to align to PIV-I profiles • Wildcard certificate allowances were make for serverAuth device certificates with similar requirements for the Common allowance	• aligns with PIV-I profiles Allows - wildcard certificate issuance/usage
The initial identity authentication sub-section was reorganized for readability, as well as: • Allowance for 'electronic authentication' (similar to derived capabilities in Common) provided certain conditions and processes are followed • Restriction on device certificate to only be issued within one organization was removed for interoperability	Allows: • a similar capability to derived • organizations to issue device certificates to partners
The routine rekey identity verification was migrated up to 12 years (from 9) for medium certificates to align with Common v2.0	None - Less restrictive timeline every 12 years
A new Section 3.5 was created on identification and authentication for key recovery requests in alignment with Common v2.1	None - incorporated as part of the KRP consolidation
Section 4 Reorganized to align to Common v2.0, additional changes include: • Certificate applications now must be processed within 90 days of identity verification	None - up from 30 days
• Entity CAs must now notify subscribers when PIV-I certificates are available (previously a no stipulation)	Potential need for notifications to subscriber
• A restriction in publication of PIV-I Authentication and PIV-I Card Authentication certificates was stipulated	None - these are generally not published
• Private key security is now generalized for all FBCA certificate policies (previously Medium and above)	Potential need to update Basic agreements
• Circumstances for Certificate renewal, rekey, modification and revocation expanded for clarity	None - adds clarity to established processes

• CRL issuance frequency aligned to Common (24 hours online and 35 days for offline), offline defined • Certificate suspension limits now defined (no longer than the life of the certificate) to assist with CRL hygiene • Key Recovery responsibilities and processes incorporated from KRP consolidation	None - less restrictive than current policy Entities may need to plan for CRL removal (if they support suspension) None - aligns with KRP
Section 5 Reorganized to align to Common, changes include: • Physical access requirements for Key Recovery systems added • Trusted roles section expanded to address RA (as officers) and Key Recovery roles and responsibilities • Key Recovery system principles and mechanisms, disaster recovery/business continuity procedures, and CP/CPS stipulations added to personnel training requirements (if applicable) • Audit logging and Archive sections updated to align to Common v2.2 o Audit logs must be reviewed once per month for basic and above (down from once every two months and now includes basic) o Archive retention periods updated to be more specific for certain types of records (CA records for 3 years after the lifetime of hte CA) and it now provides flexibility for archiving RA type records (3 years after certificate expiration) • Private key compromise procedures expanded to account for KRS per KRP consolidation • 72 hour reconstitution timeline after disaster removed in favor of defined recovery procedures	None: • Aligns to KRP • Updated Roles are definitional • Training is inferred based on job role Potential need to plan for more frequent log processing Potential to extend archive retention periods for some CAs, but more flexible for other types of records None - incorporated as part of KRP None - less restrictive
Section 6 Reorganized to align to Common, changes include: • Key sizes/algorithms streamlined and updated to align to Common v2.0 and SP 800-78 (Removed references to SHA-1) • Key usage purposes made critical and updated to align to Common v2.0	None - approved key sizes tabularized, SHA1 depricated Key usage must be specified and must not contain anyEKU

• CA private key storage now requires FIPS 140 Level 3 in alignment with Common • OCSP responder certificates are limited to a maximum lifetime of 120 days (down from 10 years), key pair can still be used for up to 3 years • Computer security technical requirements extended to all system software layers, references to VM/VME removed in alignment with Common v2.2 • Network security controls aligned to Common v2.0	Potential for CAs to upgrade HSMs OCSP certificates must be renewed within 120 days Allowance for containers None – reorganized for clarity
Section 7 • FBCA Profiles now referenced as [FBCA-Prof] • Object algorithm identifiers reduced to align to Common v2.0 and SP 800-78 • Entity CAs may now assert name constraints in CA certificates • All SHA1 references removed •	No negative impact: • algorithms not in use removed • less restrictive • no current SHA1 CAs/certs
Section 8 • No major updates	No negative impact
Section 9 • Restriction on publication of UUID moved to Section 4	No negative impact
Appendix A – PIV-I Smartcard Definition • No updates	No negative impact
Appendix B – CMS Requirments • No updates	No negative impact
Appendix C – In-Person Antecedant • Process defined and requirements summarized, this is an abridged version of the supplementary guidance that was archived	No negative impact
Appendix D – In-Person Antecedant • Reference names updated where needed and to be consistent with Common, all links updated	No negative impact
Appendix E – In-Person Antecedent • Unused acronyms have been removed	No negative impact

Appendix F – Glossary • Unused terms removed • Some terms added for consistency and alignment with Common (e.g., system software layers, in-person tatntecedent)	No negative impact

APPENDIX B: IMPACT OF CERTIFICATE PROFILE UPDATES

Profile Changes	CAs Impacted*

PIV-I profile worksheets were consolidated with FBCA profiles to include:
• PIV-I Authentication Certificate
  ○ Clarifies that PIV-I-Hardware CP OID is reserved for the authentication certificate and not applicable to signature or KMK
• PIV-I Card Authentication Certificate
• PIV-I Content Signing Certificate
• Delegated OCSP Responder Certificate
Some PIV-I profiles were consolidated with existing FBCA profiles:
• PIV-I Digital Signature → Signature Certifidate
  ○ rfc822Name is required if id-kp-emailProtection is asserted in Extended Key Usage
• PIV-I Key Management → Key Management
  ○ rfc822Name is required if id-kp-emailProtection is asserted in Extended Key Usage
	5 PIV-I issuers may have to modify their signing and KMK profiles for different CP OIDs

Several new profiles were drafted to include: • Intermediate/Signing CA Certificate • Authentication Certificate (non-PIV-I) • Device Certificate	No negative Impact
Authority Information Access & Certificate Revocation List Distribution Point - Require HTTP URI first	0 impacted CAs
Authority Information Access - Allow .cer	No negative impact
DN Encoding: Allow only printableString and/or UTF8	No negative impact
Optionally allow Subject Directory Attributes (e.g., citizenship) for authentication certificates (General, PIV-I, PIV-I card authentication)	No negative impact
Cross Certificate • Clarify appropriate use of requireExplicitPolicy and inhibitPolicyMapping,	No negative impact
OCSP Responder Certificate • EKU must be marked critical	1 impacted Bridge member customer CA

Section 8 References – removed and FBCA CP Appendix D is linked	No negative impact

* based on 2021 Annual Review certificate samples

X.509 Certificate Policy for the

~~For The~~

Federal Bridge Certification Authority ~~(FBCA)~~

Version ~~2.36~~3.0 [DRAFT Revision 5]

~~6 May 2022~~

TBD

Signature Page

Co-chair, Federal Public Key Infrastructure Policy Authority DATE

~~Co-Chair, Federal Public Key Infrastructure Policy Authority DATE~~

Revision History

Document Version	Document Date	Revision Details
2.1	~~12~~ January 12, 2006	**2005-03~~,~~:** Changes to the FBCA CP to modify audit cycle for consistency with Government certification and accreditation process
2.2	~~28~~ September 28, 2006	**2006-02~~,~~:** Omnibus Policy Issues Raised During the CertiPath Mapping and e-Auth Business Rules Review
2.3	~~14~~ March 14, 2007	**2007-01~~,~~:** Harmonization between Federal Bridge and Common Policy Framework
2.4	~~13~~ June 13, 2007	**2007-02~~,~~:** Clarification on multiparty physical access control in Physical Access for CA Equipment
2.5	~~12~~ July 12, 2007	**2007-03~~,~~:** SAFE Harmonization Policy Change Recommendations
2.6	~~16~~ August 16, 2007	**2007-04~~,~~:** Citizenship/Security Clearance Policy
2.7	~~26~~ September 26, 2007	**2007-05~~,~~:** Alignment of Cryptographic Algorithm Requirements with SP 800-78-1
2.8	~~15~~ February 15, 2008	**2008-01~~,~~:** Alignment of Cryptographic Algorithm Requirements with NIST Special Publication 800-57
2.9	~~13~~ August 13, 2008	**2008-02~~,~~:** Changes to FBCA CP to clarify the archive definition and how its records are intended to be used **2008-03~~,~~:** § 8.3 Assessor's Relationship to Assessed Entity
2.10	~~16~~ October 16, 2008	**2008-04~~,~~:** § 1.2 Document Identification

2.11	~~20~~ November 20, 2008	**2008-05~~,~~:** Changes to FBCA CP to include a provision for a role-based signature certificate **2008-06~~,~~:** Change to CA Key Usage Period for CAs issuing end user certificates and clarification of organizational responsibilities concerning device certificates
2.12	~~11~~ February 11, 2009	**2009-01~~,~~:** Change to the FBCA CP to remove the requirement for backing up the archive
2.13	~~10~~ December 10, 2009	**2009-02~~,~~:** Change to the FBCA CP to align key length requirements with SP 800-57
2.14	~~20~~ January 20, 2010	**2010-01~~,~~:** Remote Administration of Certification Authorities
2.15	~~8~~ April 8, 2010	**2010-02~~,~~:** § 8.1 and 8.4
2.16	~~14~~ May 14, 2010	**2010-03~~,~~:** Certificate Policy Updates to Address PIV-I
2.17	~~10~~ June 10, 2010	**2010-04~~,~~:** Specify String Format for UUID in serialNumber RDN
2.18	~~15~~ August 15, 2010	**2010-05~~,~~:** Addition of the Real ID credential for States to use in meeting FPKI Identity Proofing requirements
2.19	~~15~~ October 15, 2010	**2010-06~~,~~:** Digitally Signed Declaration of Identity
2.20	~~18~~ November 18, 2010	**2010-07~~,~~:** Legacy use of SHA-1 during the transition period January 1, 2011 to December 31, 2013
2.21	~~16~~ December 16, 2010	**2010-08~~,~~:** Clarify requirements to support CA Key Rollover

2.22	~~24~~ January 24, 2011	**2011-01~~,~~:** Protection of Subscriber Information **2011-02~~,~~:** Specify requirement for Background Check Refresh
2.23	~~4~~ February 4, 2011	**2011-03~~,~~:** Clarify key generation location for PIV-I Key Management certificates
2.24	~~25~~ February 25, 2011	**2011-04~~,~~:** Clarify CMS requirements
2.25	~~13~~ December 13, 2011	**2011-05~~,~~:** Updates to Certificate Policy to add a New Device Specific Policy (superseded by 2011-07) **2011-06~~,~~:** Remove requirements for Lightweight Directory Access Protocol (LDAP) **2011-07~~,~~:** Updates to Certificate Policy to add two New Device Specific Policies (replaces 2011-05)
2.26	~~26~~ April 26, 2012	**2012-01~~.~~:** Clarify RA audit requirements: Insert new Section 1.3.1.6, replace second paragraph in Section 8, add new last sentence to second paragraph of Section 8.4, revise Section 8.6, revise "Policy Management Authority" glossary definition.
2.27	~~2~~ December 2, 2013	**2013-01~~.~~:** FBCA CP Clarifications recommended to the FPKIMA during the Annual PKI Compliance Audit. Allow modification of cross-certificates for corrections (Section 4.8.1) and Clarify division of responsibilities between trusted roles (Section 5.2.1). **2013-02~~.~~:** Move SHA-1 policies from Common Policy to FBCA and remove 12/31/2013 restriction on all SHA-1 policies.

2.28	~~14~~ January 14, 2016	**2015-01~~.~~:** Clarify assertion of policies for devices. Change to Section 1.2. **2015-02~~.~~:** Align PIV-I card life with FIPS 201-2. Change to Sections 6.2.1, 6.3.2, Appendix A item #10.
2.29	~~20~~ May 20, 2016	**2016-01~~.~~:** Added new Section 6.2.1.1; added "Custodial Subscriber Key Stores" to glossary.
2.30	~~5~~ October 5, 2016	**2016-02~~.~~:** Allow for Long-Term CRL for retired CA key. Added to Sections 5.6 and 5.8. **2016-03~~.~~:** Allow alternate FBCA key change procedures. Added to Section 5.6.
2.31	~~29~~ June 29, 2017	**2017-01:** Align with current FPKIMA practice for CA certificates **2017-02:** Requires CAs to publish information pertaining to resolved incidents on their websites. **2017-03:** Requires CAs to notify the FPKIPA whenever a change is made to their infrastructures **2017-04:** Clarifies the period of time PIV-I card stock may continue to be used once it has been removed from the GSA Approved Products List **2017-05:** CAs cross certified with the FBCA have a single trust path to the FBCA.
2.32	~~4~~ April 4, 2018	**2018-01:** Add requirements for key recovery

2.33	~~10~~ May 10, 2018	**2018-02:** Add reference to Annual Review Requirements **2018-03:** Mandate specific EKU in certificates issued after June 30, 2019 **2018-04:** Certificate revocation requirements for transitive closure after August 15, 2018. **2018-05:** Requirements for virtual implementations
2.34	~~4~~ October 4, 2018	**2018-06**~~.~~**:** Incorporate "supervised remote identity proofing" and other new guidance as defined in NIST SP 800-63-3 effective as of October 4, 2018
2.35	~~15~~ April 15, 2019	**2019-01**~~.~~**:** Modifications to allow the FBCA to be operated in an off-line status effective as of April 15, 2019
~~2.36~~3.0	~~6 May 2022~~TBD	~~**2022-02.** Allows Federally issued PIV-I credentials to leverage cardstock used for PIV issuance, including "pre-printed," agency seals.~~**2021-01:** Modifications to align with recent applicable modifications to Common Policy CP, to include Key Recovery Policy consolidation, updates to Audit and Archive Sections, allowance for containerized technologies, incorporation of electronic authentication capabilities, and definition of in-person antecedent processes.

Table of Contents

1. INTRODUCTION

This Certificate Policy (CP) defines ~~twelve~~a number of distinct certificate policies for use by the Federal Bridge Certification Authority (FBCA) to facilitate interoperability between ~~the FBCA and other~~cross-certified Entity PKI domains~~.~~ in a peer-to-peer fashion. The ~~policies represent six different assurance levels (Rudimentary, Basic, Medium, PIV-I Card Authentication, Medium Hardware, and High) for public key~~ FBCA certificates~~. In addition, two device certificate policies at~~ issued to Entity CAs define trust through use of the *policyMappings* extension in the certificates.

Each policy defines an~~Medium~~ assurance level ~~are defined to facilitate server to server authentication between FBCA and other PKI domains. The level of assurance~~which refers to the strength of the binding between the public key and the ~~individual whose~~ subject ~~name is cited in~~of the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.

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

In this document, the term "device" means a non-person entity, i.e., a hardware device or software application. ~~The use of SHA-1 to create digital signatures is deprecated beginning January 1, 2011 according to NIST SP 800-131. However, there are some applications in use within the federal government that cannot process certificates or certificate revocation information signed using SHA-256. Therefore, a parallel SHA-1 FPKI was created to facilitate the interoperability for those unable to transition to SHA-256 by January 1, 2011. Accordingly, this CP additionally defines five certificate policies for use by the SHA-1 Federal Root Certification Authority (SHA1 Federal Root CA) to facilitate interoperability between Federal agencies and other Entity PKI domains that require the use of SHA-1 after December 31, 2010. Use of certificates asserting certificate policy OIDs that identify the use of SHA-1 under this policy should be limited to applications for which the risks associated with the use of a deprecated cryptographic algorithm have been deemed acceptable and will only be asserted within the parallel SHA-1 FPKI. CAs that issue SHA-1 end entity certificates after December 31, 2010 shall not also issue SHA-256 certificates, asserting non-SHA-1 policies.~~

A Key Recovery System (KRS) may be supported by Entity CAs that issue key management certificates. The KRS provides the computer system hardware, software, staff, and procedures to escrow private keys securely and recover them when appropriate.

~~Personal Identity Verification Interoperable (PIV-I) policies for PIV-I Hardware, PIV-I Card Authentication, and PIV-I Content Signing are for use with PIV-I smart cards (see Appendix A for more information).~~

~~The FBCA enables interoperability among Entity PKI domains in a peer-to-peer fashion. The FBCA issues certificates only to those CAs designated by the Entity operating that PKI (called~~

~~"Principal CAs"). The FBCA may also issue certificates to individuals who operate the FBCA. The FBCA certificates issued to Principal CAs act as a conduit of trust.~~

Any use of or reference to this ~~FBCA~~ CP ~~outside~~beyond the ~~purview~~context of the Federal PKI ~~Policy Authority~~(FPKI) is ~~completely~~ at the ~~using party's~~ risk~~. An Entity shall not assert the FBCA CP OIDs in any certificates the Entity CA issues, except in the *policyMappings* extension establishing an equivalency between an FBCA OID and an OID in the Entity CA's CP.~~ of the relying party.

This ~~FBCA CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Certificate Policy and Certification Practices~~CP follows the RFC 3647 framework.

~~The terms and provisions of this FBCA CP shall be interpreted under and governed by applicable Federal law.~~

1.1 OVERVIEW

1.1.1 FBCA Certificate Policy (CP)

FBCA certificates contain ~~a~~one or more registered certificate policy object ~~identifier~~identifiers (OID), which may be used by a relying party to decide whether a certificate is trusted for a particular purpose. ~~The~~ Each OID corresponds to a specific level of assurance established by this Certificate Policy (CP~~) which shall be available to Relying Parties. Each certificate issued by the FBCA will assert the appropriate level of assurance in the *certificatePolicies* extension.~~).

1.1.2 Relationship between the FBCA CP ~~&~~and the FBCA CPS

~~The FBCA~~This CP states ~~what assurance can be placed in a certificate~~the requirements for the issuance and management of certificates issued by the FBCA~~.~~, and requirements for the operation of the FBCA. The FBCA Certification ~~Practices~~Practice Statement (CPS) states how the FBCA ~~establishes that assurance~~implements the requirements.

1.1.3 Relationship between the FBCA CP and the Entity CP

This CP establishes criteria for cross-certification with Entity CAs. The FPKI Policy Authority maps Entity CP(s) to one or more of the ~~levels of assurance~~policies in the FBCA CP. The relationship between ~~these CPs~~an Entity CP and the FBCA CP is asserted in the *policyMappings* extension of the CA certificates issued to the Entity CA by the FBCA.

Entities may undertake a similar mapping process and issue a cross-certificate to the FBCA asserting the relationship of their policies to the policies defined in ~~the policyMappings extension.~~ this CP.

1.1.4 Scope

The FBCA exists to facilitate trusted electronic business transactions for Federal organizations. To facilitate the missions of the organizations, interoperability is offered to non-Federal entities. The generic term "entity" applies equally to Federal organizations and other organizations owning or operating PKI domains. As used in this CP, Entity PKI or Entity CA may refer to an

organization's PKI, a PKI provided by a commercial service, or a bridge CA serving a community of interest.

1.1.5 Interaction with PKIs External to the Federal Government

The FBCA will extend interoperability ~~with~~to non-Federal entities only when it is beneficial to the Federal Government.

1.2 DOCUMENT NAME AND IDENTIFICATION

~~There are twelve policies specified at six different levels of assurance in this~~This is the X.509 Certificate Policy~~, which are defined in subsequent sections. Each level of assurance has an~~ for the FBCA.

~~Object Identifier (OID), to be asserted in~~ Certificates issued by the FBCA~~.~~ will assert at least one of the following OIDs in the *certificatePolicies* extension. Entity ~~Principal~~ CAs may assert these OIDs only in *policyMappings* extensions of certificates issued to the FBCA. ~~The FBCA policy OIDs are registered in the NIST Computer Security Objects Registry as follows:~~

Table 1 - FBCA Certificate Policies

csor-certpolicy OBJECT IDENTIFIER	::= { 2 16 840 1 101 3 2 1 }
fbca-policies OBJECT IDENTIFIER	::= { csor-certpolicy 3 }
id-fpki-certpcy-rudimentaryAssurance	::= { fbca-policies2 16 840 1 101 3 2 1 3 1}
id-fpki-certpcy-basicAssurance	::= { fbca-policies 2 16 840 1 101 3 2 1 3 2}
id-fpki-certpcy-mediumAssurance	::= { fbca-policies2 16 840 1 101 3 2 1 3 3}
id-fpki-certpcy-mediumHardware	::= { fbca-policies2 16 840 1 101 3 2 1 3 12}
id-fpki-certpcy-medium-CBP	::= { fbca-policies ::= {2 16 840 1 101 3 2 1 3 14}
id-fpki-certpcy-mediumHW-CBP	::= { fbca-policies ::= {2 16 840 1 101 3 2 1 3 15}
id-fpki-certpcy-mediumDevice	::= { fbca-policies2 16 840 1 101 3 2 1 3 37}
id-fpki-certpcy-mediumDeviceHardware	::= { fbca-policies2 16 840 1 101 3 2 1 3 38}
id-fpki-certpcy-highAssurance	::= { fbca-policies2 16 840 1 101 3 2 1 3 4}
id-fpki-certpcy-pivi-hardware	::= { fbca-policies2 16 840 1 101 3 2 1 3 18}
id-fpki-certpcy-pivi-cardAuth	::= { fbca-policies2 16 840 1 101 3 2 1 3 19}
id-fpki-certpcy-pivi-contentSigning	::= { fbca-policies2 16 840 1 101 3 2 1 3 20}

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

~~defined for the Medium Hardware Assurance policy with the exception of identity proofing, re-key, and activation data. In this document, the term "device" is defined as~~Human Subscriber Certificates

Certificates valid for the following policies are issued to Human Subscribers:

~~a non-person entity, i.e., a hardware device or software application. The use of the mediumDevice and mediumDeviceHardware policies are restricted to devices and systems.~~

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

~~In addition, there are five certificate policies specified at two different levels of assurance associated with the SHA-1 Federal Root CA. Each level of assurance has an OID to be asserted in certificates issued by the SHA-1 Federal Root CA. Entity Principal CAs may assert these OIDs in policyMappings extensions of certificates issued to the SHA-1 Federal Root CA. The id-fpki-SHA1 policy OIDs are registered in the NIST Computer Security Objects Registry as follows:~~

~~*Table – Certificate Policy OIDs Identifying the Use of SHA-1*~~

~~id-fpki-SHA1-medium-CBP~~PIV-I Authentication certificate	~~::= { fbca-policies 21 }~~id-fpki-certpcy-pivi-hardware
~~id-fpki-SHA1-mediumHW-CBP~~Digital Signature certificate with the private key generated on a PIV-I credential	~~::= { fbca-policies 22 }~~id-fpki-certpcy-mediumHardware
~~id-fpki-SHA1-medium~~Key Management certificate associated with a PIV-I credential	~~::= { fbca-policies 23 }~~id-fpki-certpcy-mediumAssurance id-fpki-certpcy-mediumHardware
~~id-fpki-SHA1-~~All other hardware-based certificates	~~::= { fbca-policies 24 }~~id-fpki-certpcy-mediumHW-CBP id-fpki-certpcy-mediumHardware id-fpki-certpcy-highAssurance*
~~id-fpki-SHA1-devices~~All software-based certificates	~~::= { fbca-policies 25 }~~id-fpki-certpcy-rudimentaryAssurance id-fpki-certpcy-basicAssurance

	id-fpki-certpcy-medium-CBP id-fpki-certpcy-mediumAssurance

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

The requirements associated with id-fpki-certpcy-pivi-hardware are identical to id-fpki-certpcy-mediumHardware except where specifically noted in the text and further described in Appendix A.

The requirements associated with the id-fpki-certpcy-medium-CBP (commercial best practice) policy are identical to those defined for the ~~Medium Assurance~~id-fpki-certpcy-mediumAssurance policy ~~with the exception of~~except for personnel security requirements (see Section 5.3.1).

The requirements associated with the ~~Medium Hardware~~id-fpki-certpcy-mediumHardware policy are identical to those defined for the ~~Medium Assurance~~id-fpki-certpcy-mediumAssurance policy ~~with the exception of~~except for subscriber cryptographic module requirements (see Section 6.2.1).

The requirements associated with the id-fpki-certpcy-mediumHW-CBP policy are identical to those defined for the ~~Medium Hardware Assurance~~id-fpki-certpcy-mediumHardware policy ~~with the exception of~~except for personnel security requirements (see Section 5.3.1).

Personal Identity Verification Interoperable (PIV-I) Device Subscriber Certificates

Certificates valid for the following policies are issued to Device Subscribers and are limited to use with PIV-I credentials by this policy.

Card Authentication certificate with the private key on a PIV-I credential	id-fpki-certpcy-pivi-cardAuth
Content Signing certificate used to sign PIV-I data objects	id-fpki-certpcy-pivi-contentSigning

The requirements associated ~~with PIV-I Hardware and PIV-I Content Signing~~id-fpki-certpcy-pivi-contentSigning are identical to ~~Medium Hardware~~id-fpki-certpcy-mediumHardware except where specifically noted in the text and further described in Appendix A.

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

Additional Device Subscriber Certificates

FIPS 140 Level 2 or higher hardware cryptographic modules	id-fpki-certpcy-mediumDeviceHardware
FIPS 140 Level 1 or higher cryptographic modules	id-fpki-certpcy-mediumDevice

The requirements associated with ~~id-fpki-SHA1-medium policy~~the id-fpki-certpcy-mediumDevice and id-fpki-certpcy-mediumDeviceHardware policies are identical to those defined for the ~~FBCA medium policy~~id-fpki-certpcy-mediumAssurance and id-fpki-certpcy-mediumHardware policies, respectively, except ~~that the certificates asserting id-fpki-SHA1-medium are signed with SHA-1, and the issuing CAs can use SHA-1~~ for ~~generation of PKI objects such as CRLs and OCSP responses.~~

~~The requirements associated with id-fpki-SHA1-hardware policy are identical to those defined for the FBCA medium-hardware policy, except that the certificates asserting id-fpki-SHA1-hardware are signed with SHA-1~~identity proofing, re-key, and ~~the issuing CAs can use SHA-1 for generation of PKI objects such as CRLs and OCSP responses.~~activation data.

~~The requirements associated with id-fpki-SHA1-medium-CBP (commercial best practice) policy are identical to those defined for the FBCA medium-CBP policy, except that the certificates asserting id-fpki-SHA1-medium-CBP are signed with SHA-1, and the issuing CAs can use SHA-1 for generation of PKI objects such as CRLs and OCSP responses.~~

~~The requirements associated with id-fpki-SHA1-mediumHW-CBP (commercial best practice) policy are identical to those defined for the FBCA mediumHW-CBP policy, except that the certificates asserting id-fpki-SHA1-mediumHW-CBP are signed with SHA-1, and the issuing CAs can use SHA-1 for generation of PKI objects such as CRLs and OCSP responses.~~

~~The requirements associated with id-fpki-SHA1-device policy are identical to those defined for the FBCA device policy, except that the certificates asserting id-fpki-SHA1-device are signed with SHA-1, and the issuing CAs can use SHA-1 for generation of PKI objects such as CRLs and OCSP responses.~~

~~1.3 PKI ENTITIES~~

1.3 PKI PARTICIPANTS

The following are roles relevant to the administration and operation of the FBCA and the relationships with cross-certified Entities.

1.3.1 PKI Authorities

1.3.1.1 Federal Chief Information Officers Council

The Federal Chief Information Officer (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 (FPKI) and oversees the operation of the organizations responsible for governing and promoting its use. In particular, this CP was established under the authority ~~of~~ and ~~with the~~ approval of the Federal CIO Council.

1.3.1.2 Federal PKI Policy Authority (FPKIPA)

The Federal Public Key Infrastructure Policy Authority (FPKIPA) is a ~~group~~sub-council comprised of U.S. Federal Government ~~Agencies (including cabinet-level Departments)~~ agency representatives and is chartered ~~by~~under the Federal Chief Information Security Officer (CISO) Council, under the Federal CIO Council. The FPKIPA owns this certificate policy and represents the interest of the Federal CIOs~~.~~ and Federal CISOs.

The FPKIPA is responsible for:

- ~~The FBCA~~Maintaining this CP,
- ~~The FBCA CPS,~~
- ~~Accepting~~Approving applications from Entities ~~desiring~~requesting cross-certification with the FBCA,
- Ensuring the legitimacy of the applicant organization and the authority of designated individuals to ~~interoperate using~~act on behalf of the ~~FBCA~~Entity,
- Determining the mappings between certificates issued by applicant Entity CAs and the ~~levels of assurance set forth~~policies defined in the FBCA CP (which will include objective and subjective evaluation of the respective CP contents and any other facts deemed relevant by the FPKIPA), and
- After an Entity is ~~authorized to interoperate using~~ cross-certified with the FBCA, ensuring continued conformance ~~of that Entity with applicable requirements as a condition for allowing continued interoperability using the FBCA~~.

The FPKIPA will execute a Memorandum of Agreement (MOA) with each cross-certified Entity setting forth the respective responsibilities and obligations of both parties and the mappings between the applicable certificate ~~levels of assurance~~policies contained in this 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.)~~

1.3.1.3 FPKI Management Authority (FPKIMA)

The FPKIMA is the ~~organization~~government program that operates and maintains the ~~FBCA and the SHA1~~ Federal ~~Root CA~~PKI operational environment on behalf of the U.S. Government~~, subject to the direction of the FPKIPA. All of the requirements for the SHA1 Federal Root CA are identical to the FBCA except that the SHA1 Federal Root CA and entity CAs cross certified~~

~~with the SHA1 Federal Root CA use SHA-1 for generation of PKI objects such as certificates, Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) responses~~.

1.3.1.4 FPKI Management Authority Program Manager

The Program Manager is the individual within the FPKIMA who has principal responsibility for overseeing the ~~proper~~ operation of the ~~FBCA~~Federal Bridge CA, including the ~~FBCA~~required repository, and selecting the FPKIMA staff. ~~The Program Manager is selected by the FPKIMA and reports to the FPKIPA. The FPKIMA Program Manager must hold a Top Secret~~For additional personnel security ~~clearance.~~controls associated with this role see Section 5.3.1.

~~1.3.1.5 Entity Principal Certification Authority (CA)~~

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

~~It should be noted that an Entity may request that the FBCA cross-certify with more than one CA within the Entity; that is, an Entity may have more than one Principal CA. Additionally, this CP may refer to CAs that are "subordinate" to the Principal CA. The use of the term "subordinate CA" shall encompass any CA under the control of the Entity that has a certificate issued to it by the Entity Principal CA or any CA subordinate to the Principal CA, whether or not the Entity employs a hierarchical or other PKI architecture.~~

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

~~1.3.1.6~~1.3.1.5 Entity PKI Policy Management Authority

Entity PKIs ~~(including other Bridges)~~ that are cross-certified with the Federal Bridge ~~shall~~CA must identify an individual or group that is responsible for maintaining the entity PKI CP and for ensuring that all Entity PKI components ~~(e.g., CAs, CSSs, CMSs, RAs)~~ are operated in compliance with the entity PKI CP. ~~This body is referred to as Entity~~Cross-certified Bridges must ensure member PKIs are operated comparably with the Bridge PKI ~~Policy Management Authority (PMA) within this~~ CP.

The Entity PKI PMA ~~shall be~~is responsible for notifying the FPKIPA of any change to the infrastructure that has the potential to affect the FPKI operational environment at least two weeks prior to implementation; all new artifacts (CA certificates, ~~CRL DP,~~ Certificate Revocation List Distribution Point (CRLDP), Authority Information Access (AIA) and/or Subject Information Access (SIA) URLs, etc.) produced as a result of the change ~~shall~~must be provided to the FPKIPA within 24 hours following implementation.

1.3.2 Certification Authorities

The CA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to Subscribers. The CA is responsible for issuing and managing certificates including:

- The certificate manufacturing process
- Publication of certificates
- Revocation of certificates
- Generation and destruction of CA signing keys
- Ensuring that all aspects of the CA services, operations, and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

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

1.3.2.1 Entity Cross-Certified Certification Authority (CA)

The Entity designates at least one CA within its PKI to receive a cross-certificate from the FBCA. This document refers to this CA as the Entity cross-certified CA. In addition, this CP may refer to CAs that are "subordinate" to the Entity cross-certified CA. The use of the term "subordinate CA" shall encompass any CA under the control of the Entity that is subordinate to the cross-certified CA.

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

~~*1.3.1.7*~~*1.3.2.2 Federal Bridge Certification Authority (FBCA)*

The FBCA is ~~the entity~~ operated by the FPKIMA ~~that~~and is authorized by the FPKIPA to create, sign, and issue public key certificates ~~to Principal CAs.~~. As operated by the FPKIMA, the FBCA is responsible for all aspects of the issuance and management of a certificate including:

- ~~Control over the registration process,~~
- ~~The identification and authentication process,~~
- The certificate manufacturing process,
- Publication of certificates,
- Revocation of certificates,
- Re-key of FBCA signing material, and
- Ensuring that all aspects of the FBCA services and FBCA operations and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.3 Card Management System (CMS)

The Card Management System is responsible for managing smart card token content. In the context of this policy, the CMS requirements are associated with the PIV-I policies only. Entity CAs issuing PIV-I certificates are responsible for ensuring that all CMSs meet the requirements described in this document, including all requirements specified in Appendix B. In addition, the CMS must not be issued any certificates that express the id-fpki-certpcy-pivi-hardware or id-fpki-certpcy-pivi-cardAuth policy OID.

1.3.4 Registration Authority (RA)

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

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

The FPKIPA acts as the Trusted Agent for the FBCA. Entity CAs designate their own RAs.

A Trusted Agent is authorized by a CA to act on its behalf and may record information from and verify biometrics (e.g., photographs) on presented credentials on behalf of an RA for Applicants who cannot appear in person. Trusted Agents are not Trusted Roles.

~~1.3.2~~1.3.5 Certificate Status Servers

PKIs may optionally include an authority that provides status information about certificates on behalf of a CA through online transactions. ~~In particular,~~ PKIs may include Online Certificate Status Protocol (OCSP) responders to provide online status information. Such an authority is termed a Certificate Status Server (CSS). Where the CSS is identified in certificates as an authoritative source for revocation information, the operations of that authority are considered within the scope of this CP. Examples include OCSP servers that are identified in the ~~authority information access (~~AIA~~)~~ extension. OCSP servers that are locally trusted, as described in RFC ~~2560~~6960, are not covered by this policy. Entity CAs that issue PIV-I certificates must provide an OCSP responder.

~~1.3.3~~1.1.1 ~~Registration Authority (RA)~~

~~The RA collects and verifies each Subscriber's identity and information for inclusion in the Subscriber's public key certificate. The FPKIMA acts as the RA for the FBCA, and performs its function in accordance with a CPS approved by the FPKIPA. Entity CAs designate their own RAs. The requirements for RAs in the FBCA and Entity PKIs are set forth elsewhere in this document.~~

~~1.3.4~~1.1.1 ~~Card Management System (CMS)~~

~~The Card Management System is responsible for managing smart card token content. In the context of this policy, the CMS requirements are associated with the PIV-I policies only. Entity~~

~~CAs issuing PIV-I certificates are responsible for ensuring that all CMSs meet the requirements described in this document, including all requirements specified in Appendix B. In addition, the CMS shall not be issued any certificates that express the PIV-I Hardware or PIV-I Card Authentication policy OID.~~

~~1.3.5 Subscribers~~

1.3.6 ~~A Subscriber is the user or device to whom or to which a certificate is issued. FBCA Subscribers include only FPKIMA personnel and~~Key Recovery Authorities

For organizations that have implemented Key Recovery, the applicable requirements for physical, personnel, and procedural security controls, technical security controls, and Compliance Audit apply as follows:

- CA requirements apply to the KED and to the DDS
- RA requirements apply to the KRA and KRA automated systems
- RA requirements apply to the KRO and KRO automated systems, when ~~determined by the FPKIPA, network or hardware devices. Where certificates are issued to devices, the entity must have a human sponsor~~the KRO has privileged access to the KED

1.3.6.1 Key Escrow Database

The KED is defined as the function, system, or subsystem that maintains the key escrow repository and responds to key registration requests. The KED also responds to key recovery requests from two or more KRAs or self-recovery by a current subscriber.

Section 5.2.1.2 contains the description of Trusted Roles required to operate the KED.

1.3.6.2 Data Decryption Server

A DDS is an automated system that has the capability to obtain subscriber private keys from the KED or another DDS for data monitoring or other purposes (e.g., email inspection). DDSs do not provide keys to Subscribers or other Third-Party Requestors. A DDS has access to escrowed key management keys and must meet all security requirements of the KED as outlined in this policy.

Implementation of a DDS is optional based on organizational operations.

1.3.6.3 Key Recovery Agent

A KRA is an individual who is ~~responsible for carrying out Subscriber duties. Note that CAs are sometimes technically~~ authorized, as specified in the applicable Practice Statement (KRPS or CPS), to recover an escrowed key. The KRAs send the recovered key to the KRO or directly to the Requestor. The KRAs have high level, sensitive access to the KED and are considered "Trusted Roles (see Section 5.2.1). KRAs can recover large numbers of keys, the number and location of KRAs should be closely controlled.

KRAs may additionally conduct requestor identity verification and authorization validation when KROs are not used.

1.3.6.4 Key Recovery Official

A Key Recovery Official (KRO) may optionally be used to support identity verification and authorization validation tasks.

1.3.7 Key Recovery Requestors

A Requestor is the person or DDS that requests the recovery of a decryption private key. A Requestor may be the Subscriber or a third-party (e.g., supervisor, corporate officer, or law enforcement officer) authorized to request recovery of a Subscriber's escrowed key on behalf of the Subscriber or on behalf of the organization. Any individual who can demonstrate a verifiable authority and a need to obtain a recovered key may be considered a Requestor.

1.3.7.1 Internal Third-Party Requestor

An Internal Third-Party Requestor is any Requestor who is in the Subscriber's supervisory chain or otherwise authorized to obtain the Subscriber's key for the Issuing Organization (i.e., the organization on behalf of which the CA issues certificates to subscribers~~" in a PKI. However,)~~.

1.3.7.2 External Third-Party Requestor

An External Third-Party Requestor is someone (e.g., investigator) outside the Issuing Organization with a court order or other legal instrument to obtain the decryption private key of the Subscriber.

1.3.8 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate. The term "Subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information. A Subscriber may be referred to as an "Applicant" after applying for a certificate, but before the certificate issuance procedure is completed.

There is a subset of Human Subscribers who will be issued role-based certificates. These certificates identify a specific role on behalf of which the Subscriber is authorized to act rather than the Subscriber's name. These certificates are issued in the interest of supporting accepted business practices. The role-based certificate can be used in situations where non-repudiation is desired. Normally, it will be issued in addition to an individual Subscriber certificate. ~~does not refer to CAs~~ A specific role may be identified in certificates issued to multiple Subscribers; however, the key pair will be unique to each individual role-based certificate. For example, there may be four individuals with a certificate issued in the role of "Watch Commander". However, each of the four certificates will have unique keys and certificate serial numbers.

~~1.3.6~~1.3.9 Affiliated Organizations

Subscriber certificates may be issued ~~in conjunction with~~on behalf of an organization, other than the organization operating the Entity PKI, that has a relationship with the subscriber; this is termed affiliation. The organizational affiliation will be indicated in the certificate. Affiliated

Organizations are responsible for verifying the affiliation at the time of certificate application and requesting revocation of the certificate if the affiliation is no longer valid.

~~1.3.7~~1.3.10 Relying Parties

A relying party ~~uses a~~ is the entity that relies on the validity of the binding of the Subscriber's ~~certificate~~identity to ~~verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the Subscriber.~~a public key. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The relying party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate's private key. A relying party may use information in the certificate (such as certificate policy identifiers, key usage, or extended key usage) to determine ~~the suitability of the certificate for a particular use.~~its appropriate usage.

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

For this certificate policy, the relying party may be any entity that wishes to validate the binding of a public key to the name of a Subscriber.

~~1.3.8~~1.3.11 Other Participants

~~The FBCA and Entity~~ CAs may require the services of other security, community, and application authorities~~. If required, the FBCA or Entity CPS shall identify the parties, define the services, and designate the mechanisms used to support these services.~~, such as compliance auditors.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

Subscriber certificates issued by Entity CAs may be used for authentication, key management, signature, and confidentiality requirements. The sensitivity of the information processed or protected using certificates issued by FBCA or an Entity CA will vary significantly. ~~Relying Parties must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Relying Party for its application and is not controlled by this CP.~~ To provide sufficient granularity, this CP specifies security requirements at six ~~increasing, qualitative~~different levels of assurance: Rudimentary, Basic, Medium, PIV-I Card Authentication, Medium Hardware, and High. ~~It is assumed that the FBCA will issue at least one High assurance certificate, so the FBCA will be operated at that level.~~

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

~~to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to Federal statues and regulations.~~
~~The~~ following table provides ~~a brief description of the~~additional guidance for determining which policy may be most appropriate ~~uses for~~based on the sensitivity of the information processed or protected using these certificates ~~at each level of assurance defined in this CP~~. These descriptions are intended as guidance and are not binding.

Assurance Level	Appropriate Certificate Uses
Rudimentary	This level provides the lowest degree of assurance concerning identity of the individual. One of the primary functions of this level is to provide data integrity to the information being signed. This level is relevant to environments in which the risk of malicious activity is considered to be low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used for the latter where certificates having higher levels of assurance are unavailable.
Basic	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.
Medium	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. This level of assurance includes the following certificate policies: Medium, Medium CBP, and Medium Device. ~~The use of SHA-1 to create digital signatures is deprecated beginning January 1, 2011. As such, use of certificates associated with the id-fpki-SHA1-medium, id-fpki-SHA1-medium-CBP, and id-fpki-SHA1-devices policy OIDs should be limited to applications for which the risks associated with the use of a deprecated cryptographic algorithm have been deemed acceptable.~~
PIV-I Card Authentication	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include contactless smart card readers where use of an activation PIN is not practical.

Assurance Level	Appropriate Certificate Uses
Medium Hardware	This level is relevant to environments where 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. This level of assurance includes the following certificate policies: Medium Hardware, Medium Hardware CBP, Medium Device Hardware, PIV-I Hardware, and PIV-I Content Signing. ~~The use of SHA-1 to create digital signatures is deprecated beginning January 1, 2011. As such, use of certificates associated with the id-fpki-SHA1-hardware and id-fpki-SHA1-mediumHW-CBP policy OIDs should be limited to applications for which the risks associated with the use of a deprecated cryptographic algorithm have been deemed acceptable.~~
High	This level is reserved for cross-certification with government entities and is appropriate for those environments 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.

Federal relying parties should review more detailed guidance governing the use of electronic signatures (which include the use of digital certificates) issued by the Office of Management and Budget ~~implementing the Government Paperwork Elimination Act (Federal Register May 2000: Volume 65, Number 85, Page 25508),~~, as well as more detailed subordinate guidance issued by other agencies pursuant to OMB direction (such as NIST Federal Information Processing Standards~~, NIST~~ and Special Publications ~~and electronic record retention guidance provided by the National Archives and Records Administration).~~).

1.4.2 Prohibited Certificate Uses

~~No stipulation.~~

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

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

The FPKIPA is responsible for all aspects of this CP.

1.5.2 Contact Person

Contact information for the support and co-chairs for the FPKIPA is fpki@gsa.gov~~Questions regarding this CP shall be directed to the Chair of the Federal PKI Policy~~

~~Authority, whose address can be found at http://www.idmanagement.gov/fpkipa.~~

~~.~~

1.5.3 Person Determining ~~Certification Practices Statement~~CPS Suitability for the Policy

The Certification Practices Statement must conform to the corresponding Certificate Policy. The FPKIPA is responsible for asserting whether the FBCA CPS conforms to ~~the FBCA~~this CP. 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~~must 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 ~~shall submit~~submits the FBCA CPS and the results of a compliance audit to the FPKIPA for approval. ~~The FPKIPA shall vote to accept or reject the CPS. If rejected, the FPKIMA shall resolve the identified discrepancies and resubmit to the FPKIPA.~~ The FBCA ~~is required to~~must meet all facets of the policy. The FPKIPA ~~will~~does not issue waivers.

Entity CAs ~~shall~~must submit their CPS and the results of their compliance audit to the appropriate authority (See Section 1.5.3) for approval. An Entity CA's CPS ~~shall be~~is required to meet all facets of its policy. Waivers, while discouraged, may be permitted in order to meet urgent unforeseen operational requirements. Any waivers issued by Entity CAs are considered changes to the corresponding CP~~,~~ and may result in revocation of the cross-certificate by the FPKIPA.

1.6 DEFINITIONS AND ACRONYMS

See ~~Sections 11~~Appendix D and ~~12~~Appendix E.

2. PUBLICATION &AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The FPKIMA shall operate repositories to support FBCA operations.

Entity PKIs are responsible for operation of repositories to support their PKI operations.

Entities who cross-certify with the FBCA shall ensure interoperability with the FBCA repository.

2.1.1 FBCA Repository Obligations

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

- X.500 Directory Server System that is optionallypublicly accessible through the Lightweight Directory Access Protocol,

> Practice Note: The X.500 Directory Server System supporting LDAP will remain available until such time as the FPKIMA has determined that the Federal PKI community no longer requires Directory System Protocol (DSP).

- Availability of the information as required by the certificate information posting and retrieval stipulations of this CP,repository system must be designed and

Access control implemented to provide 99% availability overall and communication mechanisms when needed to protect repository information as described in later sections.limit scheduled down-time to 0.5% annually.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 Publication of Certificates and Certificate Status

CA and End Entity certificates shall onlymust contain valid Uniform Resource Identifiers (URIs) that are publicly accessible by relying parties, for the purposes of certification path building and for revocation checking.

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

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

- a certs-only Cryptographic Message Syntax file that has an extension of .p7c, or to the FBCA and all CRLs

- a single DER encoded certificate that has an extension of .cer

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

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

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

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

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

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

2.2.2 Publication of CA Information

This CP, the FBCA CPS and the annual PKI Compliance Audit Letter for the FBCA are publicly available on https://www.idmanagement.gov/governance/fpkiaudit/.

Entity CPs must be available in public repositories ~~shall contain all CA certificates issued by~~ .

Time or ~~to the Entity PKI and CRLs issued by the Entity PKI.~~

~~For the FBCA, mechanisms and procedures shall be designed to ensure CA certificates and CRLs are available for retrieval 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually.~~

~~Entity CAs being considered for cross certification shall be designed to comply with this requirement.~~

~~Practice Note: Where repository systems are distributed, the availability figures apply to the system as a whole, rather than each component. Availability targets exclude network outages.~~

~~2.2.21.1.1 Publication of CA Information~~

~~The FPKIMA shall publish information concerning the FBCA necessary to support its use and operation. The FBCA CP shall be publicly available on the FPKIPA website (see http://www.idmanagement.gov/fpkipa). The FBCA CPS will not be published; a redacted version of the CPS will be publicly available from the FPKIPA website (see http://www.idmanagement.gov/fpkipa).~~

~~Publication of CA information in the Entity repositories is a local decision.~~

~~2.2.3 Interoperability~~

~~Where certificates and CRLs are published in directories, standards-based schemas for directory objects and attributes are recommended. Detailed information is available in technical guidance from the FPKIMA; for more information, see the FPKIMA website (see http://www.idmanagement.gov/fpkima).~~

2.3 FREQUENCY OF PUBLICATION

This CP and any subsequent changes ~~shall be~~are made publicly available within thirty (30) days of approval.

Publication requirements for CRLs are provided in Sections 4.9.7 and 4.9.12.

2.4 ACCESS CONTROLS ON REPOSITORIES

~~The FPKIMA and Entity CAs shall protect any repository~~Repositories hosting CA certificates, CRLs, and pre-generated OCSP responses (if implemented) must be publicly accessible. Information not intended for public dissemination or modification~~. Certificates and certificate status information in the FBCA repository shall be publicly available through the Internet~~ must be protected.

~~Direct and/or remote access to information in Entity CA repositories shall be determined by the Entity pursuant to the rules and statutes that apply to that entity. Certificates and certificate status information in the Entity repository should be publicly available through the Internet wherever reasonable. At a minimum, the Entity repositories shall make CA certificates and CRLs issued by the Entity PKI and CA certificates issued to the Entity PKI available to Federal Relying Parties.~~

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

3. IDENTIFICATION ~~&~~AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

~~The FBCA shall only generate~~ This CP establishes requirements for both subject distinguished names and ~~sign~~subject alternative names.

CA certificates ~~that~~must contain a non-null subject Distinguished Name (DN). ~~Certificates issued by the FBCA may also include alternative name forms.~~

~~For Entity CAs, the following rules apply.~~ All ~~CA and~~ RA certificates ~~shall~~must include a non-NULL subject DN. ~~All certificates issued to end entities, except those issued at the Rudimentary level of assurance, shall include a non-NULL subject DN. Certificates issued at the Rudimentary level of assurance may include a null subject DN if they include at least one alternative name form. Certificates at all levels of assurance may include alternative name forms.~~ This CP does not restrict the types of names that can be used.

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

Assurance Level	Naming Requirements
Rudimentary	Non-Null Subject Name, or Null Subject Name if Subject Alternative Name is populated and marked critical
Basic	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical
Medium (all policies)	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical
PIV-I Card Authentication	Non-Null Subject Name, and Subject Alternative Name
High	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical

~~PIV-I Hardware certificates shall indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:~~

~~For certificates with an Affiliated Organization:~~

~~cn=*Subscriber's full name*, ou=*Affiliated Organization Name*,{*Base DN*}~~

~~For certificates with no Affiliated Organization:~~

~~cn=*Subscriber's full name*, ou=Unaffiliated, ou=*Entity CA's Name*,{*Base DN*}~~

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

3.1.1.1 Subject Names

Certificates issued to Subscribers must include distinguished names that are comprised of a base distinguished name (Base DN) and additional relative distinguished names (RDNs). The Entity CP must define the permitted Base DN(s).

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

Role-based and group certificates may be issued under any non-PIV-I human subscriber policy.

- Role-based certificates identify a specific role on behalf of which one or more subscribers are authorized to act rather than the subscriber's name. Where the organization is implicit in the role, it may be omitted. Where the role alone is ambiguous, the organization must be present in the DN.
- The subjectName DN in a group certificate must not imply that the subject is a single individual, e.g., by inclusion of a human name form

For PIV-I Card Authentication subscriber certificates, use of the ~~subscriber~~subscriber's common name is prohibited~~.~~, instead a serialNumber=UUID is required.

~~PIV-I Card Authentication certificates shall~~The UUID must be encoded within the serialNumber attribute using the UUID string representation defined in Section 3 of RFC 4122.

PIV-I Hardware certificates may be issued to individuals external to the entity operating the CA. Such individuals may or may not be affiliated with an organization. In these cases, the PIV-I Hardware certificates must indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For PIV-I Hardware certificates with an Affiliated Organization:

~~serialNumber~~cn=Subscriber's full name, ou=Affiliated Organization Name, {Base DN}

For PIV-I cardAuth certificates with an Affiliated Organization:

serial number=UUID, ou=Affiliated Organization Name~~,{~~, {Base DN}

For PIV-I Hardware certificates with no Affiliated Organization:

~~serialNumber~~cn=Subscriber's full name, ou=Unaffiliated, ou=Entity CA's Name, {Base DN}

For PIV-I cardAuth certificates with no Affiliated Organization:

serial number=UUID, ou=Unaffiliated, ou=Entity CA's Name~~,~~ {, {Base DN}

~~The~~This requirement does not apply to CAs that issue PIV-I certificates only to a single organization, designated in the CA issuer name.

PIV-I Content Signing certificates must clearly indicate the organization administering the CMS.

3.1.1.2 Subject Alternative Names

PIV-I Hardware and PIV-I Card Authentication certificates must include a subject alternate name extension, containing a UUID ~~shall be~~value encoded ~~within the serialNumber attribute using the UUID string representation defined~~as a URI as specified in Section 3 of [RFC 4122 ~~(e.g., "f81d4fae-7dec-11d0-a765-00a0c91e6bf6").~~].

PIV-I Card Authentication certificates must not include any other name in the subject alternative name extension.

Subscriber certificates that contain id-kp-emailProtection in the EKU must include a subject alternative name extension that includes a rfc822Name.

For Device Subscriber certificates that assert serverAuth in the Extended Key Usage:

- Wildcard domain names are permitted in the dNSName values only if all sub-domains covered by the wildcard fall within the same application, cloud service, or system boundary within the scope of the sponsoring organization.
- Wildcards must not be used in subdomains that host more than one distinct application platform.

3.1.2 Need for Names to Be Meaningful

Names used in the certificates issued by ~~the FBCA and/or Entity~~ CAs must identify the person or object to which they are assigned in a meaningful way.

The common name in the distinguished name must represent the Subscriber in a way that is easily understandable for humans. For Human Subscribers, this will typically be a legal name.

When DNs are used, the directory information tree must accurately reflect organizational structures.

When DNs are used, the common name must respect name space uniqueness requirements and must not be misleading. This does not preclude the use of pseudonymous certificates as defined in Section 3.1.3. The subject name in CA certificates must match the issuer name in certificates issued by the CA, as required by [RFC 5280].

~~When User Principal Names (UPN) are used, they must be unique and accurately reflect organizational structures.~~

3.1.3 Anonymity or Pseudonymity of Subscribers

CA certificates must not contain anonymous or pseudonymous identities.

The FBCA ~~shall~~does not issue anonymous certificates. Pseudonymous certificates may be issued by the FBCA to support internal operations. ~~CA certificates issued by the FBCA shall not contain anonymous or pseudonymous identities.~~

DNs in subscriber certificates issued by Entity CAs may contain a pseudonym (such as a large number) as long as name space uniqueness requirements are met.

CAs may issue role-based or group certificates that identify subjects by their organizational roles. Each identified 'role' or 'group' must meet name space uniqueness requirements.

3.1.4 Rules for Interpreting Various Name Forms

~~No stipulation for the FBCA.~~

Rules for interpreting distinguished name forms are specified in [X.501].

Rules for interpreting e-mail addresses are specified in [RFC 5322].

Rules for interpreting PIV-I certificate UUID names are specified in [RFC 4122].

Entity CAs ~~must~~may specify additional rules for interpreting names in Subscriber certificates in the Entity CP or a referenced certificate profile. (The rules may be simply a description of naming conventions.)

~~Rules for interpreting PIV-I certificate UUID names are specified in RFC 4122.~~

3.1.5 Uniqueness of Names

Name uniqueness must be enforced by the ~~FBCA~~CA.

Each CA and ~~Entity CAs~~its associated RAs must enforce name uniqueness within the X.500 namespace. When other name forms are used, they too must be allocated such that name uniqueness is ensured for certificates issued by that CA.

> Practice Note: For distinguished names, name uniqueness is enforced for the entire name rather than a particular attribute (e.g., the common name).

The FPKIPA is responsible for ensuring name uniqueness in certificates issued by the FBCA. Entity CAs ~~shall~~must identify the authority that is responsible for ensuring name uniqueness in certificates issued by the entity CA. Name uniqueness is not violated when multiple certificates are issued to the same entity.

3.1.6 Recognition, Authentication, ~~&~~and Role of Trademarks

The FPKIPA ~~shall resolve~~resolves any name collisions or disputes regarding FBCA-issued certificates brought to its attention. Consistent with Federal Policy, the FBCA will not knowingly use trademarks in names unless the subject has the rights to use that name.

Entity CPs must identify the use and role of trademarks within their PKI environments.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

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

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

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

In the case where ~~a~~ key generation is ~~generated by~~performed under the CA or ~~RA either (1) directly on the party's hardware or software token; or (2) in a key generator that benignly transfers the key to the party's token, then~~RA's direct control, proof of possession is not required~~.~~ (e.g., key management certificates generated in a system allowing key escrow).

3.2.2 Authentication of Organization Identity

Requests for ~~FBCA, Entity~~ CA~~, or Subscriber~~ certificates ~~in the name of an Affiliated organization shall~~must include the organization name, address, and documentation of the existence of the organization.

~~The FPKIMA or Entity RA shall~~ Before issuing CA certificates, an authority for the issuing CA must verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

Before issuing subscriber certificates on behalf of an affiliated organization, the issuing CA must verify the authority of requesting representatives.

3.2.3 Authentication of Individual Identity

~~PIV-I Hardware~~For each certificate issued, the CA must authenticate the identity of the individual requestor.

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

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

3.2.3.1 Authentication of Human Subscribers

For Subscribers, the FPKIMA or Entity CA, and/or associated RAs ~~shall~~must ensure that the applicant's identity information is verified in accordance with the process established by the applicable CP and CPS. Process information ~~shall depend~~depends upon the certificate level of assurance and ~~shall~~must be addressed in the ~~FBCA or Entity~~applicable CPS. ~~The documentation and authentication requirements shall vary depending upon the level of assurance.~~

~~For Medium and High Assurance, identity shall be established no more than 30 days before initial certificate issuance Entity CAs being considered for cross certification must comply with this requirement.~~

The ~~FPKIMA, Entity~~ CAs and/or RAs ~~shall~~must record the information set forth below for issuance of each certificate:

- The identity of the person performing the identification and either;
    - A signed declaration by that person that he or she verified the identity of the applicant as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law. ~~The signature on the declaration may be either a handwritten or digital signature using a certificate that is of equal or higher level of assurance as the credential being issued;~~
    - An auditable record linking the authentication of the person performing the identification to their verification of each Applicant.

- If in-person or supervised remote[1] identity proofing is done, a unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- If electronic authentication is done, a unique identifying number(s) from the signature or authentication certificate must be retained (e.g., certificate, serial number, thumbprint, SKI, public key, etc.)
- The date of the verification; and either:
    - An auditable record indicating the applicant accepted the certificate; or
    - A declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature (see Practice Note) and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

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

y sign
he
latter case, if the applicant fails to sign the declaration of identity, then the certificate must be revoked.

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

Assurance Level	Identification Requirements
Rudimentary	No identification requirement; applicant may apply and receive a certificate by providing his or her e-mail address

[1] The minimum requirements associated with supervised remote identity proofing are described in NIST SP 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing,* Section 5.3.3. In addition, the supervised remote process for PIV-I policies must have the capability of capturing an approved biometric.

Assurance Level	Identification Requirements
Basic	Identity may be established by in-person proofing before a Registration Authority or Trusted Agent; or remotely verifying information provided by applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, date of birth, address and other personal information in records are consistent with the application and sufficient to identify a unique individual. Address confirmation: a) Issue credentials in a manner that confirms the address of record supplied by the applicant; or b) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice.
Medium (all policies)	Identity must be established by in-person or supervised remote proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided must be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are one Federal Government-issued Picture I.D., one REAL ID Act compliant picture ID[2], or two Non-Federal Government I.D.s, one of which must be a photo I.D. Any credentials presented must be unexpired. PIV-I identity must be verified in accordance with the requirements specified for issuing PIV in Section 2.7 of [FIPS 201] For PIV-I, the use of an in-person antecedent is not applicable.

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

Assurance Level	Identification Requirements
High	Identity established by in-person appearance before the Registration Authority or Trusted Agent; information provided must be checked to ensure legitimacy Credentials required are either one Federal Government-issued Picture I.D., one REAL ID Act compliant picture ID., or two Non-Federal Government I.D.s, one of which must be a photo I.D. (e.g., Driver's License)

A CPS must indicate what actors, roles, responsibilities and activities are leveraged when relying on in-person antecedent to support identity proofing (e.g., agreement with a professional organization to use a member identification number and associated provided point of contact information as antecedent, or electronic authentication using a medium or above certificate being traced back to the initial identity proofing event).

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

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

For PIV-I Certificates: PIV-I Hardware certificates must be issued only to human subscribers. The following biometric data shallmust be collected during the identity proofing and registration process, and shallmust be formatted in accordance with [NIST SP 800-76-2] (see Appendix A):

- An electronic facial image used for printing facial image on the card, as well as for performing visual authentication during card usage. A new facial image shall be collected each time a card is issued; and;
- Two electronic fingerprints to be stored on the card for automated authentication during card usage.; and

The table below summarizes the identification requirements for each level of assurance.Assurance Level	Identification Requirements
Rudimentary	No identification requirement; applicant may apply and receive a certificate by providing his or her e-mail address
Basic	Identity may be established by in-person proofing before a Registration Authority or Trusted Agent; or remotely verifying information provided by applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are consistent with the application and sufficient to identify a unique individual. Address confirmation: a) Issue credentials in a manner that confirms the address of record supplied by the applicant; or b) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice.
Medium (all policies)	Identity shall be established by in-person or supervised remote proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are one Federal Government-issued Picture I.D., one REAL ID Act compliant picture ID[3], or two Non-Federal Government I.D.s, one of which shall be a photo I.D. Any credentials presented must be unexpired. Clarification on the trust relationship between the Trusted Agent and the applicant, which is based on an in-person antecedent identity

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

The table below summarizes the identification requirements for each level of assurance.Assurance Level	Identification Requirements
	proofing event, can be found in the *FBCA Supplementary Antecedent, In-Person Definition* document. For PIV-I, credentials required are two identity source documents in original form. The identity source documents must come from the list of acceptable documents included in *Form I-9, OMB No. 1115-0136, Employment Eligibility Verification*. At least one document shall be a valid State or Federal Government-issued picture identification (ID). For PIV-I, the use of an in-person antecedent is not applicable.
High	Identity established by in-person appearance before the Registration Authority or Trusted Agent; information provided shall be checked to ensure legitimacy 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)

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

3.2.3.2 Authentication of Human Subscribers for Role-based Certificates

There is a subset of Human Subscribers who will be issued role-based certificates. These certificates will identify a specific role on behalf of which the subscriber is authorized to act rather than the subscriber's name and are issued in the interest of supporting accepted business practices. The role-based certificate can be used in situations where non-repudiation is desired. Normally, it will be issued in addition to an individual Subscriber certificate. A specific role may be identified in certificates issued to multiple subscribers, however, the key pair will be unique to each individual role-based certificate (i.e. there may be four individuals carrying a certificate issued in the role of "*Chief Information Officer*" however, each of the four individual certificates will carry unique keys and certificate identifiers). Roles for which role-based certificates may be issued are limited to those that uniquely identify a specific individualrole within an organization (e.g., *Chief Information Officer* is a unique individualrole whereas *Program Analyst* is not). Role-based certificates shallmust not be shared, but shallmust be issued to individual subscribers and protected in the same manner as individual certificates.

The FPKIMA and/or Entity CAs shallCAs must record the information identified in Section 3.2.3.1 for a sponsor associated with the role before issuing a role-based certificate. The sponsor

must hold an individual certificate in his/her own name issued by the same ~~CA~~Entity at the same or higher assurance level as the role-based certificate.

The procedures for issuing role-based tokens must comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations).

For pseudonymous certificates that identify subjects by their organizational roles, the CA ~~shall~~must validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

Practice Note: When determining whether a role-based certificate is warranted, consider whether the role carries inherent authority beyond the job title. Role-based certificates may also be used for individuals on temporary assignment, where the temporary assignment carries an authority not shared by the individuals in their usual occupation, for example: "*Shift Lead, Security Operations Center*".

3.2.3.3 Authentication of Human Subscribers for Group Certificates

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

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

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

3.2.3.4 Authentication of Devices

Some computing and communications devices (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases, the device must have a human sponsor. The sponsor is

responsible for the security of the private key and for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name) or unique software application name
- Equipment or software application public keys
- Equipment or software application authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the sponsor when required

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

The registration information ~~shall~~must be verified to an assurance level commensurate with the certificate assurance level being requested. For certificates ~~issued with~~that assert a certificate policy mapped to the ~~medium Device and~~ id-fpki-certpcy-mediumDevice or id-fpki-certpcy-mediumDeviceHardware policies, registration information ~~shall~~must be verified commensurate with the Medium assurance level. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

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

3.2.4 Non-verified Subscriber Information

Except for the rudimentary assurance level, all Subscriber information ~~that is not verified shall not be~~ included in certificates must be verified.

3.2.5 Validation of Authority

For cross-certification, the ~~FPKIMA shall validate~~FPKIPA validates the representative's authorization to act in the name of the organization.

Entity CAs must validate the requestor's authority to act in the name of the organization before issuing organizational certificates.

3.2.6 Criteria for Interoperation

The FPKIPA ~~shall determine~~determines the criteria for cross-certification with the FBCA. See also the Federal Public Key Infrastructure Bridge Application Process Overview document [BRIDGE PROCESS] and the Federal Public Key Infrastructure Annual Review Requirements [AUDIT] document. ~~Under no circumstances shall any certificate~~ Entity CAs must not have more than one intentional trust path to the FBCA~~, irrespective of extension processing~~.

Note: Multiple trust paths created as a result of certificate renewal or CA rekey do not violate the single trust path requirement above.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

~~In the event that a Principal CA re-key is required, a new certificate will be issued to Principal CAs by the FBCA. Before issuance, the Principal CA shall identify itself through use of its current signature key or the initial registration process. If it has been more than three years since a Principal CA was identified as required in Section 3.2, identity shall be re-established through the initial registration process.~~

If an Entity CA cross-certified with the FBCA performs a re-key, it must request a new cross-certificate from the FPKIPA.

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

Assurance Level	Routine Re-key Identity Requirements for Subscriber Signature, Authentication and Encryption Certificates
Rudimentary	Identity may be established through use of current signature key.
Basic	Identity may be established through use of current signature key, except that identity ~~shall~~must be reestablished through initial ~~registration~~identity validation process at least once every 15 years from the time of initial registration.

Assurance Level	Routine Re-key Identity Requirements for Subscriber Signature, Authentication and Encryption Certificates
Medium (all policies) and PIV-I Card Authentication	Identity may be established through use of current signature key, except that identity ~~shall~~must be established through initial ~~registration~~identity validation process at least once every ~~nine~~twelve (12) years from the time of initial registration. For certificates asserting policies mapped to id-fpki-certpcy-mediumDevice ~~and~~ or id-fpki-certpcy-mediumDeviceHardware ~~certificates~~, identity may be established through the use of the device's current signature key or ~~using means commensurate with the strength~~the signature key of the ~~certificate being requested, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration~~device's human sponsor.
~~PIV-I Card Authentication~~	~~Identity may be established through use of the current signature key certificate, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration.~~
High	Identity may be established through use of current signature key, except that identity ~~shall~~must be established through initial ~~registration~~identity validation process at least once every three years from the time of initial registration.

3.3.2 Identification and Authentication for Re-key after Revocation

After a certificate has been revoked other than during a renewal or update action, the subscriber is required to go through the initial registration process described in Section 3.2 to obtain a new certificate~~. (This applies to all certificates issued by both Entity CAs and the FBCA.)~~, unless identity can be verified through the use of biometrics on file through the chain of trust defined in [FIPS 201].

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION ~~REQUEST~~REQUESTS

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

3.5 IDENTIFICATION AND AUTHENTICATION FOR KEY RECOVERY REQUESTS

This section is applicable only for those Entity CAs that support key escrow and recovery of private keys.

3.5.1 KRA Authentication

The KRA must authenticate to the KED or DDS directly or using a public key certificate issued by the associated PKI. The assurance level of the certificate must be the same as or greater than that of the certificate whose corresponding private key is being recovered and must meet the requirements of an RA credential.

3.5.2 KRO Authentication

The KRO must authenticate to the KRA using a public key certificate issued by the associated PKI. The assurance level of the certificate must be the same as or greater than that of the certificate whose corresponding private key is being recovered and must meet the requirements of an RA credential.

3.5.3 Subscriber Authentication

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

For automated self-recovery, the Subscriber must be authenticated to the KED using a valid public key certificate. The assurance level of the Subscriber certificate must be equal to or greater than that of the certificate whose corresponding private key is being recovered.

3.5.4 Third-Party Requestor Authentication

The KRA or KRO must verify the identity and authorization of the Requestor prior to initiating the key recovery request.

Third-Party Requestor identity authentication must be commensurate with the assurance level of the certificate associated with the key being recovered. Identity must be established using one of the following methods:

- Procedures specified in Section 3.2.3 for authentication of an individual identity during initial registration for the specified certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose corresponding private key is being recovered).
- Certificate-based authentication (e.g., digitally signed e-mail or client-authenticated TLS) that can be verified using current, valid (i.e., un-revoked) public key certificates at the requested certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose corresponding private key is being recovered).

3.5.5 Data Decryption Server Authentication

The DDS must authenticate to the KED directly using a public key certificate issued by the associated PKI. The assurance level of the certificate must be the same as or greater than that of the highest assurance level encryption certificates issued by the associated PKI.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

The Certificate application process must provide sufficient information to:

- Establish the Applicant's authorization by the employing or sponsoring agency to obtain a certificate. See Section 3.2.3 for requirements.
- Establish and record the identity of the Applicant. See Section 3.2.3 for requirements.
- Obtain the Applicant's public key and verify the Applicant's possession of the private key. See Section 3.2.3 for requirements.
- Verify the information included in the certificate.

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

This section specifies requirements for initial application for certificate issuance.

Entities seeking to cross-certify with the FBCA ~~shall~~must fulfill the application requirements as specified in the U.S. Government Public Key Infrastructure Cross-Certification Criteria and Methodology. The FPKIPA ~~shall act~~acts on the application and, upon making a determination to issue a certificate ~~and entering into the~~establishes an MOA with the Entity~~, shall authorize~~. The FPKIPA identifies the Entity's authorized representatives, provides the appropriate certificate policy mappings and authorizes the FPKIMA to issue the cross-certificate to the Entity.

The FBCA may issue ~~end-entity~~Subscriber certificates to trusted personnel where necessary for the internal operations of the FBCA. The FBCA ~~will~~does not issue ~~end-entity~~Subscriber certificates for any other reasons.

4.1.1 ~~Submission of~~Who Can Submit a Certificate Application

For the FBCA, the certificate application ~~shall~~must be submitted to the FPKIPA by an authorized representative of the Entity CA.

For Entity CAs, this CP makes no stipulations regarding submission of certificate applications beyond those in Section 4.1 above.

4.1.2 Enrollment Process and Responsibilities

All communications supporting the certificate application and issuance process must be authenticated and protected from modification. Communications may be electronic or out-of-band.

Any electronic communication of shared secrets must be protected.

Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair must be used.

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

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

Entities applying for cross-certification are responsible for providing accurate information on their certificate applications. Upon issuance, each certificate issued by the FBCA ~~shall be~~is manually checked to ensure each field and extension is properly populated with the correct information before the certificate is delivered to the Entity.

For Entity CAs~~, all communications among PKI authorities supporting the~~ Subscribers are responsible for providing accurate information on their certificate ~~application and issuance process shall be authenticated and protected from modification.~~

applications.

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

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

4.2 CERTIFICATE APPLICATION PROCESSING

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

4.2.1 Performing Identification and Authentication Functions

For the FBCA, the identification and authentication of the applicant ~~shall be~~is performed by the ~~FPKIMA~~FPKIPA.

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

4.2.2 Approval or Rejection of Certificate Applications

For the FBCA, the FPKIPA may approve or reject a certificate application. See Section 1.1.5.

For Entity CAs, the Entity CP shall identify the person or organizational body that may accept or reject a certificate application.

This CP makes no other stipulation regarding Approval or Rejection of Certificate Applications in Entity PKIs.

4.2.3 Time to Process Certificate Applications

~~No stipulation.~~

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

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions During Certificate Issuance

The FPKIMA verifies the source of a certificate request before issuance. CA certificates created by the FBCA ~~shall be~~are checked to ensure that all fields and extensions are properly populated. ~~After generation and verification, the FPKIMA shall post CA certificates in the FBCA repository system.~~

Upon receiving the request, Entity CAs ~~shall~~ /RAs must:

- Verify the ~~source~~identity of ~~a~~ the requestor.
- Verify the authority of the requestor and the integrity of the information in the certificate request.
- Verify all attribute information received from a Subscriber before ~~issuance~~inclusion in a certificate.
- Build and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate).
- Make the certificate available to the Subscriber after confirming that the Subscriber has formally acknowledged the obligations described in Section 9.6.3.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate ~~Issuance~~

~~The FBCA process for subscriber notification is defined in the U.S. Government Public Key Infrastructure Cross-Certification Criteria and Methodology. (See http://www.idmanagement.gov/fpkima/tech_requirements.cfm)~~

~~Practice Note: Where notification is not an integral component of the issuance process, CAs should proactively notify subscribers that certificates have been generated.~~

~~For Entity CAs, no stipulation.~~

The FPKIMA notifies the Entity CA of certificate issuance.

Practice Note: Where notification is not an integral component of the issuance process, CAs should proactively notify subscribers that certificates have been generated.

For PIV-I, Entity CAs must inform the Subscriber of the creation of a certificate and make the certificate available to the Subscriber.

4.4 CERTIFICATE ACCEPTANCE

Before a subscriber can make effective use of its private key, ~~a PKI Authority shall convey to~~ the subscriber ~~its~~must accept the responsibilities ~~as~~ defined in Section 9.6.3 by accepting the Subscriber agreement.

4.4.1 Conduct Constituting Certificate Acceptance

For the FBCA, failure to object to the certificate or its contents constitutes acceptance of the certificate.

For certificates issued by an Entity CP, certificate acceptance is governed by the Entity CP.

4.4.2 Publication of the Certificate by the CA

As specified in Section 2.2.1, all CA certificates ~~shall~~must be published in ~~FBCA or Entity~~ a PKI repository accessible over the Internet.

PIV-I authentication and card authentication certificates must not be distributed via public repositories.

This specification makes no other stipulation regarding publication of Subscriber certificates.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

For the FBCA, notification of certificate issuance will be provided to all cross-certified entities.

For Entity CAs, the FPKIPA ~~shall~~must be notified at least two weeks prior to the issuance of a new CA certificate or issuance of new inter-organizational CA cross-certificates. ~~The notification shall assert that the new CA cross-certification does not introduce multiple paths to a CA already participating in the FPKI.~~ In addition, all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the CA certificate issuance ~~shall~~must be provided to the FPKIPA within 24 hours following issuance.

~~Practice Note: The process for notifying the FPKIPA shall be included in the MOA.~~

Practice Note: The process for notifying the FPKIPA is included in the MOA.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

~~For High, Medium Hardware, Medium, and Basic Assurance, subscribers shall~~Subscribers must protect their private keys from access by other parties. ~~For Rudimentary assurance, no stipulation.~~

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

4.5.2 Relying Party Public Key and Certificate Usage

~~FBCA-issued~~ Certificates specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. ~~The FBCA issues~~CAs issue CRLs specifying the current status of all unexpired ~~FBCA~~ certificates. ~~It is recommended that~~ Relying parties should process certificate and ~~comply with this~~status information ~~whenever using FBCA issued~~as specified in [X.509] when relying on certificates ~~in a transaction.~~.

4.6 CERTIFICATE RENEWAL

~~Certificate renewal consists of issuing~~Renewing a certificate means creating a new certificate with a new ~~validity period and~~ serial number ~~while retaining~~where all ~~other~~certificate subject information ~~in the original certificate~~, including the subject public key~~. Frequent renewal of certificates may assist in reducing the size of CRLs.~~ and subject key identifier, remain unchanged.

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

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

4.6.1 Circumstance for Certificate Renewal

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

~~Certificates may also be renewed when a CA re-keys.~~

PIV-I certificates must not be renewed, except during recovery from CA key compromise (see Section 5.7.3). In such cases, the renewed certificate must expire as specified in the original Subscriber certificate.

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

4.6.2 Who May Request Renewal

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

For other CA certificates and Delegated OCSP responder certificates, the corresponding operating authority may request renewal.

For Entity CAs that support renewal, ~~such~~subscriber renewal requests ~~shall only~~must be accepted only from certificate subjects, PKI sponsors or RAs. Additionally, a CA may perform renewal of its subscriber certificates without a corresponding request, such as when the CA re-keys.

4.6.3 Processing Certificate Renewal Requests

For the FBCA, certificate renewal for reasons other than re-key of the FBCA ~~shall~~must be approved by the FPKIPA.

~~For Entity CAs, no stipulation.~~

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

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

4.6.4 Notification of New Certificate Issuance to Subscriber

~~The FPKIMA shall notify Entity CAs upon issuance of new certificates.~~

~~For Entity CAs, no stipulation.~~

As specified in Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

~~Failure to object to a FBCA-issued certificate constitutes acceptance of the certificate.~~

~~For Entity CAs, no stipulation.~~

As specified in Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

As specified in Section 4.4.2.~~2.1, all CA certificates shall be published in the FBCA or Entity repositories.~~

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

~~The FPKIMA shall inform the FPKIPA of any certificate issuance.~~

~~For Entity CAs, no stipulation.~~

As specified in Section 4.4.3.

4.7 CERTIFICATE RE-KEY

~~Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. Re-key of a certificate~~

~~does not require a change to the subjectName and does not violate the requirement for name uniqueness.~~

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

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

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

4.7.1 Circumstance for Certificate Re-key

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

The FBCA will issue new cross-certificates to ~~Principal~~Entity CAs when ~~a currently recognized Principal CA has~~they have generated a new key pair and a valid and unexpired MOA exists between the FPKIPA and the Entity PKI.

~~For Entity CAs, no stipulation.~~

Section 6.3.2 establishes maximum usage periods for private keys for both CAs and Subscribers.

4.7.2 Who May Request Certification of a New Public Key

The FPKIMA may request certification of a new FBCA public key ~~for~~from currently cross-certified Entity ~~Principal~~ CAs.

~~For Entity CAs that support~~ For Entity CA certificates and Delegated OCSP responder certificates, the corresponding operating authority may request re-key~~, such requests shall only be accepted from the subject~~ of its own certificate.

Subscribers with a currently valid certificate may request re-key of the certificate ~~or PKI sponsors. Additionally,~~. CAs and RAs may ~~initiate re-key of a subscriber's certificates without a corresponding request~~request certification of a new public key on behalf of a Subscriber. The human sponsor of a device may request re-key of the device certificate.

4.7.3 Processing Certificate Re-keying Requests

Before performing re-key, the ~~FPKIMA shall~~CA must identify and authenticate ~~Principal CAs~~the requestor by performing the identification processes defined in Section 3.2 or Section 3.3.

~~The validity period associated with the new certificate must not extend beyond the period of the MOA.~~

~~For Entity CAs, see Sections 3.2 and 3.3.~~

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

4.7.4 Notification of New Certificate Issuance to Subscriber

~~The FPKIMA shall notify Entity CAs upon issuance of new certificates.~~

~~For Entity CAs, no stipulation.~~

As specified in Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

~~For the FBCA, failure to object to the certificate or its contents constitutes acceptance of the certificate.~~

~~For Entity CAs, no stipulation.~~

As specified in Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

As specified in Section 4.4.2.~~2.1, all CA certificates shall be published in the FBCA or Entity repositories.~~

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

~~The FPKIMA shall inform the FPKIPA of any certificate issuance.~~

~~For Entity CAs, no stipulation.~~

~~*4.8 MODIFICATION*~~

As specified in Section 4.4.3.

4.8 CERTIFICATE MODIFICATION ~~CONSISTS OF~~

Modifying a certificate means creating a new ~~certificates with subject information (e.g., a name or email address)~~certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. ~~For example, an Entity CA may perform certificate modification for a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The new certificate may have the same or different subject public key.~~

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

4.8.1 Circumstance for Certificate Modification

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

~~For Entity CAs, no stipulation.~~

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

4.8.2 Who May Request Certificate Modification

The FPKIMA or the Entity ~~Principal CA~~ may request certificate modification for ~~currently~~current cross-~~certified Entity Principal CAs~~certificates.

~~For Entity CAs, no stipulation.~~

For Entity CA certificates and Delegated OCSP responder certificates, the corresponding operating authority may request modification.

Subscribers with a currently valid certificate may request modification of the certificate. The human sponsor of a device may request modification of the device certificate. CAs and RAs may request certificate modification on behalf of a Subscriber.

4.8.3 Processing Certificate Modification Requests

The FPKIMA ~~shall perform~~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 SIA extension; or
- Minor name changes (e.g., change CA1 to CA2) as part of key rollover procedures.

~~The validity period associated with the new certificate must not extend beyond the period of the MOA.~~

For Entity CAs, proof of all subject information changes must be provided to the RA or other designated agent and verified before the modified certificate is issued. If the modified certificate is issued with a new (different) public key, the additional requirements specified in Section 4.7.3 must also apply.

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

4.8.4 Notification of New Certificate Issuance to Subscriber

~~The FPKIMA shall notify Entity CAs upon issuance of new certificates.~~

~~For Entity CAs, no stipulation.~~

As specified in Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

~~For the FBCA, failure to object to the certificate or its contents constitutes acceptance of the certificate.~~

~~For Entity CAs, no stipulation.~~

As specified in Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

As specified in Section 4.4.2.~~2.1, all CA certificates shall be published in the FBCA or Entity repositories.~~

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

~~The FPKIMA shall inform the FPKIPA of any certificate issuance.~~

~~For Entity CAs, no stipulation.~~

As specified in Section 4.4.3.

4.9 CERTIFICATE REVOCATION ~~&~~AND SUSPENSION

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

For High, PIV-I, Medium Hardware, Medium, and Basic Assurance, all CAs ~~shall~~must publish CRLs.

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

4.9.1 Circumstances for Revocation

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

- Identifying information or affiliation components of any names in the certificate becomes invalid. Examples include
  - Subscriber no longer affiliated with sponsoring entity
  - A wild card certificate has been issued with a name where PKI Sponsor does not exercise control of the entire namespace associated with the wild card certificate.
- Privilege attributes asserted in the Subscriber's certificate are reduced.
- The Subscriber can be shown to have violated the stipulations of its Subscriber agreement.
- There is reason to believe the private key has been compromised.
- The Subscriber or other authorized party (as defined in the CPS) asks for his/her certificate to be revoked.
- The failure of a CA to adequately adhere to the requirements of its CP or the approved CPS.

There are three circumstances under which certificates issued by the FBCA will be revoked:

- ~~The first circumstance is when~~ The FPKIPA requests an FBCA-issued certificate be revoked. ~~This will be the normal mechanism for revocation in cases where the FPKIPA determines that an Entity PKI does not meet the Federal PKI policy requirements or certification of the Entity PKI is no longer in the best interests of the Federal Government.~~
- ~~The second circumstance is when the Management Authority~~The FPKIMA receives an authenticated request from a previously designated official of the Entity responsible for the ~~Principal~~ CA.
- ~~The third circumstance is when~~ The FBCA Operational personnel determine that an emergency has occurred that may impact the integrity of the certificates issued by the FBCA. Under such circumstances, the following individuals may authorize immediate certificate revocation:
    - ~~Chair,~~ FPKIPA Co-chair, or
    - Other personnel as designated by ~~the Chair,~~a FPKIPA Co-chair.

The FPKIPA ~~shall~~must meet as soon as practicable to review the emergency revocation.

~~Entity~~ CAs ~~that implement certificate revocation shall~~must, at a minimum, revoke certificates for the reason of key compromise upon receipt of an authenticated request from an appropriate entity.

For certificates that express an organizational affiliation, Entity CAs ~~shall~~must require that the organization ~~must~~ inform the Entity CA of any changes in the subscriber affiliation. If the affiliated organization no longer authorizes the affiliation of a Subscriber, the Entity CA ~~shall~~must revoke any certificates issued to that Subscriber containing the organizational affiliation. If an organization terminates its relationship with an Entity CA such that it no longer provides affiliation information, the Entity CA ~~shall~~must revoke all certificates affiliated with that organization.

~~Whenever any of the above circumstances occur~~If it is determined that revocation is required, the associated certificate ~~shall~~must be revoked and placed on the CRL. Revoked certificates ~~shall~~must be included on all new publications of the certificate status information until the certificates expire.

4.9.2 Who Can Request Revocation

A CA may summarily revoke certificates it has issued. A written notice and brief explanation for the revocation must subsequently be provided to the Subscriber.

A Subscriber or sponsor of device certificates may request revocation of their own certificates.

The RA or other authorized agency officials may request the revocation of a Subscriber's certificate.

An FBCA issued certificate may be revoked upon direction of the FPKIPA or upon an authenticated request by a designated official of the Entity responsible for the ~~Principal CA (such official or officials shall be identified in the MOA as authorized to make such a request).~~CA named in the certificate.

Entity CAs ~~that implement certificate revocation shall~~must, at a minimum, accept revocation requests from subscribers. Entity CAs that issue certificates in association with Affiliated Organizations ~~shall~~must accept revocation requests from the Affiliated Organization named in the certificate. Requests for certificate revocation from other parties may be supported by Entity CAs. Note that an Entity ~~Principal CA~~ may always revoke ~~the certificate~~certificates it has issued to the FBCA without any FPKIPA action.

4.9.3 Procedure for Revocation Request

Upon receipt of a revocation request involving an FBCA-issued certificate, the FPKIMA ~~shall authenticate the request and apprise the FPKIPA. The FPKIPA may, at its discretion, take whatever measures it deems appropriate to verify the need for revocation. If the revocation request appears to be valid, the FPKIPA shall direct the FPKIMA to revoke the certificate. The FPKIMA shall give prompt oral or electronic notification to the FPKIPA co-chairs and previously designated officials in all entities having a Principal CA with which the FBCA interoperates.~~must authenticate the request and apprise the FPKIPA.

If a revocation is due to a certificate or systems compromise or an Entity ~~Principal~~ CA violation of the Memorandum of Agreement with the FPKIPA, the ~~FPKIMA~~FPKIPA will notify previously designated officials ~~in~~of all cross-certified entities ~~having a Principal CA with which the FBCA interoperates~~.

Entity CAs ~~that implement certificate revocation shall~~must revoke certificates upon receipt of sufficient evidence of compromise or loss of the subscriber's corresponding private key. ~~A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed).~~ Where subscribers use hardware tokens, but excluding PIV-I certificates, revocation is optional if all the following conditions are met:

- the revocation request was not for key compromise;
- the ~~hardware token~~cryptographic module does not permit the user to export the signature private key;
- the Subscriber surrendered the token to the PKI;
- the token was zeroized or destroyed promptly upon surrender;
- the token has been protected from malicious use between surrender and zeroization or destruction.

For PIV-I and in all other cases not identified above, revocation of the certificates is mandatory. Even where all the above conditions have been met, revocation of the associated certificates is recommended.

Entity CAs (or delegate) ~~shall~~must collect and destroy PIV-I Cards from Subscribers whenever the cards are no longer valid, whenever possible. Entity CAs (or delegate) ~~shall~~must record destruction of PIV-I Cards.

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

4.9.4 Revocation Request Grace Period

The revocation request grace period is the time available to the subscriber within which the subscriber must make a revocation request after reasons for revocation have been identified.

In the case of key compromise, ~~FBCA subscribers (e.g.,~~ Entity CAs~~)~~ are required to request revocation within one hour~~. For all other reasons, FBCA subscribers are required to request revocation within 24 hours.~~ of confirmation of the compromise.

~~For Entity CAs, see Section 9.6.3.~~

4.9.5 Time within which CA must Process the Revocation Request

~~The FBCA and~~ CA certificates are revoked once all necessary notification periods have elapsed.

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

4.9.6 Revocation Checking Requirements for Relying Parties

~~No stipulation.~~

~~Practice Note: 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.~~

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

Practice Note: Use of revoked certificates could have damaging or catastrophic consequences. 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

For this CP, CRL issuance encompasses both CRL generation and publication.

~~For the FBCA and Entity CAs, see~~CRLs must be issued periodically, even if there are no changes to be made, to ensure timeliness of information. The table below ~~for~~ specifies the issuing frequency of routine CRLs. CRLs may be issued more frequently than specified below.

~~*Table 4 FBCA and Entity CA*~~ **CRL Issuance Frequency**

Assurance Level	Maximum Interval for Routine CRL Issuance	
	Online	Offline*
Rudimentary	No stipulation	No Stipulation
~~Basic~~	~~24 hours~~	~~31 Days~~
~~Medium (all~~All other policies~~)~~	24 hours	~~31~~35 Days
~~PIV-I Card Authentication~~	~~24 hours~~	~~31 Days~~
~~High~~	~~24 hours~~	~~31 Days~~

*An offline CA may incorporate locally attached network equipment such as an HSM or storage array. The CA system and any such locally attached network equipment must be completely isolated (air-gapped) from all other networks and computing systems.

CAs may be operated in an offline manner if the CA only issues:

- CA certificates
- (optionally) CSS certificates, ~~and~~
- (optionally) end user certificates solely for the administration of the ~~principal~~Entity CA~~.~~, and
- (optionally) end user certificates that contain the contentSigning EKU.

However, the interval between routine CRL issuance ~~shall~~must never exceed ~~31~~35 days. ~~Such CAs must meet the requirements specified in section 4.9.12 for issuing Emergency CRLs. (Note: such CAs will also be required to notify the FPKIMA upon Emergency CRL issuance. This requirement will be included in the MOA between the FPKIPA and the Entity.)~~

4.9.8 Maximum Latency ~~of~~for CRLs

~~4.9.8~~ For CAs that operate online, CRLs

~~CRLs shall~~ must be published within 4 hours of generation.

For CAs that operate offline, pre-generated CRLs intended for publication more than 4 hours after generation must be protected in the same manner as the CA. All pre-generated CRLs not yet published must be securely destroyed whenever the CA revokes any certificate. The CPS must describe protections and processes used for generation and protection of any pre-generated CRLs.

Furthermore, each CRL ~~shall~~must be published no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

Note: If pre-generation of CRLs is implemented, the thisUpdate field will be the date of generation. The nextUpdate value will be beyond the date of planned publication.

4.9.9 On-line Revocation/Status Checking Availability

If on-line revocation/status checking is supported by an Entity CA, the latency of certificate status information ~~distributed on-line by Entity CAs or their delegated status responders~~ must meet or exceed the requirements for CRL issuance stated in 4.9.7.

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

For PIV-I certificates, CAs ~~shall~~must support on-line status checking via OCSP [RFC ~~2560~~6960].

4.9.10 On-line Revocation Checking Requirements

~~No stipulation.~~

On-line revocation status checking is optional for relying parties. For certificates where revocation status online checking is not available, CRLs must be used.

4.9.11 Other Forms of Revocation Advertisements Available

A CA may ~~also~~ use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements:

- The alternative method must be described in the CA's approved CPS.
- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.
- The alternative method must meet the issuance and latency requirements for CRLs stated in Sections 4.9.7 and 4.9.8.

4.9.12 Special Requirements Related to Key Compromise

In the event of an Entity ~~Principal~~ CA private key compromise or loss, the FPKIMA must revoke the cross-certificate ~~shall be revoked and a~~, publish an emergency CRL ~~shall be published at the earliest~~as soon as feasible ~~time by~~, and notify the ~~FPKIMA.~~ FPKPA and all cross-certified entities.

For Entity CAs, when a CA certificate is revoked or subscriber certificate is revoked because of compromise, or suspected compromise, of a private key, ~~a~~an emergency CRL must be ~~issued~~published as specified below:

Assurance Level	Maximum Latency for Emergency CRL Issuance
Rudimentary	No stipulation
Basic	24 hours after notification
Medium (all policies)	18 hours after notification
PIV-I Card Authentication	18 hours after notification
High	~~Six~~6 hours after notification

4.9.13 Circumstances for Suspension

Suspension ~~shall~~is not ~~be used~~supported by the FBCA.

~~For Entity CAs, no stipulation.~~

Entity CAs may support certificate suspension and restoration for Subscriber certificates. If suspension and restoration are supported by the Entity CA, the CPS must describe under what circumstances certificates may be suspended and provide details for the corresponding sections below.

4.9.14 Who Can Request Suspension

~~For Entity CAs, no stipulation.~~

For Entity CAs that support suspension, those authorized to request suspension of a certificate must be identified.

4.9.15 Procedure for Suspension Request

~~For Entity CAs, no stipulation.~~

For Entity CAs that support suspension, a request to suspend a certificate must identify the certificate to be suspended, explain the reason for suspension, and allow the request to be authenticated.

The reason code CRL entry extension shall be populated with "certificateHold".

4.9.16 Limits on Suspension Period

~~For Entity CAs, no stipulation.~~

For Entity CAs that support suspension, the maximum time period a certificate may be suspended must be specified. The CPS must describe in detail how this maximum suspension period is enforced. If the subscriber has not removed the certificate from hold (suspension) within that period, the certificate must be revoked. Certificates must not be published on a CRL with a reason code of "certificateHold" beyond the expiration date of the certificate.

Practice Note: In order to mitigate the threat of unauthorized person removing the certificate from hold, the subscriber identity should be authenticated in person using initial identity proofing process described in Sections 3.2.3 or 3.3.2

4.10 CERTIFICATE STATUS SERVICES

~~No stipulation.~~

See Section 4.9.9 for OCSP.

If additional certificate status services are supported, they must be described in the CPS.

4.10.1 Operational Characteristics

~~No stipulation.~~

~~-~~Where applicable this must be described in the CPS.

4.10.2 Service Availability

~~No stipulation.~~

Where applicable this must be described in the CPS.

4.10.3 Optional Features

~~No stipulation.~~

Where applicable this must be described in the CPS.

4.11 END OF SUBSCRIPTION

No stipulation.

4.12 KEY ESCROW &AND RECOVERY

~~The FBCA shall not perform any encryption key recovery functions involving Entity CAs, and shall not store any information encrypted by the FBCA public key that may require key recovery capabilities. However, if encryption key pairs need to be issued by the FBCA covering~~

~~repository system access or for other purposes, the FPKIPA shall publish applicable requirements for that purpose.~~

The FBCA does not support key escrow and recovery.

The following sections are applicable for those Entity CAs that support key escrow and recovery.

4.12.1 Key Escrow and Recovery Policy and Practices

CA private keys are never escrowed.

Subscriber key management keys may be escrowed to provide key recovery. ~~CAs that support private key escrow for key management keys shall do one of the following:~~

- ~~Adopt the *FPKI Key Recovery Policy* (KRP) and develop a Key Recovery Practice Statement (KRPS) describing the procedures and controls~~When implemented ~~to comply with the FPKI KRP; or~~
- ~~Develop a KRP that establishes security and authentication~~, key recovery requirements ~~comparable to the FPKI KRP.~~must be documented in a Key Recovery Policy (KRP). The KRP may be a separate document or ~~combined with the organization's Certificate Policy (CP). Develop a KRPS describing the procedures and controls implemented to comply with the organization's KRP.~~

~~In both cases, the KRPS may be a separate document or~~ may be combined with the ~~CPS~~CP.

Key Recovery policies and practices ~~shall~~must satisfy privacy and security requirements for CAs issuing and managing digital certificates under the Entity's CP.

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

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

Under no circumstances will a subscriber signature key be ~~held in trust by~~escrowed.

4.12.1.1 Key Escrow Process and Responsibilities

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

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

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

4.12.1.2 Key Recovery Process and Responsibilities

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

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

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

Subscribers may use electronic or manual means to request their own escrowed keys from the KRS. The Subscriber may submit the request to the KED, KRA or KRO. If the request is made electronically, the subscriber must digitally sign the request or authenticate to a recovery service using an associated authentication or signature certificate with an assurance level equal to or greater than that of the escrowed key. Manual requests must be made in person, and include proper identity verification by the KRA in accordance with Section 3.2.3.1.

Internal Third-Party Requestors may use electronic or manual means to request the Subscribers' escrowed keys. The Requestor must submit the request to the KRA or KRO. If the request is made electronically, the Requestor must digitally sign the request using an authentication or signature certificate with an assurance level equal to or greater than that of the escrowed key. Manual requests must be made in person, and must include proper identity verification by the KRA in accordance with Section 3.2.3.1.

External Third-Party Requestors must use manual means to request the Subscribers' escrowed keys. The Requestor must submit the request to the KRA or KRO. Manual requests must be made in person, and must include proper identity verification by the KRA in accordance with Section 3.2.3.1.

DDSs must use electronic means to request Subscribers' escrowed keys. Requests must be authenticated as specified in Section 3.5.5.

Third party key recovery in and of itself does not require revocation of a subscriber certificate. This does not prohibit Subscribers from requesting revocation of their own certificates for any reason.

4.12.1.2.1 Key Recovery Through KRA

The KRA must provide access to a copy of an escrowed key only in response to a properly authenticated and authorized key recovery request. Such access requires the actions of at least two KRAs. All copies of escrowed keys must be protected using two-person control procedures during recovery and delivery to the authenticated and authorized Requestor. Split key or password procedures are considered adequate two-person controls, provided they comply with technical controls in Section 6.2.2.

Practice Note: A combination of physical, procedural, and technical security controls can be used to enforce continuous two-person control during recovery and delivery of escrowed keys. The KRS should be designed to maximize the ability to enforce two-person control technically.

The KRA is not required to notify subscribers of a third-party key recovery.

4.12.1.2.2 Automated Self-Recovery

A current Subscriber's escrowed keys may be provided directly to the Subscriber without imposition of two-person control requirements. The KED must only provide escrowed keys to current Subscribers without two-person control upon:

- Verifying that the authenticated identity of the Requestor is the same as the Subscriber associated with the escrowed keys being requested;
- Sending notification to the Subscriber of all attempts (successful or unsuccessful) to recover the Subscriber's escrowed keys that are made by entities claiming to be the subscriber. If the KED does not have information (e.g., an e-mail address) necessary to send notification to the Subscriber of a key recovery request, then the KED must not provide the Subscriber with the requested key material using the automated recovery process

  Practice Note: Where possible, the e-mail address will be from the subject alternative name field of the certificate being recovered.

- Ensuring that the escrowed keys are being sent only to the authenticated Subscriber associated with the escrowed keys; and
- Ensuring that the escrowed keys are encrypted during transmission using cryptography of equal or greater strength than provided by the escrowed keys.

4.12.1.2.3 Key Recovery During Token Issuance

When a Subscriber (individual and/or group/role sponsor or member) is issued a new certificate on a hardware token, private key management keys for the Subscriber may be recovered as part of the issuance process as long as the KED uses secure means, such as Global Platform Secure Channel Protocol, to inject the key history onto the hardware token directly.

The hardware token must meet FIPS 140 Level 2 hardware requirements and the key must be injected into the token such that it is not thereafter exportable.

4.12.1.2.4 Key Recovery by Data Decryption Server

A DDS must be under two-person control, as is required for any CA or KED. A DDS is permitted to automatically recover keys from the KED. The KED must perform the following activities prior to releasing the key:

- Authenticating the Requestor as a legitimate DDS;
- Verifying that the DDS is authorized to recover the escrowed key for the Issuing Organization to which the key belongs;
- Ensuring that the escrowed keys are protected during transmission using cryptography or other means of equal or greater strength than provided by the escrowed keys.

A combination of physical, procedural, and technical security controls must be used to enforce continuous two-person control on the DDSs. The DDSs must be designed to maximize the ability to enforce two-person control technically.

Practice Note: The DDS is considered under two-person control when any human action performed on the DDS requires two persons.

4.12.1.3 Who Can Submit a Key Recovery Application

Subscribers may request recovery of their own escrowed keys. Key recovery may also be requested by internal Third-Party Requestor permitted by the Issuing Organization policy, and by authorized external Third-Party Requestors (e.g., law enforcement personnel with a court order from a competent court).

4.12.1.3.1 Requestor Authorization Validation

The KRA or the KRO, as an intermediary for the KRA, must validate the authorization of the Requestor. KRAs should consult with Issuing Organization management and/or legal counsel, as appropriate.

Issuing Organizations must determine internal notification requirements for External Third-Party key recovery requests and account for situations where the law requires the KED to release the Subscriber's private key without organizational notification.

Nothing in this document is intended to change the current procedures for obtaining information about individuals in connection with such requests.

4.12.1.3.2 Subscriber Authorization Validation

Current Subscribers are authorized to recover their own escrowed key material.

4.12.1.3.3 KRA Authorization Validation

The KED must verify that the KRA has appropriate privileges to obtain the keys for the identified Subscriber's organization.

4.12.1.3.4 KRO Authorization Validation

The KED or KRA must verify that the KRO is authorized to request keys for the identified Subscriber.

4.12.1.3.5 Data Decryption Server Authorization Validation

The KED must verify that the DDS recovery request falls within the organizational scope for which the DDS was established.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

~~For the FBCA, no stipulation.~~

~~Entity~~ The FBCA does not support session key encapsulation and recovery.

CAs that support session key encapsulation and recovery ~~shall~~must identify the document describing the practices in the ~~applicable~~associated CP.

5. FACILITY, MANAGEMENT ~~&~~, AND OPERATIONS CONTROLS

5.1 PHYSICAL CONTROLS

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

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

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

5.1.1 Site Location ~~&~~and Construction

The location and construction of the facility housing ~~the FBCA and Entity~~ CA equipment, as well as sites housing remote workstations used to administer the CAs, ~~shall~~must be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, ~~shall~~must provide robust protection against unauthorized access to ~~the FBCA and Entity~~all CA equipment and records.

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

The ~~FBCA and Entity~~ CA equipment, to include remote workstations used to administer the CAs, ~~shall~~must always be protected from unauthorized access. The security mechanisms ~~shall~~must be commensurate with the level of threat in the equipment environment. Since the FBCA must plan to issue certificates at all levels of assurance, it ~~shall be~~is operated and controlled on the presumption that it will be issuing at least one High Assurance certificate.

The physical security requirements pertaining to CAs that issue only Basic Assurance certificates are:

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

In addition to those requirements, the following requirements ~~shall~~ apply to CAs that issue Medium, Medium Hardware, or High assurance certificates:

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

~~Practice Note: Multiparty physical access control to CA equipment can be achieved by any combination of two or more trusted roles (see Section 5.2.2) as long as the tasks being conducted are segregated in accordance with the requirements and duties defined for each trusted role. As an example, an Auditor and an Operator might access the site housing the CA equipment to perform a tape backup, but only the Operator may perform the tape backup.~~

Practice Note: Multiparty physical access control to CA equipment can be achieved by any combination of two or more trusted roles (see Section 5.2.2) as long as the tasks being conducted are segregated in accordance with the requirements and duties defined for each trusted role. As an example, an Auditor and an Operator might access the site housing the CA equipment to perform a tape backup, but only the Operator may perform the tape backup.

Removable cryptographic modules, activation information used to access or enable cryptographic modules, and other sensitive CA equipment ~~shall~~must be placed in secure containers when not in use. Activation data ~~shall~~must be either ~~be~~ memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and ~~shall~~must not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA.

A security check of the facility housing the ~~FBCA or Entity~~ CA equipment or remote workstations used to administer the CAs (operating at the Basic Assurance level or higher) ~~shall~~must occur if the facility is to be left unattended. At a minimum, the check ~~shall~~must verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when "open", and secured when "closed"; and for ~~the FBCA~~offline CAs, that all equipment other than the repository is shut down~~);~~).
- Any security containers are properly secured~~;~~.
- Physical security systems (e.g., door locks, vent covers) are functioning properly~~; and~~.
- The area is secured against unauthorized access.

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

5.1.2.2 Physical Access for RA Equipment

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

5.1.2.3 Physical Access for CSS Equipment

Physical access control requirements for CSS equipment ~~(if implemented), shall~~that has signing capability must meet the CA physical access requirements specified in Section 5.1.2.1. CSS equipment that does not have a private signing key and only distribute pre-generated OCSP responses are not required to meet these requirements.

5.1.2.4 Physical Access for CMS Equipment

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

5.1.2.5 Physical Access for KED Equipment

Physical access control requirements for KED equipment that store private keys must meet the CA physical access requirements specified in Section 5.1.2.1.

5.1.2.6 Physical Access for DDS Equipment

Physical access control requirements for DDS equipment that store or use private keys must meet the CA physical access requirements specified in Section 5.1.2.1.

5.1.2.7 Physical Access for KRA and KRO Equipment

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

5.1.3 Power and Air Conditioning

The ~~FBCA and Entity CAs (operating at the Basic Assurance level or higher) shall~~CA must have ~~backup capability~~ sufficient ~~to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of~~ alternative power ~~or air conditioning causes~~ supply in the event of a ~~shutdown. In addition, the FBCA~~primary power source failure to either maintain CA operations or, at a minimum, prevent loss of data. The repositories (containing ~~FBCA issued~~CA certificates ~~and~~, CRLs~~) shall~~, and pre-generated OCSP responses) must be

provided with uninterrupted power sufficient for a minimum of six (6) hours operation in the absence of commercial power~~. Entity CAs shall employ appropriate mechanisms,~~ to ~~ensure~~maintain availability and avoid denial of ~~repositories as specified in Section 2.2.1~~service.

5.1.4 Water Exposures

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

Water exposure from fire prevention and protection measures (e.g~~.~~., sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention ~~&~~and Protection

~~No stipulation.~~

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

Sensitive media and documentation that are no longer needed for operations ~~shall~~must be destroyed in a secure manner. For example, sensitive paper documentation ~~shall~~must be shredded, burned, or otherwise rendered unrecoverable.

5.1.8 Off-Site Backup

~~For the FBCA and Entity CAs operating at the Basic Assurance level or higher, full system~~CA backups sufficient to recover from system failure ~~shall~~must be made on a periodic schedule. Backups ~~are to~~must be performed and stored off-site not less than once per week. At least one full backup copy ~~shall~~must be stored at an off-site location separate from the ~~FBCA or Entity~~ CA equipment. Only the latest full backup need be retained. The backup ~~shall~~must be stored at a site with physical and procedural controls commensurate to that of the operational ~~FBCA or Entity CA~~CA.

For offline CAs, the backup must be performed each time the system is turned on or once per week, whichever is less frequent.

Requirements for CA private key backup are specified in Section 6.2.4.

5.2 PROCEDURAL CONTROLS

Unless stated otherwise, the requirements in this section apply equally to the FBCA and Entity CAs.

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The ~~people~~personnel selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust ~~for all uses of the FBCA or an Entity CA.~~the entire PKI. 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.

Trusted Role appointments must be documented and archived as defined in Section 5.4 and Section 5.5.

5.2.1.1 Certification Authority Trusted Roles

The requirements of this policy are defined in terms of four roles~~. (Note:; implementing organizations may define additional roles provided~~ the ~~information derives from the Certificate Issuing and Management Components (CIMC) Protection Profile.)~~following separation of duties are enforced.

1. *Administrator* – authorized to install, configure, and maintain the CA, or, optionally, KED or DDS; establish and maintain system accounts; configure audit parameters; and generate PKI component keys.

2. *Officer* – authorized to request or approve certificate issuance and revocations.

3. *Auditor* – authorized to review, maintain, and archive audit logs.

4. *Operator* – authorized to perform system backup and recovery.

Administrators do not issue certificates to subscribers.

~~The~~These four roles ~~required for each level of assurance~~ are ~~identified in Section 5.2.4.~~ employed at the CA, CMS, KRS, and CSS locations as appropriate. Separation of duties ~~shall~~must comply with Section 5.2.4, and requirements for two-person control with Section 5.2.2, regardless of the titles and numbers of Trusted Roles.

5.2.1.2 Registration Authority Trusted Roles

An RA may be considered an Officer as defined in Section 5.2.1.1 and is responsible for:

- verifying initial identity, as described in Section 3.2;
- entering Subscriber information, and verifying correctness;
- securely communicating requests to and responses from the CA;
- receiving and distributing Subscriber certificates;

The RA role is highly dependent on implementation and local requirements. The responsibilities and controls for RAs shall be explicitly described in the CPS of a CA if the CA uses an RA.

5.2.1.3 Key Recovery Trusted Roles

Due to the security implications and impacts to confidentiality services associated with key recovery, the number and location of Key Recovery Trusted Roles should be closely controlled.

Some PKIs may leverage the RAs to fulfill Key Recovery functions.

5.2.1.3.1 Key Recovery Agent (KRA)

Entity PKIs that support key escrow and recovery must define what trusted roles cover the following responsibilities to ensure that the following functions occur according to the stipulations of the applicable policy:

- Authorized to authenticate requests and recover copies of escrowed keys; and
- Authorized to distribute copies of recovered keys to Requestor, with protection as described in Section 4.12.1.2.1.

5.2.1.3.2 Key Recovery Official (KRO)

Entity PKIs that support key escrow and recovery may have KROs defined as Trusted Roles if they have privileged access to the KED.

A KRO's responsibilities are to ensure that the following functions occur according to the stipulations of the applicable policy:

- Authorized to verify a Requestor's identity and authorization as stated by this policy;
- Authorized to build key recovery requests on behalf of authorized Requestor;
- Authorized to securely communicate key recovery requests to and responses from the KRA; and
- Authorized to participate in distribution of escrowed keys to the Requestor, as described by the associated practice statement (CPS or KRPS).

5.2.2 Number of Persons Required per Task

Only one person is required per task for CAs operating at the Rudimentary and Basic Levels of Assurance.

Two or more persons are required for CAs operating at the Medium (all policies) or High Levels of Assurance for the following tasks:

- CA, KED, or DDS key generation~~;~~.
- CA signing key activation~~;~~.
- CA, KED, or DDS private key backup.

Where multiparty control ~~for logical access~~ is required, at least one of the participants ~~shall~~must be an Administrator. All participants must serve in a trusted role as defined in Section 5.2.1.

Multiparty control for logical access ~~shall~~must not be achieved using personnel that serve in the Auditor Trusted Role.

~~Physical access to the CAs does not constitute a task as defined in this section. Therefore, two-person physical access control may be attained as required in Section 5.1.2.1.~~

5.2.3 Identification and Authentication for Each Role

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

5.2.4 Roles Requiring Separation of ~~Roles~~Duties

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

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

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

Assurance Level	Role Separation Rules
High	Individual personnel ~~shall~~must be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume only one of the Officer, Administrator and Auditor roles. Individuals designated as Officer or Administrator may ~~also~~ assume the Operator role. An auditor may not assume any other role. The CA and RA software and hardware ~~shall~~must identify and authenticate its users and ~~shall~~must enforce these roles. No individual shall have more than one identity.

The FBCA ~~shall operate~~operates at the High Assurance level.

5.3 PERSONNEL CONTROLS

5.3.1 ~~Background,~~ Qualifications, Experience, ~~& Security~~and Clearance Requirements

~~Each Entity shall identify at least one individual or group responsible and accountable for the operation of each CA in that Entity. For the FBCA, these are the FPKIPA and the FPKIMA.~~

All persons filling trusted roles ~~shall~~must be selected on the basis of loyalty, trustworthiness, and integrity. For the FBCA and Federal Agency PKIs, regardless of the assurance level, all trusted roles ~~are required to~~must be held by U.S. citizens. For PKIs operated at Medium Assurance and Medium Hardware, each person filling a trusted role must satisfy at least one of the following:

- The person ~~shall~~must be a citizen of the country where the CA is located; or
- For PKIs operated on behalf of multinational governmental organizations, the person ~~shall~~must be a citizen of one of the member countries; or
- For PKIs located within the European Union, the person ~~shall~~must be a citizen of one of the member States of the European Union; or
- For PKIs other than the FBCA and Federal Agency PKIs, the person ~~shall~~must have a security clearance equivalent to U.S. Secret or higher issued by a NATO member nation or major non-NATO ally as defined by the International Traffic in Arms Regulation (ITAR) – 22 CFR 120.32; or
- For RA personnel only, in addition to the above, the person may be a citizen of the country where the RA is located.

For PKIs, ~~apart from~~other than the FBCA and Federal Agency PKIs, only operated at Rudimentary, Basic, Medium-CBP and Medium Hardware-CBP, there is no citizenship requirement or security clearance specified.

The FPKIMA ~~personnel acting in trusted roles shall~~Program Manager must hold a TOP SECRET security ~~clearances.~~ clearance.

5.3.2 Background Check Procedures

FPKIMA personnel acting in trusted roles ~~shall~~must, at a minimum, undergo procedures necessary to be cleared at the TOP SECRET level.

~~Entity~~ CA personnel ~~shall, at~~must receive a ~~minimum, pass~~favorable adjudication after undergoing a background investigation covering the following areas:

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

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

Adjudication of the background investigation ~~shall~~must be performed by a competent adjudication authority using a process consistent with [Executive Order 12968~~ August 1995~~] or ~~later, or an~~ equivalent ~~level of investigation and adjudication~~.

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

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

~~Practice Note for nongovernmental partners: The qualifications of the adjudication authority and procedures utilized to satisfy these requirements must be demonstrated before cross certification with the FBCA.~~

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

Practice Note for nongovernmental partners: The qualifications of the adjudication authority and procedures utilized to satisfy these requirements must be demonstrated before cross certification with the FBCA.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the ~~FBCA~~CA or ~~Entity CA shall~~RA must receive comprehensive ~~training in all operational duties they are expected to perform, including disaster recovery and business continuity procedures~~.

~~In addition, personnel performing duties with respect to the operation of the FBCA or Entity CA shall receive comprehensive training, or demonstrate competence, in the following areas:~~

~~CA/RA~~Training must be conducted in the following areas:

- CA (or RA) security principles and mechanisms;
- Key Recovery System security principles and mechanisms;
- All PKI software versions in use on the CA (or RA) system~~.~~;
- All PKI duties they are expected to perform;
- Disaster recovery and business continuity procedures; and
- Stipulations of the applicable CP and CPS.

Documentation ~~shall~~must be maintained identifying all personnel who received training and the level of training completed. ~~Where competence was demonstrated in lieu of training, supporting documentation shall be maintained.~~

5.3.4 Retraining Frequency ~~&~~and Requirements

Individuals responsible for PKI roles ~~shall~~must be aware of changes in the ~~FBCA and Entity~~ CA operation. Any significant change to the operations ~~shall~~must have a training (awareness) plan, and the execution of such plan ~~shall~~must be documented. Examples of such changes are ~~FBCA and Entity~~ CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

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

5.3.5 Job Rotation Frequency ~~&~~and Sequence

~~For the FBCA,~~Job rotation is optional. Any job rotation frequency and sequencing procedures ~~shall~~must provide for continuity and integrity of the ~~FBCA~~CA services.

~~For Entity CAs, no stipulation.~~

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

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

5.3.6 Sanctions for Unauthorized Actions

~~The FPKIMA shall~~A CA must take appropriate administrative and disciplinary actions ~~where~~against personnel who have performed actions involving the ~~FBCA~~CA or its ~~repository~~RAs that are not authorized in ~~this~~the corresponding CP, ~~the FBCA~~ CPS, or other documented procedures ~~published by the FPKIMA.~~

~~For Entity CAs, no stipulation~~.

5.3.7 Independent Contractor Requirements

~~Contractor personnel employed~~Contractors fulfilling Trusted Roles must be subject to ~~perform functions pertaining to the FBCA or an Entity CA shall meet the~~ all personnel requirements ~~set forth~~stipulated in the ~~FBCA~~ corresponding policy.

PKI vendors who provide any services must establish procedures to ensure that any subcontractors perform in accordance with the CP ~~or Entity CP, as applicable~~and the CPS.

5.3.8 Documentation Supplied to Personnel

~~For the FBCA and Entity CAs,~~ Documentation sufficient to define duties and procedures for each trusted role ~~shall~~must be provided to the personnel filling that role.

5.4 AUDIT LOGGING PROCEDURES

The objective of audit log ~~files shall be generated for~~ processing is to review all ~~events relating to the security of the FBCA or Entity CAs.~~ actions to ensure they are made by authorized parties and for legitimate reasons.

At a minimum, audit records must be generated for all applicable events identified in Section 5.4.1 of this policy and must be available during audit reviews and third-party audits. For CAs operated in a virtual ~~machine~~ environment ~~(VME)~~, audit ~~logs shall~~records must be generated for all applicable events on ~~both the virtual machine (VM) and isolation kernel (i.e. hypervisor).~~application software and all system software layers.

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

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

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

When Key escrow and Recovery is supported, all KED audit records of unsuccessful key recoveries must be analyzed to determine the cause and to ensure that the KRS is operating correctly and securely, and is not vulnerable to unauthorized use.

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

5.4.1 Types of Events Recorded

~~A message from any source received by the FBCA or Entity CA requesting an action related to the operational state of the CA is an auditable event.~~ All security auditing capabilities of CA operating system and CA applications required by this CP must be enabled during installation. At a minimum, each audit record ~~shall~~must include the following (either recorded automatically or manually for each auditable event):

- ~~The~~What type of event~~,~~ occurred;
- ~~The~~ Date and time when the event occurred~~,~~;
- ~~A~~Where the event occurred (e.g., on what systems or in what physical locations);
- Source of the event;
- Outcome of the event to include success or failure ~~indicator, where appropriate,~~
- ~~The identity of the entity;~~ and ~~/or operator (of the FBCA or Entity CA) that caused the event.~~

~~Detailed audit requirements are listed in the table below according to the level of assurance. The FBCA shall record the events identified in the table for High Assurance.~~

~~All security auditing capabilities of the FBCA or Entity CA operating system and CA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. Where events cannot be automatically recorded, the CA shall implement manual procedures to satisfy this requirement.~~

- Identity of any individuals, subjects, or objects/entities associated with the event.

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

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

~~Auditable Event~~	~~Rudimentary~~	~~Basic~~	~~Medium (all policies) & PIV-I Card Authentication~~	~~High~~
~~SECURITY AUDIT~~				

Auditable Event	Rudimentary	Basic	Medium (all policies) & PIV-I Card Authentication	High
Any changes to the Audit parameters, e.g., audit frequency, type of event audited		X	X	X
Any attempt to delete or modify the Audit logs		X	X	X
Obtaining a third-party time-stamp		X	X	X
IDENTIFICATION AND AUTHENTICATION				
Successful and unsuccessful attempts to assume a role		X	X	X
The value of *maximum authentication attempts* is changed		X	X	X
The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login		X	X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts		X	X	X
An Administrator changes the type of authenticator, e.g., from password to biometrics		X	X	X
LOCAL DATA ENTRY				
All security-relevant data that is entered in the system		X	X	X
REMOTE DATA ENTRY				
All security-relevant messages that are received by the system		X	X	X
DATA EXPORT AND OUTPUT				
All successful and unsuccessful requests for confidential and security-relevant information		X	X	X
KEY GENERATION				

Auditable Event	Rudimentary	Basic	Medium (all policies) & PIV-I Card Authentication	High
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X	X	X
PRIVATE KEY LOAD AND STORAGE				
The loading of Component private keys	X	X	X	X
All access to certificate subject private keys retained within the CA for key recovery purposesPractice Note: Events related to CA certificate issuance may be different from those related to subscriber certificate issuance.	X	X	X	X
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE				
All changes to the trusted public keys, including additions and deletions	X	X	X	X
SECRET KEY STORAGE				
The manual entry of secret keys used for authentication			X	X
PRIVATE AND SECRET KEY EXPORT				
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X	X
CERTIFICATE REGISTRATION				
All certificate requests	X	X	X	X
CERTIFICATE REVOCATION				
All certificate revocation requests		X	X	X
CERTIFICATE STATUS CHANGE APPROVAL				
The approval or rejection of a certificate status change request		X	X	X
CA CONFIGURATION				

Any security-relevant changes to the configuration of the CA		X	X	X
ACCOUNT ADMINISTRATION				
Roles and users are added or deleted	X	X	X	X
The access control privileges of a user account or a role are modified	X	X	X	X
CERTIFICATE PROFILE MANAGEMENT				
All changes to the certificate profile	X	X	X	X
REVOCATION PROFILE MANAGEMENT				
All changes to the revocation profile		X	X	X
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT				
All changes to the certificate revocation list profile		X	X	X
MISCELLANEOUS				
Appointment of an individual to a Trusted Role	X	X	X	X
Designation of personnel for multiparty control			X	X
Installation of the Operating System		X	X	X
Installation of the CA		X	X	X
Installing hardware cryptographic modules			X	X
Removing hardware cryptographic modules			X	X
Destruction of cryptographic modules		X	X	X
System Startup		X	X	X
Logon Attempts to CA Applications		X	X	X
Receipt of Hardware/Software			X	X
Attempts to set passwords		X	X	X
Attempts to modify passwords		X	X	X

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

~~Equipment failure~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Electrical power outages~~			~~X~~	~~X~~
~~Uninterruptible Power Supply (UPS) failure~~			~~X~~	~~X~~
~~Obvious and significant network service or access failures~~			~~X~~	~~X~~
~~Violations of Certificate Policy~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Violations of Certification Practice Statement~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Resetting Operating System clock~~		~~X~~	~~X~~	~~X~~

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

Auditable Event	Rudimentary	Basic	Medium (all policies), PIV-I Card Authentication & High
SECURITY AUDIT			
Any changes to the Audit parameters, e.g., audit frequency, type of event audited		X	X
Any attempt to delete or modify the Audit logs		X	X
IDENTIFICATION AND AUTHENTICATION			
Platform or CA application level authentication attempts		X	X
The value of maximum authentication attempts is changed		X	X
The number of unsuccessful authentication attempts exceeds the		X	X

maximum authentication attempts during user login			
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts		X	X
An Administrator changes the type of authenticator, e.g., from smart card login to password		X	X
DATA ENTRY AND OUTPUT			
Any additional event that is relevant to the security of the CA (such as remote or local data entry or data export); must be documented		X	X
KEY GENERATION			
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X	X
PRIVATE KEY LOAD AND STORAGE			
The loading of CA, RA, CSS, CMS, or other keys used by the CA in the lifecycle management of certificates	X	X	X
All access to certificate subject private keys retained within the CA for key recovery purposes	X	X	X
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE			
Any changes to public keys used by components of the CA to authenticate other components or authorize certificate lifecycle requests (e.g., RA or CMS trust stores)	X	X	X
PRIVATE AND SECRET KEY EXPORT			

The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X
CERTIFICATE REGISTRATION			
All records related to certificate request authorization, approval and signature, whether generated directly on the CA or generated by a related external system or process	X	X	X
CERTIFICATE REVOCATION			
All records related to certificate revocation request authorization, approval and execution, whether generated directly on the CA or generated by a related external system or process		X	X
CERTIFICATE STATUS CHANGE APPROVAL			
All records related to certificate status change request authorization, approval and execution, whether generated directly on the CA or generated by a related external system or process		X	X
CA CONFIGURATION			
Any security-relevant changes to the configuration of the CA. The specific configuration items relevant to the environment in which the CA operates must be identified and documented.		X	X
ACCOUNT ADMINISTRATION			
Roles and users are added or deleted	X	X	X
The access control privileges of a user account or a role are modified	X	X	X
CERTIFICATE PROFILE MANAGEMENT			

All changes to the certificate profile	X	X	X
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT			
All changes to the certificate revocation list profile		X	X
MISCELLANEOUS			
Appointment of an individual to a designated Trusted Role	X	X	X
Installation of the Operating System		X	X
Installation of the CA		X	X
Installing hardware cryptographic modules			X
Removing hardware cryptographic modules			X
Destruction of cryptographic modules		X	X
System Startup		X	X
Logon Attempts to CA Applications		X	X
Receipt of Hardware/Software			X
Attempts to set passwords		X	X
Attempts to modify passwords		X	X
Backing up CA internal database		X	X
Restoring CA internal database		X	X
Records of manipulation of critical files (e.g., creation, renaming, moving), critical files will vary between installation, and must be identified in the relevant documentation			X

The date and time any CA artifact is posted to a public repository			X
Access to CA internal database			X
All certificate compromise notification requests		X	X
Loading tokens with certificates			X
Shipment and receipt of tokens containing key material, or tokens that allow access to key material (e.g., HSM operator cards)			X
Zeroizing tokens		X	X
Re-key of the CA	X	X	X
Configuration changes to the CA server involving:			
- Hardware		X	X
- Software		X	X
- Operating System		X	X
- Patches		X	X
- Security Profiles			X
PHYSICAL ACCESS / SITE SECURITY			
Personnel Access to room housing CA			X
Access to the CA server			X
Known or suspected violations of physical security		X	X
ANOMALIES			
Software Error conditions		X	X
Software check integrity failures		X	X

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

5.4.2 Frequency of Processing Log

~~Audit logs shall be reviewed in accordance to the table below. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the log. Examples of irregularities include discontinuities in the logs and loss of audit data. Actions taken as a result of these reviews shall be documented.~~

~~For the FBCA, the FPKIMA shall explain all significant events in an audit log summary.~~

Audit records must be reviewed at least once every month for online CAs that issue certificates at Basic or above. For offline CAs, the audit logs must be reviewed when the system is activated or every 30 days, whichever is later. CSS, CMS, IDMS and KRS audit log processing frequency shall align with the CA audit log processing frequency.

Assurance Level	Review Audit Log
Rudimentary	Only required for cause
~~Basic~~	~~Only required for cause~~
~~Medium (all policies)~~Basic	At least once ~~every two months~~ ~~Statistically significant set of security audit data generated by Entity CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity~~per month

Assurance Level	Review Audit Log
Medium (all policies) & PIV-I Card Authentication	At least once ~~every two months~~ ~~Statistically significant set of security audit data generated by Entity CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity~~per month
High	At least once per month ~~Statistically significant set of security audit data generated by Entity CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity~~

~~For the FBCA, 100% of security audit data generated by the FBCA since the last review shall be examined.~~

5.4.3 Retention Period for Audit Logs

~~For Medium, Medium Hardware, and High Assurance, audit logs shall be retained on-site until reviewed, as well as being retained in the manner described below. For Rudimentary and Basic Assurance, audit logs shall be retained on-site for at least two months or until reviewed, as well as being retained in the manner described below. The individual who removes audit logs from the FBCA or Entity CA system shall be an official different from the individuals who, in combination, command the FBCA or an Entity CA signature key.~~

At all assurance levels other than Rudimentary audit records must be accessible until reviewed, in addition to specific records being archived as described in Section 5.5

Practice Note: OMB M-21-31 requires Federal agencies maintain all audit records in active storage for a minimum of 12 months from generation.

5.4.4 Protection of Audit Logs

~~FBCA (or Entity CA)~~ System configuration and operational procedures must be implemented together to ensure that ~~:~~

- ~~Only personnel assigned to trusted roles have read access to the logs;~~
- only authorized ~~people~~individuals may move or archive audit ~~logs;~~records and

~~Audit logs~~ that audit records are not modified.

~~The entity performing audit log archive need not have modify access, but~~ Collection of the audit records from the CA system must be performed by, witnessed by or under the control of trusted roles who are different from the individuals who, in combination, command the CA signature key.

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

Procedures must be implemented to protect ~~archived data~~audit records from deletion or destruction ~~prior to the end of the audit log retention period (note that deletion requires modification access).~~

~~The off-site storage location for audit logs shall be~~ before they are reviewed. as described in Section 5.4.2. To protect the integrity of audit records, they must be transferred to a ~~safe, secure location separate~~backup environment distinct from the ~~location~~environment where the ~~data was~~audit records are generated.

> ~~Practice Note: If a system over-writes audit logs after a given time, the audit log is not considered deleted or destroyed if the audit log has been backed up and archived.~~

5.4.5 Audit Log Backup Procedures

Audit ~~logs~~records and audit summaries ~~shall~~must be backed up at least monthly. ~~A copy of~~

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

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

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system may or may not be external to the ~~FBCA or Entity~~ CA system~~.~~ or KRS. Automated audit processes ~~shall~~must be invoked at system (or application) startup, and cease only at system (or application) shutdown. ~~Should it become apparent~~ Audit collection systems must be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files). If an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, ~~then the FPKIMA Administrator (or comparable Entity authority) shall determine whether to suspend FBCA operation (or Entity CA operation respectively)~~operations must be suspended until the problem ~~is~~has been remedied.

5.4.7 Notification to Event-Causing Subject

~~This CP imposes~~There is no requirement to ~~provide notice~~notify a subject that an event was audited ~~to the individual, organization, device, or application that caused the event~~. Real-time alerts are neither required nor prohibited by this policy.

5.4.8 Vulnerability Assessments

~~FBCA personnel shall routinely assess whether the CA system or its components have been attacked or breached.~~

~~For Entity~~ CAs~~, personnel shall~~ must perform routine vulnerability assessments ~~for evidence~~ of ~~malicious activity.~~

~~Practice Note: The security audit data should be reviewed by the security auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Security auditors should check for continuity of the security audit data.~~

~~5.5 RECORDS ARCHIVE~~

~~Executive branch agencies must follow either~~the security controls described in the ~~General Records Schedules established by the National Archives and Records Administration or an agency-specific schedule as~~ applicable~~. All other entities shall~~ policy.

For Federal Agencies operating under this policy, self-assessment of controls and control effectiveness (e.g., FISMA) must be performed in accordance with the frequency determined by the risk rating of the CA.

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

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

Practice Note: The security audit data should be reviewed by the security auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, requests for escrowed keys, attempted access of escrowed keys, unauthenticated responses, and other suspicious or unusual activity. Security Auditors should check for continuity of the security audit data.

5.5 RECORDS ARCHIVAL

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

~~FBCA or Entity~~ The primary objective of the CA archive ~~records shall be sufficiently detailed as~~is to ~~verify that the FBCA or Entity CA was properly operated as well as verify~~prove the

validity of any certificate (including those revoked or expired) issued by the ~~FBCA or Entity CA~~CA in the event of dispute regarding the use of the certificate.

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

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

5.5.1 Types of Events Archived

At a minimum, the following data ~~shall~~must be recorded for archive ~~in accordance with~~as specified for each assurance level:

Data To Be Archived	Rudimentary	~~Basic~~All Other Policies	~~Medium (all policies) & PIV-I Card Authentication~~	~~High~~
~~CA accreditation (if applicable)~~	~~X~~	~~X~~	~~X~~	~~X~~
Certificate Policy	X	X	~~X~~	~~X~~
Certification Practice Statement / Key Recovery Practice Statement	X	X	~~X~~	~~X~~
Contractual obligations	X	X	~~X~~	~~X~~
Other agreements concerning operations of the CA or KRS	X	X	~~X~~	~~X~~
System and equipment configuration	X	X	~~X~~	~~X~~

Data To Be Archived	Rudimentary	~~Basic~~All Other Policies	~~Medium (all policies) & PIV-I Card Authentication~~	~~High~~
Modifications and updates to system or configuration	X	X	~~X~~	~~X~~
~~Certificate requests~~All records related to certificate request authorization, approval and signature, whether generated directly on the CA or generated as part of a related external system or process	X	X	~~X~~	~~X~~
~~Revocation requests~~All records related to certificate revocation, whether generated directly on the CA or generated as part of a related external system or process		X	~~X~~	~~X~~
Subscriber identity Authentication data as per Section 3.2.3		X	~~X~~	~~X~~
Documentation of receipt and acceptance of certificates (if applicable)		X	~~X~~	~~X~~
Subscriber Agreements		X	~~X~~	~~X~~
Documentation of receipt of tokens		X	~~X~~	~~X~~

Data To Be Archived	Rudimentary	~~Basic~~All Other Policies	~~Medium (all policies) & PIV-I Card Authentication~~	~~High~~
All certificates issued or published	X	X	~~X~~	~~X~~
Record of CA Re-key	X	X	~~X~~	~~X~~
~~All CRLs issued and/or published~~		~~X~~	~~X~~	~~X~~
Other data or applications to verify archive contents		X	~~X~~	~~X~~
~~Compliance Auditor reports~~Audit summary reports generated by internal reviews and documentation generated during third party audits		X	~~X~~	~~X~~
Any changes to the Audit parameters, e.g., audit frequency, type of event audited		X	~~X~~	~~X~~
Any attempt to delete or modify the Audit logs		X	~~X~~	~~X~~
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X	~~X~~	~~X~~
All access to certificate subject private keys retained ~~within the CA~~	X	X	~~X~~	~~X~~

Data To Be Archived	Rudimentary	~~Basic~~All Other Policies	~~Medium (all policies) & PIV-I Card Authentication~~	~~High~~
for key recovery purposes				
~~All~~ Changes to ~~the~~ trusted public keys~~,~~ used or published by the CA including ~~additions~~certificates used for trust between the CA and ~~deletions~~other components such as CMS, RA, etc	X	X	~~X~~	~~X~~
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	~~X~~	~~X~~
The approval or rejection of a certificate status change request		X	~~X~~	~~X~~
Appointment of an individual to a Trusted Role (to include KRA/KRO)	X	X	~~X~~	~~X~~
Destruction of cryptographic modules		X	~~X~~	~~X~~
All certificate compromise notifications		X	~~X~~	~~X~~

Data To Be Archived	Rudimentary	~~Basic~~All Other Policies	~~Medium (all policies) & PIV-I Card Authentication~~	~~High~~
Remedial action taken as a result of violations of physical security		X	~~X~~	~~X~~
Violations of Certificate Policy	X	X	~~X~~	~~X~~
Violations of Certification Practice Statement	X	X	~~X~~	~~X~~

5.5.2 Retention Period for Archive

~~The minimum retention periods for archive data are identified below. Executive branch agencies must follow either the General Records Schedule established by the National Archives and Records Administration or an agency-specific schedule as applicable. All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities.~~

~~This minimum retention period for these records is intended only to facilitate the operation of the FBCA and the entities' CAs.~~

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

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

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

~~Assurance Level~~	~~Minimum Retention Period~~
~~Rudimentary~~	~~7 Years & 6 Months~~
~~Basic~~	~~7 Years & 6 Months~~
~~Medium (all policies)~~**~~Practice Note~~**~~: RA archive records can be retained for as long as business purposes require; however, this policy does not waive any organizational policies that may require the destruction of such records or otherwise limit their retention periods.~~	~~10 Years & 6 Months~~
~~PIV-I Card Authentication~~	~~10 Years & 6 Months~~
~~High~~	~~20 Years & 6 Months~~

Practice Note: If the archive records are maintained separately from the CA, communication processes may be required to determine when archive records are no longer needed based on related public certificates.

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

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

5.5.3 Protection of Archive

~~No unauthorized user shall be~~Only Auditors, as described in Section 5.2, or other personnel specifically authorized by the CA, are permitted to ~~write to~~add or delete records from the archive. ~~For the FBCA, archived records may be moved to another medium when authorized by the FPKIMA Administrator.~~Deletion of records identified in Section 5.5.1 before the end of the retention period is not permitted under any circumstances. The contents of the archive ~~shall~~must not be released except in accordance with Sections 9.3 ~~&~~and 9.4.

~~Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents.~~ Archive media ~~shall~~must be stored in a safe, secure storage facility geographically separate from the ~~FBCA or Entity CA itself.~~CA in accordance with its records retention policies. The transfer process between the backup environment and archive location must be documented.

~~If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site.~~
~~Alternatively, an Entity may retain data using whatever procedures have been approved by NARA for that category of documents. Applications required to process the archive data shall also be maintained for a period determined by the FPKIPA for the FBCA (or Entity for the Entity CA).~~

~~Prior to the end of the archive retention period, the FPKIMA shall provide archived data and the applications necessary to read the archives to an FPKIPA-approved archival facility, which shall retain the applications necessary to read this archived data.~~

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

- Maintain the hardware or software required to process or read the archive records, or
- Define a process to transfer records to a new format or medium when the old format or medium becomes obsolete and verify the integrity of the records after transfer

5.5.4 Archive Backup Procedures

If a cross-certified entity chooses to ~~back up~~backup its archive records, the CPS or a referenced document ~~shall~~must describe how the records are backed up and managed.

5.5.5 Requirements for Time-Stamping of Records

CA archive records ~~shall be automatically time-stamped as~~must have accurate timestamps when they are ~~created.~~ added to the archive.

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

The CPS ~~shall~~or KRPS must describe how system clocks used for ~~time-stamping~~timestamping are maintained in synchrony with an authoritative time standard.

5.5.6 Archive Collection System (Internal or External)

~~No stipulation.~~

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

5.5.7 Procedures to Obtain ~~&~~and Verify Archive Information

Procedures detailing how to create, verify, package, transmit, and store archive information ~~shall~~must be ~~published~~included in the ~~applicable~~ CP, KRP, CPS, or ~~CPS~~KRPS.

~~The contents of the archive shall not be released except as determined by the FPKIPA for the FBCA (or Entity for the Entity CA) or as required by law.~~Copies of records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents.

5.6 KEY CHANGEOVER

~~To minimize risk from compromise of a CA's private~~ Each CA's signing key~~, that~~ must have a validity period as described in Section 6.3.2.

Prior to the end of a CA's signing key ~~may~~validity period, a new CA must be ~~changed often;~~established or a re-key on the existing CA must be performed. This is referred to as key changeover. From that time on, only the new key ~~will be used for certificate signing purposes. The older, but still valid, public key will be available to verify old signatures until all of the~~ is used to sign CA and Subscriber certificates ~~signed using the associated~~. The old private key ~~have also expired.~~may continue to be used to sign CRLs and OCSP Responder certificates. If the old private key is used to sign OCSP Responder certificates or CRLs that cover certificates signed with that key, ~~then~~ the old key must be retained and protected.

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

~~For the FBCA, key changeover procedures will either:~~

~~Establish~~When a CA performs a key changeover and thus generates a new public key, the CA must notify all CAs, RAs, and Subscribers that rely on the CA's certificate that it has been changed. The CA must do one of the following:

- Generate key rollover ~~certificates where a certificate containing the old public key will be signed by the new private key, and a~~ certificate ~~containing~~, where the new public key ~~will be~~is signed by the old private key~~;~~, and vice versa or
- ~~If the DN is changed at the same time as the key, new cross certificates shall be established with the Federal Common Policy CA.~~

~~Entity CAs cross certified with the FBCA must be able to continue to interoperate with the FBCA after the FBCA performs a key rollover, whether or not the FBCA DN is changed.~~

- ~~Entity CAs either must establish key rollover certificates as described above or must~~ Obtain a new CA certificate for the new public key from each issuer of the ~~issuers of their~~ current ~~certificates.~~ CA certificate(s).

> ~~Practice Note: For example, a CA in a hierarchical PKI may obtain a new CA certificate from its superior CA rather than establish key rollover certificates.~~

5.7 COMPROMISE &AND DISASTER RECOVERY

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

5.7.1 Incident and Compromise Handling Procedures

The members of The FPKIPA shallmust be notified within 24 hours if any ofthe FBCA or an Entity CA experiences the following cases occur:

- suspected or detected compromise of the CA systems;
- physical or electronic attempts to penetrate penetration of CA systems;
- successful denial of service attacks on CA components;
- any incident preventing the CA from issuing a CRL within 24 hours of prior to the nextUpdate time specified inof the next update field of its currently validprevious CRL.;

This will allow member entities to protect their interests as Relying Parties.

The FPKIMA shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the applicable CPS.

- In the eventsuspected or detected compromise of a CSS;
- suspected or detected compromise of an incident as described above, the Entity shall notify the FPKIPA within 24 hours of incident discovery, along withRA.

The notification must include preliminary remediation analysis.

Within 10 business days ofOnce the incident resolutionhas been resolved, the organization operating the CA shall post a notice on its public web page identifying the incident andmust provide notification directly to the FPKIPA which includes detailed measures taken to remediate the FPKPAincident. The public notice shallmust include the following:

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

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

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

When computing resources, software, and/or data are corrupted, the FBCA and Entity CAs shallmust respond as follows:

- Before returning to operation, ensure that the system's integrity has been restored
- If the CA signature keys are not destroyed**,** CA operation ~~shall~~must be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in Section 4.9.7~~, Table 4~~.
- If the CA signature keys are destroyed**,** CA operation ~~shall~~must be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

In the event of an incident as described above, the Entity CA ~~shall~~must post a notice on its web page identifying the incident and provide notification to the FPKIPA. See Section 5.7.1 for contents of the notice.

5.7.3 Entity (CA) Private Key Compromise Procedures

~~If the FBCA or Entity CA signature keys are compromised or lost (such that compromise is possible even though not certain):~~

5.7.3.1 CA Private Key Compromise Procedures

In the event of a CA private key compromise, the following operations must be performed:

- The CA must immediately inform the FPKIPA and ~~all of its member~~ any entities ~~shall be notified so that entities may issue CRLs revoking any cross-~~known to be distributing the CA certificate (e.g., in a root store).
- The CA must request revocation of any certificates issued to the compromised CA~~;~~.
- ~~A~~The CA must generate new ~~FBCA or Entity CA key pair shall be generated by the FBCA or Entity CA~~ keys in accordance with ~~procedures set forth in the FBCA or Entity CPS; and~~Section 6.1.1.1.
- ~~New FBCA or Entity CA certificates shall be issued to Entities also in accordance with the FBCA or Entity CPS.~~

If the CA ~~distributes its~~distributed the public key in a ~~self-signed~~Trusted Certificate, the CA must perform the following operations:

- Generate a new ~~self-signed certificate shall be distributed~~ Trusted Certificate.
- Securely distribute the new Trusted Certificate as specified in Section 6.1.4.
- ~~The FPKIMA or Entity~~Initiate procedures to notify Subscribers of the compromise.

Subscriber certificates issued prior to compromise of the CA private key may be renewed automatically by the CA under the new key pair (see Section 4.6) or the CA may require Subscribers to repeat the initial certificate application process.

The CA governing body ~~shall~~is encouraged to also investigate and report to the FPKIPA what caused the compromise or loss~~, and what measures~~.

5.7.3.2 KRS Private Key Compromise Procedures

In the event that the KED or DDS is compromised or is suspected to be compromised, the following operations must be performed:

- Notify the FPKIPA of the compromise
- Provide detail concerning the root cause, operational impact, and initial remediation actions
- Determine the extent of the compromise
- Gain concurrence from the FPKIPA on planned resolution. This may include revocation of certificates associated with the compromised private keys stored in the KED or DDS.

If a KRA or KRO certificate is revoked due to compromise, the potential exists for some Subscribers' escrowed keys to have been ~~taken to preclude recurrence.~~exposed during a recovery process, the following operations must be performed:

~~The Entity CA shall post a notice on its web page describing the compromise. See Section 5.7.1 for contents of the notice.~~

- Audit record review by the audit administrator to identify all potentially exposed escrowed keys.
- Revocation of each of the potentially exposed escrowed keys, according to procedures specified in Section 4.9.3, to include Subscriber notification of the revocation
- Reissuance of the KRA or KRO authentication certificate

5.7.4 Business Continuity Capabilities after a Disaster

The ~~FBCA~~CA repository system ~~shall~~must be deployed ~~so as~~ to provide 24-hour, 365 day per year availability~~. The FPKIMA shall implement features to provide~~ with high levels of repository reliability.

~~The FPKIMA shall operate a hot backup site, whose purpose is to ensure continuity of operations in the event of failure of the primary site. The FBCA operations shall be designed to restore full service within six (6) hours of primary system failure.~~

~~The FPKIMA or Entity Principal CA shall at the earliest feasible time securely advise the FPKIPA and all of its member entities in the event~~CAs must have recovery procedures in place to reconstitute the CA after failure.

In the case of a disaster ~~where the FBCA or Entity Principal~~whereby the CA installation is physically damaged and all copies of the ~~FBCA or Entity Principal~~ CA signature ~~keys~~key are destroyed~~.~~

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

~~5.8 CA & RA TERMINATION~~

~~In the event of termination of the FBCA operation, certificates signed by the FBCA shall be revoked~~ as a result, the FPKIPA must be notified at the earliest feasible time, and the FPKIPA ~~shall advise entities that have entered into MOAs with~~must take whatever action it deems appropriate.

5.8 CA OR RA TERMINATION

Whenever possible, the FPKIPA ~~that FBCA operation has terminated so they may revoke certificates they have issued to the FBCA. Prior to FBCA~~must be notified at least two weeks prior to the termination of an Entity CA. For emergency termination, CAs must follow the ~~FPKIMA shall provide~~notification procedures in Section 5.7.

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

- Notify all ~~archived data to an archival facility.~~cross-certified Entities.
- Revoke any issued certificates that have not expired~~, shall be revoked~~
- Generate and publish a final long term CRL with a nextUpdate time past the validity period of all issued certificates~~ shall be generated.~~. This final CRL ~~shall~~must be available for all relying parties until the validity period of all issued certificates has ~~past.~~ passed.
- Once the last CRL has been issued, destroy the private signing key(s) of the FBCA~~ will be destroyed~~.
- Transfer all archive data to an archival facility.

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 the FBCA is terminated~~besought.

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

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

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION ~~&~~AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

Cryptographic keying material used to sign certificates, CRLs or status information ~~by the FBCA shall~~must be generated in [FIPS 140] validated cryptographic modules~~. Cryptographic keying material used to sign certificates, CRLs or status information by Entity CAs shall be generated in FIPS 140 validated cryptographic modules~~ as specified in Section 6.2.1 or modules validated under equivalent international standards.

~~For the FBCA, the modules shall meet or exceed Security Level 3. For Entity CAs, the modules shall meet or exceed Security Level 1 (for Rudimentary), Security Level 2 (for Basic, Medium, or Medium Hardware), or Security Level 3 (for High).~~ Multiparty control is required for CA key pair generation ~~for the FBCA and for Entity CAs operating at the Medium, Medium Hardware, or High levels of assurance~~, as specified in Section ~~5~~6.2.2.

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

> ~~Practice Note: If the audit trail identifies and documents any failures or anomalies in the key generation process, along with the corrective action taken, the key generation process need not be restarted but may continue.~~

For High, Medium Hardware, and Medium Assurance, an independent third party ~~shall~~must validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

6.1.1.2 Subscriber Key Pair Generation

Subscriber key pair generation may be performed by the subscriber, CA, or RA. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in Section 6.1.2 must also be met.

Key generation ~~shall~~must be performed using a FIPS approved method or equivalent international standard.

For PIV-I ~~Hardware certificates, to be used~~, all keys, except for ~~digital signatures and/or authentication, and PIV-I Card Authentication certificates, subscriber~~ key ~~generation shall~~management, must be ~~performed~~generated on ~~hardware tokens that meet~~ the ~~requirements of~~card. (See Appendix A~~.~~.)

For all other certificates at the High and Medium Hardware assurance levels, subscriber key generation ~~shall~~must be performed using a validated hardware cryptographic module as specified

in Section 6.2.1. For Medium and Basic assurance, either validated software or validated hardware cryptographic modules ~~shall~~must be used for key generation as specified in Section 6.2.1.

6.1.1.3 CSS Key Pair Generation

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

6.1.1.4 PIV-I Content Signing Key Pair Generation

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

6.1.2 Private Key Delivery to Subscriber

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

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

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

The ~~FBCA (or Entity~~ CA~~)~~ must maintain a record of the subscriber acknowledgement of receipt of the token.

6.1.3 Public Key Delivery to Certificate Issuer

For CAs ~~operating at the Basic, Medium, Medium Hardware, or High level of assurance~~issuing certificates that assert policies other than Rudimentary, the following requirements apply:

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

For Rudimentary Assurance, no stipulation.

6.1.4 CA Public Key Delivery to Relying Parties

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

~~Self-signed~~ root CA certificates ~~shall~~must be conveyed to relying parties in a secure fashion to preclude substitution attacks. Acceptable methods include:

~~Practice Note: Known acceptable methods for self-signed certificate delivery include:~~

- ~~The CA loading a self-signed certificate onto tokens delivered to Relying Parties via secure mechanisms;~~
- ~~Secure distribution of self-signed certificates through secure out-of-band mechanisms;~~
- ~~Comparison of the hash of the self-signed certificate against a hash value made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and~~
- ~~Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.~~

~~Other methods that preclude substitution attacks may be considered acceptable.~~

- ~~Key rollover certificates are signed with the CA's current private key, so~~ Secure distribution ~~is~~ of the certificate through secure out-of-band mechanisms;

~~Practice Note: To ensure the availability of the new public key, the key rollover certificates should be distributed using repositories.~~

- Download the certificate from a Federal Government operated web site secured with a currently valid certificate and subsequent comparison of the hash of the certificate against a hash value made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not ~~required.~~ acceptable as an authentication mechanism)

~~CA Certificates are signed with the issuing CA's current private key, so secure distribution is not required.~~

Practice Note: Other methods that preclude substitution attacks may be considered acceptable.

6.1.5 Key Sizes

~~All FIPS-approved signature algorithms shall be considered acceptable~~This CP requires use of RSA PKCS #1, RSASSA-PSS, or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below.

~~For CAs that distribute self-signed certificates to relying parties, the CA's subject public keys in such certificates shall be at least 2048 bits for RSA, or at least 224 bits for ECDSA. Those CAs that distribute self-signed certificates and whose key pairs were generated before September 13, 2005 may be 1024 bits for RSA. Public keys in all self-signed certificates generated after 12/31/2010 that expire after 12/31/2030 shall be at least 3072 bits for RSA, or at least 256 bits for ECDSA.~~

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

~~CAs that generate certificates and CRLs under this policy shall use SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 hash algorithm when generating digital signatures. For Rudimentary and Basic Assurance, signatures on certificates and CRLs that are issued after 12/31/2013 shall be generated using, at a minimum, SHA-224. For Medium and High Assurance, signatures on certificates and CRLs that are issued after 12/31/2010 shall be generated using, at a minimum, SHA-224, however, RSA signatures on CRLs that are issued before January 1, 2012, and that include status information for certificates that were generated using SHA-1 may be generated using SHA-1. RSA signatures on CRLs that only provide status information for certificates that were generated using SHA-1 may continue to be generated using SHA-1. Signatures on certificates and CRLs that are issued after 12/31/2030 shall be generated using, at a minimum, SHA-256. For Medium assurance, signatures on certificates and CRLs asserting certificate policy OIDs that identify the use of SHA-1 may be generated using SHA-1. CAs that issue end entity certificates that assert non-SHA1 policies after December 31, 2010 must not also issue end entity certificates signed with SHA-1.~~

Certificates ~~issued to OCSP responders that only include SHA-1 certificates may be signed using SHA-1.~~

~~Where implemented, CSSes shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs. After December 31, 2010, for Medium and High Assurance, OCSP responders that generate signatures on OCSP responses using SHA-1 shall only provide signed responses that are pre-produced (i.e., any signed response that is~~

~~provided to an OCSP client shall have been signed before the OCSP responder received the request from the client).~~

~~End-entity certificates shall~~ must contain ~~public keys that are at least 1024~~ 2048-, 3072-, or 4096-bit ~~for~~ RSA~~, DSA~~ keys, or ~~Diffie-Hellman,~~256- or ~~160 bits for~~384-bit elliptic curve ~~algorithms. The following special conditions also apply:~~keys.

- ~~End-entity certificates that expire after 12/31/2030 shall contain public keys that are at least 3072 bits for RSA or DSA, or 256 bits for elliptic curve algorithms.~~
- ~~End-entity certificates that include a keyUsage extension that only asserts the *digitalSignature* bit that expire on or after 12/31/2013 shall contain public keys that are at least 2048 bits for RSA or DSA, or 224 bits for elliptic curve algorithms.~~
- ~~Beginning 01/01/2011, all valid end-entity certificates that include a keyUsage extension that asserts the *nonRepudiation*, *keyEncipherment*, *dataEncipherment*, or *keyAgreement* bit shall contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.~~
- ~~Beginning 01/01/2011, all valid end-entity certificates that do not include a keyUsage extension shall contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.~~

	CA certificates that expire on or before December 31, 2030	CA certificates that expire after December 31, 2030
Minimum Key Size	RSA: 2048 Elliptic Curve: 256	RSA: 3072 Elliptic Curve: 256
Hash Algorithm	SHA-256, SHA-384, or SHA-512	SHA-256, SHA-384, or SHA-512

	Subscriber certificates that expire on or before December 31, 2030	Subscriber certificates that expire after December 31, 2030
Minimum Key Size	RSA: 2048 Elliptic Curve: 256	RSA: 3072 Elliptic Curve: 256
Hash Algorithm	SHA-256, SHA-384, or SHA-512	SHA-256, SHA-384, or SHA-512

All ~~end-entity~~Subscriber certificates associated with PIV-I ~~shall~~must contain public keys and algorithms that conform to [NIST SP 800-78].

~~The FBCA shall not issue a cross-certificate with a validity period extending beyond 12/31/2010 to any Entity Principal CA unless all of the following conditions apply:~~

- ~~Certificates, other than self-signed certificates, that expire after 12/31/2030 are signed with keys of at least 3072 bits for RSA or at least 256 bits for ECDSA.~~
- ~~Certificates that expire after 12/31/2010 are signed with keys of at least 2048 bits for RSA or at least 224 bits for ECDSA.~~
- ~~End-entity certificates that include a keyUsage extension that asserts the *nonRepudiation*, *keyEncipherment*, *dataEncipherment*, or *keyAgreement* bit that expire on or after 12/31/2010 contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.~~
- ~~End-entity certificates that do not include a keyUsage extension that expire on or after 12/31/2010 contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.~~

Use of Transport Layer Security (TLS~~ or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys through 12/31/2010. Use of TLS~~) or another protocol providing similar security to accomplish any of the requirements of this CP ~~shall~~must require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 2048-bit RSA or equivalent for the asymmetric keys~~ after 12/~~. After December 31~~/2010.~~, 2030, use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP ~~shall~~must require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 3072-bit RSA or equivalent for the asymmetric keys~~ after 12/31/2030~~.

KED and DDS keys must be at equal to or stronger than the keys being escrowed.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters ~~for signature algorithms defined in the Digital Signature Standard (DSS) shall~~generation and quality checking must be ~~generated~~conducted in accordance with [NIST SP 800-89]. Key validity must be confirmed in accordance with ~~FIPS 186.~~[NIST SP 800-56A].

~~Parameter quality checking (including primality testing for prime numbers) shall be performed in accordance with FIPS 186; additional tests may be specified by the FPKIPA.~~

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

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

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

~~Subscriber certificates shall assert key usages based on the intended application of the key pair. In particular, certificates~~ All certificates must include a critical Key Usage extension

- Certificates to be used only for ~~digital signatures (including~~ authentication~~) shall~~ must set only the digitalSignature ~~and/or *nonRepudiation* bits.~~ bit.
- Certificates to be used ~~for key or data encryption shall set the~~by Human Subscribers for digital signatures must set the digitalSignature and nonRepudiation bits.
- Certificates that have the nonRepudiation bit set, must not have keyEncipherment ~~and/or *dataEncipherment* bits.~~ bit or keyAgreement bit set.
- Certificates to be used for encryption (RSA) must set the keyEncipherment bit.
- Certificates to be used for key agreement ~~shall~~(ECC) must set the keyAgreement bit.
- CA certificates must set only cRLSign and keyCertSign bits.

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

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

Rudimentary, Basic, and Medium Assurance Level certificates may include a single key for use with encryption and signature in support of legacy applications. Such dual-use certificates ~~shall~~must be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CP. Such dual-use certificates ~~shall~~must never assert the non-repudiation key usage bit, and ~~shall~~must not be used for authenticating data that will be verified on the basis of the dual-use certificate at a future time. Entities are encouraged at all levels of assurance to issue Subscribers two key pairs, one for key management and one for digital signature and authentication.

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

~~If a certificate is used for authentication of ephemeral keys, the~~ The Extended Key Usage ~~bit in the certificate must assert the *digitalSignature* bit and may or may not assert *keyEncryption* and *keyAgreement* depending on the public key in the certificate.~~extension must not contain *anyExtendedKeyUsage* {2.5.29.37.0}.

PIV-I Content Signing certificates ~~shall~~must include ~~an extended key usage of~~a critical Extended Key Usage extension that asserts only *id-fpki-pivi-content-signing* {2.16.840.1.101.3.8.7} (see [PIV-I Profile]).

PIV-I Card Authentication certificates must include a critical Extended Key Usage extension that asserts id-piv-cardAuth {2.16.840.1.101.3.6.8}

6.2 PRIVATE KEY PROTECTION ~~&~~AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards ~~&~~and Controls

The relevant standard for cryptographic modules is [FIPS ~~PUB~~ 140~~,~~], *Security Requirements for Cryptographic Modules*. A FIPS 140 Level 1 or higher validated cryptographic module must be used for all cryptographic operations.

Cryptographic modules ~~shall~~must be minimally validated to the FIPS 140 level identified in this section. Additionally, the FPKIPA reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by the FBCA.

~~Practice Note: The Federal PKI Policy Authority may determine that other comparable validation, certification, or verification standards are sufficient when cross-certifying with non-U.S. government PKIs.~~

~~The table below summarizes the minimum requirements for cryptographic modules; higher levels may be used.~~

~~Assurance Level~~	~~CA, CMS & CSS~~	~~Subscriber~~	~~RA~~
~~Rudimentary~~	~~Level 1 (Hardware or Software)~~Practice Note: The Federal PKI Policy Authority may determine that other comparable validation, certification, or verification standards are sufficient when cross-certifying with non-U.S. government PKIs.	~~N/A~~	~~Level 1 (Hardware or Software)~~
~~Basic~~	~~Level 2 (Hardware or Software)~~	~~Level 1~~	~~Level 1 (Hardware or Software)~~
~~Medium~~	~~Level 2 (Hardware)~~	~~Level 1~~	~~Level 2 (Hardware)~~
~~PIV-I Card Authentication~~	~~Level 2 (Hardware)~~	~~Level 2 (Hardware)~~	~~Level 2 (Hardware)~~
~~Medium Hardware~~	~~Level 2 (Hardware)~~	~~Level 2 (Hardware)~~	~~Level 2 (Hardware)~~
~~High~~	~~Level 3 (Hardware)~~	~~Level 2 (Hardware)~~	~~Level 2 (Hardware)~~

~~PIV-I Cards are PKI tokens that have private keys associated with certificates asserting policies mapped to PIV-I hardware or PIV-I cardAuth. PIV-I Cards shall only~~The table below summarizes the minimum FIPS 140 requirements for cryptographic modules; higher levels may be used.

Assurance Level	CA	CMS & CSS	Subscriber	RA
Rudimentary	Level 1	Level 1	N/A	Level 1
Basic	Level 2	Level 2	Level 1	Level 1
Medium	Level 3 (Hardware)	Level 2 (Hardware)	Level 1	Level 2 (Hardware)
PIV-I Card Authentication	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
Medium Hardware	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
High	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

PIV-I Cards must be issued using card stock that has been tested and approved by the FIPS 201 Evaluation Program and listed on the GSA Approved Products List (APL). Card stock that has been removed from the APL may continue to be issued for no more than one year after GSA approved replacement card stock is available. PIV-I cards issued using the deprecated card stock may continue to be used until the current subscriber certificates expire, unless otherwise notified by the FPKIPA/FPKIMA. ~~On an annual basis, for each PCI configuration used (as defined by the FIPS 201 Evaluation Program), one populated, representative sample PIV-I Card shall be submitted to the FIPS 201 Evaluation Program for testing.~~

For hardware tokens associated with PIV-I, see Appendix A for additional requirements.

Any pseudo-random numbers used for key generation material must be generated using a FIPS-validated cryptographic module.

6.2.1.1 Custodial Subscriber Key Stores

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

Cryptographic modules for Custodial Subscriber Key Stores at the Rudimentary Assurance Level ~~shall~~must be no less than FIPS 140 Level 1 (Hardware or Software). For all other levels, the cryptographic module ~~shall~~must be no less than FIPS 140 Level 2 Hardware.

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

6.2.2 Private Key Multi-Person Control

Use of the FBCA private signing key ~~shall require~~requires action by multiple persons as set forth in Section 5.2.2 of this CP.

Use of the Entity CA private signing key ~~shall~~and CSS private signing key must require action by multiple persons at Medium, Medium Hardware, and High Assurance as set forth in Section 5.2.2 of this CP.

PIV-I Content Signing key activation requires the same multiparty control established for the Entity CA (see Section 5.2.2).

6.2.3 Private Key Escrow

~~6.2.3.1 Escrow of FBCA and Entity CA~~ CA private ~~signature key~~

~~Under no circumstances shall an FBCA or Entity CA signature key used to sign certificates or CRLs be~~keys are never escrowed.

~~6.2.3.2 Escrow of CA encryption~~Human Subscriber key management keys

~~The FBCA shall not perform any encryption~~ may be escrowed to provide key recovery ~~functions involving encryption keys issued to Entity CAs. However, if encryption key pairs need to be issued by the~~as described in Section 4.12.1.

~~FBCA covering repository system access or for other purposes, the Federal PKI Policy Authority shall publish applicable requirements for that purpose.~~

~~For Entities, no stipulation.~~

~~6.2.3.3 Escrow of Subscriber private signature keys~~

Subscriber private signature keys ~~shall not be escrowed.~~

~~6.2.3.4 Escrow of Subscriber private encryption and dual use keys~~

~~Subscriber private dual use keys shall~~must not be escrowed.

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

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

6.2.4 Private Key Backup

~~6.2.4.1 Backup~~All backups of ~~FBCA & Entity~~ CA ~~Private Signature Key~~

~~FBCA~~, CSS, and PIV-I Content Signing private signature keys ~~shall~~must be ~~backed up~~accounted for and protected under the same multi-person control~~,~~ as ~~specified in Section 5.2.2.~~

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

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

~~6.2.4.2 Backup of subscriber private signature key~~

~~At the Medium Hardware and High assurance levels, Subscriber private signature keys may not be backed up or copied.~~

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

Private Key	Backup
CA • all applicable policies	Required
CSS • all applicable policies	Optional
PIV-I Content Signing • id-fpki-certpcy-pivi-contentSigning	Optional
Hardware Signature and Authentication • id-fpki-certpcy-highAssurance • id id-fpki-certpcy-pivi-cardAuth • id-fpki-certpcy-pivi-hardware	Not Permitted
Hardware Subscriber Key Management • id-fpki-certpcy-mediumHardware • id-fpki-certpcy-mediumHW-CBP	Optional

Hardware Device • id-fpki-certpcy-mediumDeviceHardware	Optional
Software Signature and Authentication • id-fpki-certpcy-rudimentaryAssurance • id-fpki-certpcy-basicAssurance • id-fpki-certpcy-mediumAssurance • id-fpki-certpcy-medium-CBP	Optional *
Software Subscriber Key Management • id-fpki-certpcy-rudimentaryAssurance • id-fpki-certpcy-basicAssurance • id-fpki-certpcy-mediumAssurance • id-fpki-certpcy-medium-CBP	Optional
Software Device • id-fpki-certpcy-mediumDevice	Optional

* Software Subscriber private signature keys may be backed up or copied, but must be held in the Subscriber's control.

6.2.5 ~~Backed up subscriber~~Private Key Archival

CA private signature keys ~~shall not be stored in plain text form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.~~

~~Backup of~~and Subscriber ~~Key Management Private Keys~~private signature keys must not be archived.

~~Backed up~~CAs may maintain an archive of escrowed Subscriber private key management keys ~~shall not be stored in plain text form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.~~

~~6.2.4.3 Backup of CSS Private Key~~

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

~~6.2.4.4 Backup of PIV-I Content Signing Key~~

~~Backup of PIV-I Content Signing private signature keys may be required to facilitate disaster recovery. In which case, PIV-I Content Signing private signature keys shall be backed up under multi-person control.~~

~~*6.2.4.5 Backup of Device Private Keys*~~

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

~~6.2.5 Private Key Archival~~

~~Private signature keys shall not be archived.~~

~~For private encryption keys (key management or key transport), no stipulation~~accordance with Sections 4.12, 5.1, 5.2, and 6.2.1.

6.2.6 Private Key Transfer into or from a Cryptographic Module

~~FBCA~~A CA private key must not exist in plain text outside the cryptographic module.

CA, CSS and ~~Entity CA~~PIV-I Content Signing private signature keys may be exported from the cryptographic module only to perform CA key backup procedures as described in Section 6.2.4. ~~1. At no time shall the CA private key exist in plain text outside the cryptographic module.~~

~~All other keys shall be generated by and in a cryptographic module. In the event that a~~ If any private key is ~~to be~~ transported from one cryptographic module to another, the private key must be ~~encrypted during transport;~~protected using a FIPS approved algorithm and at a bit strength commensurate with the key being transported. Private keys must never exist in plaintext form outside the cryptographic module boundary.

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

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in [FIPS-140~~.~~].

6.2.8 Method of Activating Private Keys

~~For the FBCA and Entity CAs that operate at the Medium, Medium Hardware, or High level of assurance, CA signing key activation requires multiparty control as specified in Section 5.2.2.~~

~~In addition, PIV-I Content Signing key activation requires the same multiparty control established for the Entity CA (see Section 5.2.2).~~

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

~~For PIV-I Card Authentication, mediumDevice and mediumDeviceHardware user activation of the private key is not required.~~

~~For certificates issued under the mediumDevice and mediumDeviceHardware policy OIDs, the device may be configured to activate its private key without requiring its human sponsor or authorized administrator to authenticate to the cryptographic token, provided that appropriate physical and logical access controls are implemented for the device and its cryptographic token. The strength of the security controls shall be commensurate with the level of threat in the device's environment, and shall protect the device's hardware, software, and the cryptographic token and its activation data from compromise.~~

~~Methods~~Cryptographic modules must be protected from unauthorized access.

Subscriber private key activation requirements are detailed in the following table:

Mapped Policy	Activation Requirements
id-fpki-certpcy-basicAssurance id-fpki-certpcy-mediumAssurance id-fpki-certpcy-medium-CBP id-fpki-certpcy-mediumHardware id-fpki-certpcy-mediumHW-CBP id-fpki-certpcy-pivi-hardware id-fpki-certpcy-highAssurance	Passphrases, PINs, or biometrics. When passphrases or PINs are used, they must be a minimum of six (6) characters. Entry of activation data must be protected from disclosure (i.e., the data should not be displayed while it is entered).
id-fpki-certpcy-mediumDevice id-fpki-certpcy-mediumDeviceHardware	May be configured to activate the private key without requiring a human sponsor or authorized administrator to authenticate to the cryptographic token. The appropriate physical and logical access controls must be implemented for the device and its cryptographic token.

id-fpki-certpcy-pivi-contentSigning	May be configured to activate the private key without requiring a human sponsor or authorized administrator to authenticate to the cryptographic token. The appropriate physical and logical access controls must be implemented for content signing operations conformant with PIV issuance requirements (see [FIPS 201]). The strength of the security controls must be commensurate with the level of threat in the PIV-I credential issuance system's environment, and must protect the hardware, software, and the cryptographic token and its activation data from compromise.
id-fpki-certpcy-pivi-cardAuth	None.

6.2.9 Method of Deactivating Private Keys

~~Cryptographic modules that have been activated shall not be available to unauthorized access.~~ After use, the cryptographic module ~~shall~~must be deactivated~~, e.g.,~~ via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. CA Hardware cryptographic modules ~~shall~~must be ~~removed and stored~~physically secured per requirements in ~~a secure container~~Section 5.1 when not in use.

6.2.10 Method of Destroying Private Keys

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

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 OTHER ASPECTS OF KEY MANAGEMENT

6.3.1 Public Key Archival

~~The~~ Public key ~~is archived as part of the certificate~~ archival must be in accordance with Section 5.5.

6.3.2 Certificate Operational Periods~~/~~ and Key Usage Periods

~~If operated online, the FBCA shall limit the use of its private keys to a maximum of three years for certificate signing and six years for CRL signing. If the FBCA is operated offline, its private key may be used for a maximum of six years for certificate signing and ten years for CRL signing. CAs that distribute their self-signed certificates for use as trust anchors shall limit the use of the associated private key to a maximum of 20 years; the self-signed certificates shall have a lifetime not to exceed 37 years. For all other CAs, the CA shall limit the use of its private keys to a maximum of six years for subscriber certificates and ten years for CRL signing and OCSP responder certificates. Code and content signers may use their private keys for three years; the lifetime of the associated public keys shall not exceed eight years. Subscribers' signature private keys and certificates have a maximum lifetime of three years. Subscriber key management certificates have a maximum lifetime of 3 years; use of subscriber key management private keys is unrestricted.~~

~~PIV-I subscriber certificate expiration shall not be~~A CA private key may be used to sign CRLs and OCSP responder certificates for the entire usage period. All certificates signed by a specific CA key pair must expire before the end of that key pair's usage period.

Key	Private Key	Certificate
Root CA certificate (self-signed)	20 years	20 years
Federal Bridge CA certificate	10 years	10 years
Intermediate/Signing CA certificate	10 years	10 years
Cross Certificate	3 years	3 years
Subscriber Authentication	3 years	3 years
Subscriber Signature	3 years	3 years
Subscriber Encryption	Unrestricted	3 years
PIV-I Card Authentication	3 years	3 years

PIV-I Content Signing	3 years	9 years*
Code Signing	3 years	8 years
OCSP Responder	3 years	120 days
Device	3 years	3 years

* Expiration of the Content Signing certificate must be later than the expiration of the Subscriber certificates on the same PIV-I credential.

Subscriber certificates on a PIV-I card must expire no later than the expiration date of the PIV-I hardware token on which ~~the certificates~~they reside.

~~Subscriber public keys in certificates that assert the id-fpki-pivi-content-signing OID in the extended key usage extension have a maximum usage period of nine years. The private keys corresponding to the public keys in these certificates have a maximum usage period of three years. Expiration of the id-fpki-certpcy-pivi-contentSigning certificate shall be later than the expiration of the id-fpki-certpcy-pivi-hardware and id-fpki-certpcy-pivi-cardAuth certificates.~~

~~For PIV-I, CSS certificates that provide revocation status have a maximum certificate validity period of 31 days.~~

~~Practice Note: Signatures generated with these keys may be validated after expiration of the certificate.~~

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

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

Practice Note: CA signing key usage is determined in the context of the length of the validity periods of the certificates issued to and by the CA.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation ~~&~~and Installation

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

Where the ~~FBCA or an Entity~~ CA uses passwords as activation data for the CA signing key, at a minimum the activation data ~~shall~~must be changed upon CA re-key.

For Medium Assurance and above, RA and Subscriber activation data may be user-selected. The strength of the activation data must meet or exceed the requirements for authentication mechanisms stipulated for Level 2 in [FIPS 140]. If the activation data must be transmitted, it must be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

For PIV-I, in the event activation data must be reset, a successful biometric 1:1 match of the applicant against the biometrics collected in Section 3.2.3.1 is required. This biometric 1:1 match must be conducted by an RA, self-service portal that authenticates the user via the biometric, a trusted agent of the issuer.

6.4.2 Activation Data Protection

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

- memorized
- biometric in nature, or
- recorded and secured at the level of assurance associated with the activation of the cryptographic module, and ~~shall~~must not be stored with the cryptographic module.

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

6.4.3 Other Aspects of Activation Data

CAs must define any other aspects of Activation Data in its CPS.

~~For PIV-I, in the event activation data must be reset, a successful biometric 1:1 match of the applicant against the biometrics collected in Section 3.2.3.1 is required. This biometric 1:1 match must be conducted by a trusted agent of the issuer.~~

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

For ~~the FBCA,~~CAs, KEDs, and DDSs the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The ~~FBCA~~CA and its ancillary parts ~~shall~~must include the following functionality~~:~~ (these functions pertain to all system software layers, where applicable):

- ~~Require authenticated logins~~

- ~~Provide Discretionary Access Control~~
- ~~Provide a security audit capability~~
- ~~Restrict~~authenticate the identity of users before permitting access ~~control~~ to ~~FBCA services and PKI~~the system or applications;
- manage privileges of users to limit users to their assigned roles;
- ~~Enforce separation of duties for PKI roles~~
- ~~Require identification and authentication of PKI roles and associated identities~~
- ~~Prohibit object re-use or require separation for FBCA random access memory~~
- generate and archive audit records for all transactions; (see Section 5.4)
- enforce domain integrity boundaries for security critical processes;
- require use of cryptography for session communication and database security;
- ~~Archive FBCA history and audit data~~
- require self-test security-related ~~FBCA~~CA services;
- require a trusted path for identification of ~~PKI roles and associated identities~~all users;
- ~~Require a~~provide residual information protection; and
- require recovery ~~mechanism for keys and the FBCA system~~
- ~~Enforce domain integrity boundaries for security critical processes~~

~~For those portions of the FBCA operating in a VME, the following security functions also pertain to the hypervisor:~~

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

For ~~Entity CAs~~CSS, the computer security functions listed below are required~~. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The Entity CA and its ancillary parts shall include the~~

~~following functionality (in a VME,~~ (these functions ~~are~~ pertain to all system software layers, where applicable ~~to both the VM and hypervisor~~):

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

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

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see Section 5.4)
- enforce domain integrity boundaries for security critical processes; ~~and~~
- ~~support~~provide residual information protection; and
- require recovery from ~~key or~~ system failure.

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

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

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

- ~~authenticate the identity of users before permitting access to the system or applications;~~
- ~~manage privileges of users to limit users to their assigned roles;~~
- ~~generate and archive audit records for all transactions; (see section 5.4)~~
- ~~enforce domain integrity boundaries for security critical processes; and~~
- ~~support recovery from key or system failure.~~

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

6.5.2 Computer Security Rating

~~No Stipulation.~~

For the FBCA, not applicable.

Entity CAs must identify any Computer Security Rating requirements.

6.6 LIFE-CYCLE ~~SECURITY~~TECHINCAL CONTROLS

6.6.1 System Development Controls

The System Development Controls for CAs (including any remote workstations used to administer the ~~FBCA~~CA) and ~~Entity CAs~~RAs at the Basic Assurance level and above are as follows:

- ~~For commercial off-the-shelf~~Where open source software~~, the software shall be designed and developed under a formal, documented development methodology.~~
- ~~For hardware and software developed specifically for a particular CA~~ has been utilized, the applicant ~~shall~~must demonstrate that security requirements were achieved through ~~a combination of~~ software verification ~~& validation, structured development approach, and controlled development environment.~~
- ~~Where open source software has been utilized, the applicant shall demonstrate that security requirements were achieved through software verification &~~and validation and structured development/life-cycle management.
- Hardware and software ~~procured~~used to administer or operate the CA ~~shall~~must be ~~purchased~~procured and shipped in a fashion to reduce the likelihood that any ~~particular~~ component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- Custom hardware and software must be developed in a controlled environment, and the development process must be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- The CA hardware and software, including ~~the VME hypervisor, shall~~all system software layers, must be dedicated to operating and supporting the CA (i.e., the systems and services dedicated to the issuance and management of certificates). There ~~shall~~must be no other applications~~;~~, hardware devices, network connections, or component software installed which are not part of the CA operation~~. In a VME, a single hypervisor~~, administration, monitoring and security compliance of the system. CA hardware and system software layers may support multiple CAs and their supporting systems, provided all systems have comparable security controls and are dedicated to the support of the CA in compliance of the same CP.
- ~~In a VME, all VM systems must operate in the same security zone as the CA.~~
- Proper care ~~shall~~must be taken to prevent malicious software from being loaded onto the CA equipment. All applications required to perform the operation of the CA must be obtained from documented sources. Except for Offline CAs, CA and RA hardware and software ~~shall~~must be scanned for malicious code on first use and periodically thereafter.

- Hardware and software updates ~~shall~~must be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the ~~FBCA or Entity~~ CA system as well as any modifications and upgrades ~~shall~~must be documented and controlled. There ~~shall~~must be a mechanism for detecting unauthorized modification to ~~the FBCA or Entity~~ CA software or configuration. ~~A formal configuration management methodology shall be used for installation and ongoing maintenance of the FBCA or Entity CA system.~~ The ~~FBCA or Entity~~ CA software, when first loaded, ~~shall~~must be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. ~~For the FBCA,~~The CA must periodically verify the integrity of the software ~~shall be verified by the FPKIMA at least weekly (e.g., in conjunction with CRL publication).~~.

The FBCA verifies the integrity of the software when the CA is powered on.

6.6.3 Life Cycle Security ~~Ratings~~Controls

~~No stipulation.~~

CAs must identify any life cycle security control requirements in the applicable CP.

6.7 NETWORK SECURITY CONTROLS

~~Network security controls shall be employed~~This section does not apply to offline CAs.

A network guard, firewall, or filtering router must protect ~~the FBCA~~ network access to CA and ~~the FBCA repository. Networking equipment shall turn off~~KRS equipment. The network guard, firewall, or filtering router must limit services allowed to and from the CA and KRS equipment to those required to perform CA and KRS functions.

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

~~The FBCA repository shall be connected to the Internet and provide continuous service (except, when necessary, for brief periods of maintenance or backup).~~

Any boundary control devices used to protect the ~~FBCA repository or FBCA~~ local area network ~~shall~~on which PKI equipment is hosted must deny all but the necessary services to the PKI equipment ~~even if those services are enabled for other devices on the network~~.

~~Entity CAs,~~ RAs, CMSs, repositories, CSSs, and remote workstations used to administer the CAs~~, and certificate status servers shall~~ must employ appropriate network security controls.

Networking equipment ~~shall~~must turn off unused network ports and services. Any network software present ~~shall~~must be necessary to the ~~functioning~~function of the equipment.

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

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

6.8 TIME STAMPING

Asserted times ~~shall~~must be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events, see Section 5.4.1.

7. CERTIFICATE, ~~CARL/~~CRL, AND OCSP PROFILES ~~FORMAT~~

7.1 CERTIFICATE PROFILE

~~7.1.1 Version Numbers~~

~~The FBCA and Entity CAs shall issue X.509 v3 certificates~~PIV-I authentication, card authentication and content signing certificates must conform to the relevant profile worksheets in the [FBCA-PROF].

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

7.1.1 Version Number(s)

Certificates must be of type X.509 v3 (populate version field with integer "2").

7.1.2 Certificate Extensions

For all CAs, use of standard certificate extensions ~~shall~~must comply with [RFC ~~3280~~5280].

Certificates issued by the FBCA ~~shall~~must comply with ~~*Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile* [FPKI-Prof].~~[FBCA-PROF]. Certificates issued by Federal Entity CAs operating at High, Medium Hardware, and/or Medium Assurance ~~shall~~must comply with [~~FPKI~~FBCA-PROF].

Entity CAs that issue PIV-I Certificates ~~shall~~must comply with ~~[PIV-I Profile~~relevant worksheets from [FBCA-PROF].

~~Practice Note: For Entity CAs that issue PIV-I certificates, the associated CSS certificates will also comply with [PIV-I Profile].~~

~~Certificates issued by the FBCA shall~~

Practice Note: For Entity CAs that issue PIV-I certificates, the associated CSS certificates must also comply with [FBCA-PROF].

CA certificates must not include critical private extensions.

~~CA~~When used in Subscriber certificates ~~issued by Entity PKIs shall not include~~, critical private extensions~~. Subscriber certificates issued by Entity PKIs may include critical private extensions so long as interoperability within the~~ must be interoperable in their intended community of use ~~is not impaired~~.

Entity CA and Subscriber certificates may include any extensions as specified by [RFC 5280] in a certificate, but must include those extensions required by this CP. Any optional or additional extensions must not conflict with the applicable certificate and CRL profiles identified in Section 7.1

7.1.3 Algorithm Object Identifiers

Certificates issued by the FBCA and Entity CAs ~~shall~~must identify the signature algorithm using one of the following OIDs:

~~id-dsa-with-sha1~~Signature Algorithm	Object Identifier~~{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3 }~~
sha256WithRSAEncryption ~~sha-1WithRSAEncryption~~	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) ~~5 }~~11 } (1.2.840.113549.1.1.11)
sha384WithRSAEncryption ~~sha256WithRSAEncryption~~	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) ~~11 }~~12 } (1.2.840.113549.1.1.12)
~~id-RSASSA-PSS~~sha512WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) ~~10 }~~13 } (1.2.840.113549.1.1.13)
~~ecdsa-with-SHA1~~id-RSASSA-PSS	{ iso(1) member-body(2) us(840) ~~ansi-X9-62(10045) signatures(4)~~ rsadsi(113549) pkcs(1~~}~~) pkcs-1(1) 10 } (1.2.840.113549.1.1.10)
~~ecdsa-with-SHA224~~	~~{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1 }~~
ecdsa-with-SHA256	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2 } (1.2.840.10045.4.3.2)
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 } (1.2.840.10045.4.3.3)

ecdsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 } (1.2.840.10045.4.3.4)

~~Where certificates are signed using RSA with~~The PSS padding~~, the~~ scheme OID is independent of the hash algorithm~~;~~. The hash algorithm is specified as a parameter~~. RSA signatures with PSS padding may be used with the~~ (for details, see [PKCS#1]). The following are the approved hash algorithms ~~and OIDs specified below~~:

id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 } (2.16.840.1.101.3.4.2.1)
id-sha384	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 2 } (2.16.840.1.101.3.4.2.2)
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 } (2.16.840.1.101.3.4.2.3)

Certificates ~~issued by~~must use the ~~FBCA and Entity CAs shall~~following OIDs to identify the ~~cryptographic~~ algorithm associated with the subject ~~public~~ key ~~using one of the following OIDs~~:

~~id-dsa~~Public Key Algorithm	~~{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1 }~~Object Identifier
rsaEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 } (1.2.840.113549.1.1.1)
~~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 } (1.2.840.10045.2.1)

Where non-CA certificates issued on behalf of federal agencies contain an elliptic curve public key, the parameters ~~shall~~must be specified as one of the following named curves:

ansip192r1Curve	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 1 }Object Identifier
ansit163k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 1 }
ansit163r2	{ iso(1) identified-organization(3) certicom(132) curve(0) 15 }
ansip224r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 33 }
ansit233k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 26 }
ansit233r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 27 }
ansip256r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7 } (1.2.840.10045.3.1.7)
ansit283k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 16 }
ansit283r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 17 }
ansip384r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 } (1.3.132.0.34)
ansit409k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 36 }
ansit409r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 37 }
ansip521r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 35 }
ansit571k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 38 }
ansit571r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 39 }

For PIV-I, signature algorithms are limited to those identified by [NIST SP 800-78.].

7.1.4 Name Forms

Where required as set forth in Section 3.1.1, the subject and issuer fields of the base certificate shallmust be populated with an X.500 Distinguished Name. Distinguished names shallmust be composed of standard attribute types, such as those identified in [RFC3280[RFC 5280].

7.1.5 Name Constraints

All CA certificates issued by the FBCA at the Medium, Medium Hardware, or High Assurance levels shall have name constraints asserted that limit the name space of the PrincipalEntity CAs to that appropriate for their domains. Additionally, the FPKIPA may require that the FPKIMA include such

Entity CAs may assert name constraints ~~for the FBCA~~in CA certificates ~~issued at the Basic or Rudimentary levels if it deems appropriate~~.

~~For Entity CAs, no stipulation.~~

7.1.6 Certificate Policy Object Identifier

All certificates issued by the FBCA ~~or SHA1 Federal Root CA shall~~must include a certificate policies extension asserting one or more of the certificate policy OID(s) appropriate to the level of assurance with which it was issued. See Section 1.2 for specific OIDs.

An Entity ~~CAs that do~~must not ~~meet the SHA-2 requirements may~~ assert ~~a certificate policy OID that maps to the appropriate SHA-1 Federal Root CA SHA-1 OID for all~~ the FBCA CP OIDs in any certificates ~~generated using SHA-1 after December 31, 2010. When an~~ the Entity CA ~~subsequently meets~~issues, except in the ~~SHA-2 requirements, the Entity CA shall assert OIDs that can be differentiated from~~subject Domain field of the *policyMappings* extension of the ~~SHA-1~~certifies issued to FBCA establishing an equivalency between an FBCA OID and an OID in the Entity CA's CP.

Entity certificates must assert at least one certificate policy OID as specified in Section 1.2 of the Entity CP in the certificate policies extension.

Certificates issued for PIV-I card authentication or PIV-I content signing must not express any other policy OIDs ~~and map to the appropriate FBCA OID~~.

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

7.1.7 Usage of Policy Constraints Extension

The CAs may assert policy constraints in CA certificates. When this extension appears, at least one of r*equireExplicitPolicy* or *inhibitPolicyMapping* must be present. ~~When present, this extension should be marked as noncritical*, to support legacy applications that cannot process *policyConstraints*. For Subordinate CA certificates *inhibitPolicyMappings*, skip certs will be set to 0. For cross-certificates *inhibitPolicyMappings*, skip certs will be set to 1, or 2 for the Federal Bridge CA. When *requireExplicitPolicy* is included skip certs will be set to 0.~~ When present, this extension may be marked critical.

For Subordinate CA certificates *inhibitPolicyMapping*, skip certs must be set to 0. For cross-certificates *inhibitPolicyMapping*, skip certs must be set appropriately. When *requireExplicitPolicy* is included skip certs must be set to 0.

Practice Note: *inhibitPolicyMapping*, skip certs is usually set to 1 in a cross-certificate issued to a Bridge so it can do another cross-certificate mapping to its CA members. A skip certs value of 2 may be required to allow transitive trust if that Bridge issues a cross-certificate to a CA that also allows mapping, e.g., the Federal Common Policy CA also issues cross-

certificates with policy mapping. If transitive trust is not the desired behavior other constraints such as name constraints may be required to control appropriate results.

7.1.8 Policy Qualifiers Syntax ~~&~~and Semantics

Certificates issued by the FBCA ~~shall~~do not contain policy qualifiers. Certificates issued by Entity PKIs may contain policy qualifiers identified in [RFC ~~3280~~5280].

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

~~Not applicable; certificates issued by the FBCA do not include~~Certificates must contain a non-critical certificate policies extension.

7.1.10 Inhibit Any Policy Extension

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

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

7.2 CRL PROFILE

7.2.1 Version ~~Numbers~~Number(s)

~~The FBCA shall~~CAs must issue X.509 version two (2) CRLs.

~~Entity CAs operating at Basic, Medium, Medium Hardware, or High Assurance shall issue X.509 version 1 or version 2 CRLs.~~

7.2.2 CRL and CRL Entry Extensions

~~For~~Detailed CRL profiles addressing the ~~FBCA, CRL extensions shall conform to [FPKI~~use of each extension are specified in [FBCA-PROF].

7.3 OCSP PROFILE

If implemented, ~~Certificate Status Servers (~~CSS~~) shall~~ must sign responses using algorithms designated for CRL signing.

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

7.3.1 Version Number(s)

CSSs must use OCSP version 1.

7.3.2 OCSP Extensions

Critical OCSP extensions must not be used.

8. COMPLIANCE AUDIT &AND OTHER ASSESSMENTS

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

The FPKIMA shallmust have a compliance audit mechanism in place to ensure that the requirements of this CP and the FBCA CPS are being implemented and enforced.

Entity CAs must have a compliance audit mechanism in place to ensure that the requirements of their CP/CPS are being implemented and enforced. The Entity PKI PMA shall beis responsible for ensuring annual audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated.

Federal Agency PKIs must ensure they have appropriate authority to operate.

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

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

The FBCA,FPKIMA and Entity Principal CAs, CMSs, and RAs and their subordinate CAs, CMSs, and RAs shallPKIs must be subject to a periodicPKI compliance audit at least once per year for High, Medium Hardware, PIV-I Card Authentication, and Medium Assurance, and at least once every two years for Basic Assurance. The audit must include all CAs, as well as CSS, CMS & RAs, and supporting repositories. Where a status server is specified in certificates issued by a CA, the status server shallmust be subject to the same periodic compliance audit requirements as the corresponding CA. For example, if an OCSP server is specified in the authority information access extension in certificates issued by a CA, that server must be reviewed as part of that CA's compliance audit.

The compliance audit of CAs and RAs shallmust be carried out in accordance with the requirements as specified in the *FPKI Annual Review Requirements* document [AUDIT].

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

The FBCA and Entity Principal CAsPMAs have the right to require periodic and aperiodic compliance audits or inspections of subordinate CA or RA operations to validate that the subordinate entities are operating in accordance with the security practices and procedures described in their respective CPS. Further, the FPKIPA has the right to require aperiodic compliance audits of Entity Principal CAsPKIs (and, when needed, their subordinate CAs) that interoperate with the FBCA under this CP.. The FPKIPA shallmust state the reason for any aperiodic compliance audit.

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

8.2 IDENTITY ~~& /~~QUALIFICATIONS OF ASSESSOR

The auditor must demonstrate competence in the field of compliance audits. At the time of the audit, the ~~FBCA compliance auditor must be thoroughly familiar with requirements which the FPKIPA imposes on the issuance and management of FBCA certificates. Likewise, the Entity~~ CA compliance auditor must be thoroughly familiar with the requirements which ~~Entities impose~~the applicable CP imposes on the issuance and management of their certificates. The compliance auditor must perform such compliance audits as a regular ongoing business activity.

For the FBCA, in addition to the previous requirements, the auditor must 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 FPKIMA ~~shall~~must identify the compliance auditor for the FBCA.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

~~For both the FBCA and Entity CAs,~~ The compliance auditor either ~~shall~~must be a private firm, that is independent from the entity being audited, or it ~~shall~~must be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation. An example of the latter situation may be an Agency inspector general. To ~~insure~~ensure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's CA Facility or ~~certificate~~Certification Practices Statement.

The FPKIPA ~~shall~~may determine whether a compliance auditor meets this requirement.

8.4 TOPICS COVERED BY ASSESSMENT

~~The compliance audit of the FBCA shall verify that the FPKIMA is implementing all provisions of a CPS approved by the FPKIPA consistent with this CP. The audit shall also verify that the FPKIMA is implementing the relevant provisions of the MOAs between the FPKIPA and each Entity PKI.~~

The purpose of a compliance audit of ~~an Entity~~a PKI ~~shall~~must be to verify that ~~an entity subject to~~it is operating in accordance with a CPS that meets the requirements of ~~an Entity CP is complying with the requirements of those documents~~the applicable CP, as well as any MOAs between the ~~Entity~~ PKI and any other PKI. Components other than CAs may be audited fully or by using a representative sample.

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

A full compliance audit for the ~~FBCA or an Entity~~ PKI covers all aspects within the scope identified above.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

- The compliance auditor ~~shall~~must document the discrepancy and provide a copy to the FPKIMA;
- The FPKIMA will provide a copy of the discrepancy documentation to the FPKIPA Chair;
- The FPKIMA will report findings and corrective action to the FPKIPA;
- The FPKIMA ~~shall~~must determine what further notifications or actions are necessary to meet the requirements of this CP and the MOAs, and then proceed to make such notifications and take such actions without delay.
- Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the FPKIPA may direct the FPKIMA to take additional actions as appropriate, including temporarily halting operation of the FBCA.

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

- The compliance auditor ~~shall~~must document the discrepancy;
- The compliance auditor ~~shall~~must notify the responsible party promptly;
- The Entity PKI ~~shall~~must determine what further notifications or actions are necessary to meet the requirements of the Entity CP, CPS, and any relevant MOA provisions. The Entity PKI ~~shall~~must proceed to make such notifications and take such actions without delay.

When the FPKIPA receives a report of audit deficiency from an Entity PKI, the FPKIPA may direct the FPKIMA to take additional actions to protect the level of trust in the infrastructure.

8.6 COMMUNICATION OF RESULTS

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

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 ~~FBCA~~FPKI.

9.1.1 Certificate Issuance/Renewal Fees

~~No Stipulation.~~

CAs must make this determination.

9.1.2 Certificate Access Fees

~~No Stipulation.~~

Section 2 of this policy requires that CA certificates be publicly available. CAs must make this determination for access to subscriber certificates.

9.1.3 Revocation or Status Information Access Fee

~~No Stipulation.~~

CAs must not charge additional fees for revoking certificates or access to CRLs and OCSP status information.

9.1.4 Fees for other Services

~~No Stipulation.~~

CAs must make this determination.

9.1.5 Refund Policy

~~No Stipulation.~~

CAs must make this determination.

9.2 FINANCIAL RESPONSIBILITY

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

9.2.1 Insurance Coverage

~~No stipulation.~~

CAs must make this determination.

9.2.2 Other Assets

~~No stipulation.~~

CAs must make this determination.

9.2.3 Insurance/ or Warranty Coverage for End-Entities

~~No stipulation.~~

CAs must make this determination.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

~~FBCA~~CA information identified in Section 2 not requiring protection ~~shall~~must be made publicly available. Public access to organizational information must be determined by the respective organization. FPKIPA access to Entity information will be addressed in the MOA with that Entity. ~~Public access to Entity information shall be determined by the respective Entity.~~

9.3.1 Scope of Confidential Information

~~No stipulation.~~

CAs must make this determination.

9.3.2 Information not within the Scope of Confidential Information

~~No stipulation.~~

CAs must make this determination.

9.3.3 Responsibility to Protect Confidential Information

~~No stipulation.~~

Confidential business information provided to the FPKI is protected in accordance with the terms of the agreements entered into between the applicable entity and the FPKI.

Each entity PKI is responsible for maintaining the confidentiality of information clearly marked or labeled as confidential that is shared with it. The entity must treat such information with the same degree of care and security as it treats its own confidential information,

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

The FPKIMA ~~shall~~must conduct a Privacy ~~Impact~~Threshold Assessment~~. If deemed necessary,~~, and implement and maintain any required Privacy Impact Assessments and Privacy Plans in accordance with the ~~FPKIMA shall have a Privacy Plan to protect personally identifying information from unauthorized disclosure.~~requirements of the Privacy Act of 1974, as amended. The FPKIPA ~~shall~~must approve the Privacy Plan.

~~For~~ Entity CAs~~, no stipulation~~ must make this determination.

9.4.2 Information Treated as Private

~~The FBCA shall protect all subscriber personally identifying information from unauthorized disclosure. The FBCA shall also~~The FPKIMA must protect personally identifying information

for Entity personnel collected to support cross-certification and MOA requirements from unauthorized disclosure. The contents of the archives maintained by the FPKIMA ~~shall~~are not ~~be~~ released except as required by law.

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

9.4.3 Information not Deemed Private

Information included in ~~FBCA~~ certificates is not subject to protections outlined in Section 9.4.2~~.~~

~~For Entity CAs, certificates that contain the UUID in the subject alternative name extension shall~~, but may not be ~~distributed via publicly accessible repositories (e.g., LDAP, HTTP).~~ sold to a third party.

9.4.4 Responsibility to Protect Private Information

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

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

9.4.5 Notice and Consent to Use Private Information

The FPKIMA 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.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

The FPKIMA ~~shall~~does not disclose private information to any third party unless authorized by this Policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. Any request for release of information ~~shall~~must be processed according to [41 CFR 105-60.605~~.~~].

9.4.7 Other Information Disclosure Circumstances

None.

9.5 INTELLECTUAL PROPERTY RIGHTS

~~The FPKIMA will~~CAs must not knowingly violate intellectual property rights held by others.

9.6 REPRESENTATIONS &AND WARRANTIES

The obligations described below pertain to the FBCA (and, by implication, the FPKIMA), and to ~~Principal or other~~Entity CAs, which either interoperate with the FBCA or are in a trust chain up to a ~~Principal~~ CA that interoperates with the FBCA. The obligations applying to ~~Principal or other~~Entity CAs pertain to their activities as issuers of certificates. Further, the obligations focus on Entity CA obligations affecting interoperability with the FBCA. 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 FBCA, and whether the Entity is complying with the applicable MOA.

9.6.1 CA Representations and Warranties

FBCA certificates are issued and revoked at the sole discretion of the FPKIPA. When the FBCA issues a cross-certificate to a non-federal entity, it does so for the convenience of the U.S. 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 the FBCA policy.

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.

For PIV-I, Entity CAs ~~shall~~must maintain an agreement with Affiliated Organizations concerning the obligations pertaining to authorizing affiliation with Subscribers of PIV-I certificates.

9.6.2 RA Representations and Warranties

~~No stipulation.~~

An RA that performs registration functions must comply with the stipulations of the applicable policy.

9.6.3 Subscriber Representations and Warranties

For Medium, Medium Hardware, and High Assurance levels, a Subscriber ~~shall~~must be required to sign a document containing the requirements the Subscriber ~~shall~~must meet respecting protection of the private key and use of the certificate before being issued the certificate. For Basic Assurance level, the Subscriber ~~shall~~must be required to acknowledge his or her obligations respecting protection of the private key and use of the certificate before being issued the certificate.

Subscribers of Entity CAs at Basic, Medium, and High Assurance Levels ~~shall~~must agree to the following:

- Accurately represent themselves in all communications with the PKI authorities.
- Protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures.

- Promptly notify the appropriate CA upon suspicion of loss or compromise of their private keys. Such notification ~~shall~~must be made directly or indirectly through mechanisms consistent with the CA's CPS.
- Abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates.

9.6.4 Relying ~~Parties~~Party Representations and Warranties

~~None.~~

This CP does not specify the steps a relying party should take to determine whether to rely upon a certificate. The relying party decides, pursuant to its own policies, what steps to take.

9.6.5 Representations and Warranties of Affiliated Organizations

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

9.6.6 Representations and Warranties of Other Participants

None.

9.7 DISCLAIMERS OF WARRANTIES

The FPKIMA may not disclaim any responsibilities described in this CP.

9.8 LIMITATIONS OF LIABILITY

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

For Entity CAs, no stipulation.

9.9 INDEMNITIES

No stipulation.

9.10 TERM ~~&~~AND TERMINATION

Entity CAs must describe their term and termination requirements as illustrated below.

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 INDIVIDUAL NOTICES ~~&~~AND COMMUNICATIONS WITH PARTICIPANTS

The ~~Federal PKI PA shall~~FPKIPA must establish appropriate procedures for communications with Entity CAs via contracts or memoranda of agreement as applicable.

For Entity CAs, any planned change to the infrastructure that has the potential to affect the FPKI operational environment ~~shall~~must be communicated to the FPKIPA at least two weeks prior to implementation~~, and~~. All new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change must be provided to the FPKIPA within 24 hours following implementation.

For all other communications, no stipulation.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The FPKIPA ~~shall~~must review this CP at least once every year. Corrections, updates, or suggested changes to this CP ~~shall~~must be communicated to every Entity ~~Principal~~ CA. Such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.2 Notification Mechanism and Period

Proposed changes to this CP ~~shall~~must be distributed electronically to FPKIPA members and observers in accordance with the FPKIPA Charter ~~and By-laws~~.

9.12.3 Circumstances under which OID must be Changed

OIDs will be changed if the FPKIPA determines that a change in the CP reduces the level of assurance provided.

9.13 DISPUTE RESOLUTION PROVISIONS

Any dispute arising with respect to this policy or certificates issued under this policy shall be resolved by the Parties.

9.14 GOVERNING LAW

The construction, validity, performance, and effect of certificates issued under this CP for all purposes ~~shall~~must be governed by United States Federal law (statute, case law or regulation).

For Entity CAs, the construction, validity, performance, and effect of certificates issued under the Entity CP for all purposes ~~shall~~must be governed by law (statute, case law or regulation) under which the Entity operates.

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

9.15 COMPLIANCE WITH APPLICABLE LAW

The FBCA and Entity CAs are required to comply with applicable law.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

~~No stipulation.~~

CAs must make this determination.

9.16.2 Assignment

~~No stipulation.~~

CAs must make this determination.

9.16.3 Severability

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

9.16.4 Enforcement (~~Attorney~~Attorneys' Fees~~/~~ and Waiver of Rights)

~~No stipulation.~~

CAs must make this determination.

9.16.5 Force Majeure

~~No stipulation.~~

CAs must make this determination.

9.17 OTHER PROVISIONS

CAs must make this determination.

APPENDIX A: PIV-INTEROPERABLE SMART CARD DEFINITION

The intent of PIV-I is to enable issuers to issue cards that are technically interoperable with Federal PIV Card readers and applications, and that may be trusted for particular purposes through a decision of the relying Federal Agency. Thus, reliance on PIV-I Cards requires compliance with technical specifications and specific trust elements. This appendix defines the specific requirements of a PIV-I Card. It relies heavily on relevant specifications from the National Institute of Standards and Technology (NIST).

The following requirements must apply to PIV-I Cards:

1. To ensure interoperability with Federal systems, PIV-I Cards must use a smart card platform that is on GSA's FIPS 201 Evaluation Program Approved Product List (APL) and uses the PIV application identifier (AID).

2. PIV-I Cards must conform to [NIST SP 800-73-4[4]].

3. Only PIV-I Authentication certificates may assert a policy OID cross certified with the PIV-I Hardware policy OID and must conform to the [FBCA-PROF].

4. Digital signature certificates on a PIV-I credential should assert a policy mapped to mediumHardware, and key management certificates on a PIV-I credential should assert a policy mapped to either mediumAssurance or mediumHardware.

5. PIV-I Cards must contain an asymmetric X.509 Certificate for Card Authentication that:

    a. conforms to [FBCA-PROF];

    b. conforms to [NIST SP 800-73-4]; and

    c. is issued under the PIV-I Card Authentication policy.

6. PIV-I Cards must contain an electronic representation (as specified in SP 800-73 and SP 800-76) of the Cardholder Facial Image printed on the card.

7. The X.509 Certificates for Digital Signature and Key Management described in [NIST SP 800-73] are optional for PIV-I Cards.

8. Visual distinction of a PIV-I Card from that of a Federal PIV Card must ensure no suggestion of attempting to create a fraudulent Federal PIV Card. Examples of allowable visual distinction includes (but is not limited to):

[4] Special attention should be paid to UUID requirements for PIV-I.

a. Printing a phrase such as PIV-Interoperable, [Company Credential],[Organization], Local Access Only, or some other phrase that makes it clear this is not a PIV on the front of the card

b. Printing the card horizontal rather than in portrait mode,

c. Using a colored background

For non-Federally issued PIV-I, images or logos on a PIV-I Card must not be placed entirely within Zone 11F, *Agency Seal*, as defined by [FIPS 201].

9. The PIV-I Card physical topography must include, at a minimum, the following items on the front of the card:

   a. Cardholder facial image;
   b. Cardholder full name;
   c. Organizational Affiliation, if exists; otherwise, the issuer of the card; and
   d. Card expiration date.

10. PIV-I Cards must have an expiration date not to exceed 6 years of issuance.

11. Expiration of the PIV-I Card should not be later than expiration of PIV-I Content Signing certificate on the card.

12. The digital signature certificate that is used to sign objects on the PIV-I Card (e.g., CHUID, Security Object) must contain a policy OID that has been mapped to the FBCA PIV-I Content Signing policy OID. The PIV-I Content Signing certificate must conform to [FBCA-PROF].

13. The PIV-I Content Signing certificate and corresponding private key must be managed within a trusted Card Management System as defined by Appendix B.

14. At issuance, the RA must activate and release the PIV-I Card to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.1.

15. PIV-I Cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or update, the card management system must perform a challenge response protocol using cryptographic keys stored on the card in accordance with [NIST SP 800-73-4]. When cards are personalized, card management keys must be set to be specific to each PIV-I Card. That is, each PIV-I Card must contain a unique card management key. Card management keys must meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [NIST SP 800-78-4]

APPENDIX B: CARD MANAGEMENT SYSTEM REQUIREMENTS

PIV-I Cards are issued and managed through information systems called Card Management Systems (CMSs). The complexity and use of these trusted systems may vary. Nevertheless, Entity CAs have a responsibility to ensure a certain level of security from the CMSs that manage the token on which their certificates reside, and to which they issue certificates for the purpose of signing PIV-I Cards. This appendix provides additional requirements to those found above that apply to CMSs that are trusted under this Certificate Policy.

The Card Management Master Key must be maintained in a FIPS 140-2 Level 2 Cryptographic Module and conform to [NIST SP 800-78-4] requirements. Diversification operations must also occur on the Hardware Security Module (HSM). Use of these keys requires PIV-I Hardware or commensurate. Activation of the Card Management Master Key must require strong authentication of Trusted Roles. Card management must be configured such that only the authorized CMS can manage issued cards.

The PIV-I identity proofing, registration and issuance process must adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV-I credential without the cooperation of another authorized person.

Individual personnel must be specifically designated to the four Trusted Roles defined in Section 5.2.1. Trusted Role eligibility and Rules for separation of duties follow the requirements for Medium assurance in Section 5.

All personnel who perform duties with respect to the operation of the CMS must receive comprehensive training. Any significant change to CMS operations must have a training (awareness) plan, and the execution of such plan must be documented.

Audit log files must be generated for all events relating to the security of the CMS must be treated the same as those generated by the CA (see Sections 5.4 and 5.5).

A formal configuration management methodology must be used for installation and ongoing maintenance of the CMS. Any modifications and upgrades to the CMS must be documented and controlled. There must be a mechanism for detecting unauthorized modification to the CMS.

The CMS must have document incident handling procedures that are approved by the head of the organization responsible for operating the CMS. If the CMS is compromised, all certificates issued to the CMS must be revoked, if applicable. The damage caused by the CMS compromise must be assessed and all Subscriber certificates that may have been compromised must be revoked, and Subscribers must be notified of such revocation. The CMS must be re-established.

All Trusted Roles who operate a CMS must be allowed access only when authenticated using a method commensurate with PIV-I Hardware.

The computer security functions listed below are required for the CMS:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see Section 5.4)
- enforce domain integrity boundaries for security critical processes; and

support recovery from key or system failure.~~No stipulation.~~

10. BIBLIOGRAPHY

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

ABADSG	Digital Signature Guidelines, 1996-08-01. http://itlaw.wikia.com/wiki/American_Bar_Association_(ABA)_Digital_Signature_Guidelines
AUDIT	FPKI Annual Review Requirements
CIMC	Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001.
FIPS 140-2	Security Requirements for Cryptographic Modules May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 186-2	Digital Signature Standard, January 27, 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf
FIPS 201	Personal Identity Verification (PIV) of Federal Employees and Contractors http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf
FOIACT	5 U.S.C. 552, Freedom of Information Act. http://www4.law.cornell.edu/uscode/5/552.html
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E-X.509 Certificate and CRL Extensions Profile, 7 July 1997 http://csrs.nist.gov/pki/FPKI7-10.DOC
FPKI-Prof	Federal PKI X.509 Certificate and CRL Extensions Profile
ISO9594-8	Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997.
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996. http://www4.law.cornell.edu/uscode/40/1452.html
NAG69C	Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.
NIST SP 800-63-3	Digital Identity Guidelines https://csrc.nist.gov/publications/detail/sp/800-63/3/final
NIST SP 800-73	Interfaces for Personal Identity Verification (4 Parts) http://csrc.nist.gov/publications/PubsSPs.html

~~NIST SP 800-76~~	~~Biometric Data Specification for Personal Identity Verification http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf~~

NIST SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV) http://csrc.nist.gov/publications/nistpubs/800-78-2/sp800-78-2.pdf
NSD42	National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)
NS4005	NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.
NS4009	NSTISSI 4009, National Information Systems Security Glossary, January 1999.
PIV-I Profile	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, Date: April 23 2010, Reference Link: http://www.idmanagement.gov/fpki-documents
PKCS#12	Personal Information Exchange Syntax Standard, April 1997. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf
RFC 2510	Certificate Management Protocol, Adams and Farrell, March 1999.
RFC 3647	Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003.

~~11. ACRONYMS & ABBREVIATIONS~~

-

APPENDIX C: IN-PERSON ANTECEDENT

This Appendix describes the baseline requirements for an in-person antecedent identity proofing event. An Antecedent event is an in-person proofing event that occurred previously and may suffice as meeting the in-person identity proofing requirements for a new certificate. The requirement for antecedent is identical to in-person identity proofing in Section 3.2 with the exception of using an historical in-person ID proofing event, and reliance on an on-going relationship. Hence, a proposed antecedent process must

1. meet the thoroughness (rigor) of the in-person event,
2. provide supporting ID proofing artifacts or substantiate the applicant through an existing relationship, and
3. bind the individual to the asserted identity.

The Antecedent process may be appropriate when the applicant has no reasonable access to a Registration Authority or other Enrollment facility.

The Antecedent process requires that the applicant – an employee, member, or associate – has an on-going relationship with the Sponsor and that an equivalent in-person identity proofing event was conducted with the Sponsor on some previous date. The Sponsor must attest to the validity of the individual's claimed identity through this existing relationship and provide details concerning the antecedent identity proofing event, including the date of the event, unique applicant identity information and existing artifacts from the event, if any, to the RA.

The following outlines specific requirements for the antecedent identity proofing and credential issuance process.

1. Identity Proofing Relationships

   - The Sponsor of the applicant must have a contractual relationship with the Entity PKI.
   - The Sponsor must have an established relationship with the applicant. The relationship must be sufficient to enable the RA to, with a high degree of certainty, verify that the person seeking the PKI certificate is the same person that was identity proofed.
   - The Sponsor's application must contain a description of the relationship with the applicant describing the initial identity proofing or qualifications and the on-going relationship.

2. Antecedent in-person identity proofing event

   - The Applicant must have provided a National Government-issued Picture I.D., or two Non- National Government I.D.s, one of which was a photo I.D. (e.g., Driver's License) during the antecedent identity proofing event. The identity of the entity providing confirmation of the antecedent identity proofing process must be captured in an auditable record.

3. Registration Authority (RA)

The RA must base its decision concerning the validity of the applicant's claimed identity on the information provided via the Antecedent identity proofing process and verification that the applicant is the same individual.

- The RA must record the date of the antecedent in-person identity proofing event as provided by the Sponsor.
- The RA must obtain the historical artifacts from the Antecedent event, if any.
- The RA must be able to verify the applicant matches the individual who participated in the Antecedent proofing process.

4. Information source requirements.

- The Antecedent process must ensure that all data received by the RA from the Sponsor is validated, protected, and securely exchanged.
- All participants must store and exchange private information in a confidential and tamper evident manner protected from unauthorized access.

5. Binding the certificate request to the identity.

The process to bind the claimed identity to the specific certificate request must provide commensurate levels of assurance with the certificate being issued.

- A Sponsor for the applicant must provide the Entity PKI with initial contact information, (e.g., name, email address, phone number, sponsoring organization).
- The PKI must use the Sponsor provided information to contact the applicant.

APPENDIX D: REFERENCES

ABADSG	American Bar Association Digital Signature Guidelines http://itlaw.wikia.com/wiki/American_Bar_Association_(ABA)_Digital_Signature_Guidelines
APL	GSA Approved Products List (APL) https://www.idmanagement.gov/buy/#products
AUDIT	FPKI Annual Review Requirements https://www.idmanagement.gov/docs/fpki-annual-review-requirements.pdf
BRIDGE PROCESS	Federal Public Key Infrastructure Bridge Application Process Overview https://www.idmanagement.gov/docs/fpki-bridge-app-process.pdf
COMMON	X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework https://www.idmanagement.gov/docs/fpki-x509-cert-policy-common.pdf
COMMON-PROF	Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles https://www.idmanagement.gov/docs/fpki-x509-cert-profile-common.pdf
Conformance Criteria	Conformance Criteria for NIST SP 800-63A Enrollment and Identity Proofing https://www.nist.gov/system/files/documents/2020/07/02/800-63A%20Conformance%20Criteria_0620.pdf
Executive Order 12968	Executive Order 12968 - Access to Classified Information https://www.govinfo.gov/content/pkg/FR-1995-08-07/pdf/95-19654.pdf
FBCA-PROF	Federal Bridge Certification Authority (FBCA) X.509 Certificate and CRL Extensions Profile https://www.idmanagement.gov/docs/fpki-x509-cert-profiles-fbca.pdf
FIPS 140	Security Requirements for Cryptographic Modules, FIPS 140-3. https://csrc.nist.gov/publications/detail/fips/140/3/final
FIPS 201	Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201 https://csrc.nist.gov/publications/detail/fips/201/3/final

ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996. https://govinfo.library.unt.edu/npr/library/misc/itref.html
PACS	*Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.3, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group https://www.idmanagement.gov/docs/pacs-tig-scepacs.pdf
PIV-I Issuers	Personal Identity Verification Interoperability for Issuers https://www.idmanagement.gov/docs/fpki-pivi-for-issuers.pdf
PKCS#1	Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications https://www.ietf.org/rfc/rfc3447.txt
PKCS#12	PKCS #12: Personal Information Exchange Syntax https://www.ietf.org/rfc/rfc7290.txt
RFC 2585	Internet X.509 Public Key Infrastructure: Operational Protocols: FTP and HTTP https://www.ietf.org/rfc/rfc2585.txt
RFC 3647	Certificate Policy and Certification Practices Framework https://www.ietf.org/rfc/rfc3647.txt
RFC 4122	A Universally Unique IDentifier (UUID) URN Namespace https://www.ietf.org/rfc/rfc4122.txt
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. https://www.ietf.org/rfc/rfc5280.txt
RFC 5322	Internet Message Format https://www.ietf.org/rfc/rfc5322.txt
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. https://www.ietf.org/rfc/rfc6960.txt
RFC 8551	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification https://www.ietf.org/rfc/rfc8551.txt
SP 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, NIST Special

	Publication 800-37 https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
SP 800-56A	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, NIST Special Publication 800-56A https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final
SP 800-57	Recommendation for Key Management: Part 1- General, NIST Special Publication 800-57 Part 1 https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final
SP 800-63	Digital Identity Guidelines https://csrc.nist.gov/publications/detail/sp/800-63/3/final
SP 800-73	Interfaces for Personal Identity Verification https://csrc.nist.gov/publications/detail/sp/800-73/4/final
SP 800-76	Biometric Specifications for Personal Identity Verification, NIST Special Publication 800-76 https://csrc.nist.gov/publications/detail/sp/800-76/2/final
SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification, NIST Special Publication 800-78 https://csrc.nist.gov/publications/detail/sp/800-78/4/final
SP 800-79	Guidelines for the Accreditation of Personal Identity Verification Card Issuers, NIST Special Publication 800-79 https://csrc.nist.gov/publications/detail/sp/800-79/2/final
SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications, NIST Special Publication 800-89 https://csrc.nist.gov/publications/detail/sp/800-89/final
SP 800-157	Guidelines for Derived Personal Identity Verification (PIV) Credentials, NIST Special Publication 800-157 https://csrc.nist.gov/publications/detail/sp/800-157/final
X.509	ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

APPENDIX E: ACRONYMS AND ABBREVIATIONS

AES	Advanced Encryption Standard
AIA	Authority Information Access
AID	Application Identifier
APL	Approved Products List
CA	Certification Authority
~~CARL~~	~~Certificate Authority Revocation List~~
CHUID	Cardholder Unique Identifier
CIO	Chief Information Officer
CISA	Certified Information System Auditor
CISO	Chief Information Security Officer
CMS	Card Management System
CN	Common Name
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
CSS	Certificate Status Server
DDS	Data Decryption Server
DN	Distinguished Name
DNS	Domain Name System

DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
~~ERC~~ ECC	~~Enhanced Reliability Check~~Elliptic Curve Cryptography

~~FAR~~	~~Federal Acquisition Regulations~~

FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standard
FPKIMA	Federal Public Key Infrastructure Management Authority

~~FED-STD~~	~~Federal Standard~~
~~FIPS PUB~~	~~(US) Federal Information Processing Standard Publication~~

FPKI	Federal Public Key Infrastructure

~~FPKI-E~~	~~Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile~~
~~FPKISC~~	~~Federal PKI Steering Committee~~

FPKIPA	Federal PKI Policy Authority
FPKIMA	Federal PKI Management Authority
~~GPEA~~ FTCA	~~Government Paperwork Elimination Act of 1998~~Federal Tort Claims Act
GSA	General Services Administration
HTTP	Hypertext Transfer Protocol
HSM	Hardware Security Module
~~IETF~~ IANA	Internet ~~Engineering Task Force~~Assigned Numbers Authority
IDMS	Identity Management System
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer

ITAR	International Traffic in Arms Regulation
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
~~ITU-TSS~~ KED	~~International Telecommunications Union – Telecommunications System Sector~~Key Escrow Database
KRA	Key Recovery Agent
KRO	Key Recovery Officer
KRP	Key Recovery Policy
KRPS	Key Recovery Practice Statement
LDAP	Lightweight Directory Access Protocol
MOA	Memorandum of Agreement ~~(as used in the context of this CP, between an Entity and the FPKIPA allowing interoperation between the FBCA and Entity Principal CA)~~
NACI	National Agency Check with Written Inquiries
NACLC	National Agency Check with Law Enforcement Check
NIST	National Institute of Standards and Technology
NSA	National Security Agency

~~NSTISSI~~ ~~National Security Telecommunications and Information Systems Security Instruction~~

OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PIV-I	Personal Identity Verification – Interoperable
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure

PKIX	Public Key Infrastructure X.509
POC	Point of Contact
RA	Registration Authority
RDN	Relative Distinguished Name
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1
~~S/MIME~~SIA	~~Secure Multipurpose Internet Mail Extension~~Subject Information Access
SP	Special Publication
TLD	Top Level Domain
~~SSL~~TLS	~~Secure Sockets~~Transport Layer Security

~~TSDM~~ ~~Trusted Software Development Methodology~~

UPN	User Principal Name
UPS	Uninterrupted Power Supply
URI	Universal Resource Identifier
URL	Uniform Resource Locator
U.S.C.	United States Code
UUID	Universally Unique Identifier (defined by RFC 4122)
~~VM~~VPN	Virtual ~~Machine~~Private Network

~~VME~~ ~~Virtual Machine Environment~~

WWW	World Wide Web

APPENDIX F: GLOSSARY

Access	Ability to make use of any information system (IS) resource. ~~[NS4009]~~
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. ~~[NS4009]~~
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. ~~[NS4009]~~
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Affiliated Organization	Organizations that authorize affiliation with Subscribers of PIV-I certificates.
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.~~A collection of documents created or gathered by the CA and selected for long-term preservation as evidence of their activities.
~~Attribute Authority~~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. ~~An entity, recognized by the FPKIPA or comparable Entity body as having the authority to verify the association of attributes to an identity.~~
Audit Log	A chronological record of information system activities, including records of system accesses and operations performed in a given period.~~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~~Record	~~Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]~~An individual entry in an audit log related to an audited event.
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. ~~[NS4009]~~
Backup	Copy of files and programs made to facilitate recovery if necessary. ~~[NS4009]~~
Binding	Process of associating two related elements of information. ~~[NS4009]~~
Biometric	A physical or behavioral characteristic of a 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 CP, the term "certificate" refers to X.509 certificates that expressly reference the OID of this CP in the ~~"Certificate Policies" field of an X.509 v.3 certificate~~certificatePolicies extension.
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.
~~Certificate~~	~~A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies it's Subscriber, (3) contains the Subscriber's public key, (4) identifies it's operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]~~

Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certification Authority Software	Key management and cryptographic software used to manage certificates issued to Subscribers.
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 this CP, or requirements specified in a contract for services).
Certificate-Related Information	Information, such as a Subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a certification authority of the certificates ~~which~~that it has issued that are revoked prior to their stated expiration date.
Certificate Status ~~Authority~~Server (CSS)	A trusted entity that provides on-line verification to a relying party of a subject certificate's ~~trustworthiness, and may also provide additional attribute information for the subject certificate~~revocation status.
Client (application)	A system entity, usually a computer process acting on behalf of a human user~~,~~ that makes use of a service provided by a server.
~~Common Criteria~~	~~A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.~~

Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. ~~[NS4009]~~
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 entities or processes. ~~[NS4009]~~
~~Cross-Certificate~~Containerization	~~A certificate used to establish a trust relationship between two Certification Authorities.~~A form of operating system virtualization, through which applications are run in isolated user spaces called containers, all using the same shared operating system (OS).
~~Cryptographic Module~~Cross-Certificate	A certificate used to establish a trust relationship between two certification authorities. ~~The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]~~
~~Cryptoperiod~~Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. ~~Time span during which each key setting remains in effect. [NS4009]~~ [FIPS 140]
Custodial Subscriber Key Stores	Custodial Subscriber Key Stores hold keys for a number of Subscriber certificates in one location.
Data Decryption Server	An automated system that obtains subscriber private keys from the Key Escrow Database or another Data Decryption Server in order to support decryption of data entering and leaving the Enterprise. An example of such data is e-mail.
Data Integrity	Assurance that the data are unchanged from creation to reception.
Device	A non-person entity, i.e., a piece of hardware or a software application

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.
~~Dual Use Certificate~~	~~A certificate that is intended for use with both digital signature and data encryption services.~~
~~Duration~~	~~A field within a certificate which is composed of two subfields; "date of issue" and "date of next issue".~~
~~E-commerce~~	~~The use of network technology (especially the internet) to buy or sell goods and services.~~
~~Encrypted Network~~	~~A network that is protected from outside access by NSA approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks.~~
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
~~End-entity~~	~~Relying Parties and Subscribers.~~
Entity	For the purposes of this document, "Entity" refers to an organization, corporation, community of interest, or government agency with operational control of a CA.
Entity CA	A CA that acts on behalf of an Entity, and is under the operational control of an Entity. The Entity may be an organization, corporation, or community of interest. For the Federal Government, an Entity may be any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Federal Government.
~~FBCA~~FPKI Management Authority (FPKIMA)	The Federal Public Key Infrastructure Management Authority is the organization ~~selected by the Federal Public Key Infrastructure Policy Authority to be~~ responsible for operating the Federal ~~Bridge~~ Common Policy Certification Authority.

Federal Public Key Infrastructure Policy Authority (FPKIPA)	The FPKIPA is a Federal Government body responsible for setting, implementing, and administering policy decisions regarding ~~inter Entity PKI interoperability that uses the FBCA.~~the Federal PKI Architecture.
Firewall	Gateway that limits access between networks in accordance with local security policy. ~~[NS4009]~~
~~High Assurance Guard (HAG)~~	~~An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.~~
Hypervisor	Computer software, firmware or hardware that creates and runs virtual machines. A hypervisor uses native execution to share and manage hardware, allowing for multiple environments which are isolated from one another, yet exist on the same physical machine. Also known as an isolation kernel or virtual machine monitor.
In-Person Antecedent	An Antecedent event is an in-person proofing event that occurred previously and may suffice as meeting the in-person identity proofing requirements.
Information ~~System~~Systems Security Officer (ISSO)	Person responsible to the Designated Approving Authority for ensuring the security of an information system throughout its ~~lifecycle~~life-cycle, from design through disposal. ~~[NS4009]~~
~~Inside threat~~	~~An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.~~
Integrity	Protection against unauthorized modification or destruction of information. ~~[NS4009].~~ 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.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.

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 Escrow Database (KED)	The function, system, or subsystem that maintains the key escrow repository and responds to key escrow and key recovery requests from one or more Key Recovery Agents, as specified by this policy.
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one (public) key can be used to encrypt a message that can only be decrypted using the other (private) key, and (~~i~~i2) even knowing ~~one~~the public key, it is computationally infeasible to discover the ~~other~~private key.
Key Recovery	Production of a copy of an escrowed key and delivery of that key to an authorized requestor.
Key Recovery Agent (KRA)	An individual authorized to interface with the key escrow database in conjunction with one or more other key recovery agents) to cause the key escrow database to carry out key recovery requests, as specified by this policy.
Key Recovery Official (KRO)	An individual authorized to authenticate and submit key recovery requests to the Key Recovery Agent on behalf of requestor, as specified by this policy.
Key Recovery Policy (KRP)	A key recovery policy is a specialized form of administrative policy tuned to the protection and recovery of key management private keys (i.e~~.~~., decryption keys) held in escrow. A key recovery policy addresses all aspects associated with the storage and recovery of key management certificates.

Key Recovery Practices Statement (KRPS)	A statement of the practices that a Key Recovery System employs in protecting and recovering key management private keys, in accordance with specific requirements (i.e., requirements specified in the KRP).
~~Local Registration Authority (LRA)~~	~~A Registration Authority with responsibility for a local community.~~
Memorandum of Agreement (MOA)	Agreement between the FPKIPA and an Entity allowing interoperability between the Entity ~~Principal~~ CA and the FBCA.
~~Mission Support Information~~Modification (of a certificate)	~~Information that is important to the support of deployed and contingency forces.~~The act or process by which data items bound in an existing public key certificate are changed by issuing a new certificate.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
National Security System~~Naming Authority~~	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]~~An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.~~

Network Guard~~National Security System~~	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.~~Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]~~
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. ~~[NS4009]~~ 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~~, OIDS are used to uniquely identify ~~each of the seven~~certificate policies and cryptographic algorithms ~~supported~~.
Offline CA~~Out-of-Band~~	An offline certification authority is a certification authority isolated from network access, and is often kept in a powered-down state.~~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).~~

Out-of-BandOutside Threat	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 An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.on-line).
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI Sponsor	Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.
Policy Management Authority (PMA)	The individual or group that is responsible for the creation and maintenance of Certificate Policies and Certification Practice Statements, and for ensuring that all Entity PKI components (e.g., CAs, CSSs, CMSsCard Management Systems, RAs) are audited and operated in compliance with the entity PKI CP. The PMA evaluates non-domain policies for acceptance within the domain, and generally oversees and manages the PKI certificate policies. For the FBCACommon Policy, the PMA is the FPKIPA.
Principal CA	The Principal CA is a CA designated by an Entity to interoperate with the FBCA. An Entity may designate multiple Principal CAs to interoperate with the FBCA.
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 normally 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~~that contains 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~~system containing ~~information and~~ data relating to certificates or revocation data as specified in this CP~~; may also be referred~~. May refer to ~~as~~ a directory, web server, or server which only hosts pre-generated OCSP responses.
~~Responsible Individual~~	~~A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.~~
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.
~~Risk Tolerance~~	~~The level of risk an entity is willing to assume in order to achieve a potential desired result.~~
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Structural Container	An organizational unit attribute included in a distinguished name solely to support local directory requirements, such as differentiation between Human Subscribers and devices.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
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, an application or network device.
Superior CA	In a hierarchical PKI, a CA ~~who~~that has certified the certificate signature key of another CA, and ~~who~~that constrains the activities of that CA. (See subordinate CA).
Supervised Remote Identity Proofing	~~A real-time identity proofing event where the RA/Trusted Agent is not in the same physical location as the applicant/subscriber. The RA/Trusted Agent controls a device which is utilized by the applicant/subscriber in order to ensure the~~A remote identity proofing process that employs physical, technical and procedural measures ~~to~~that provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person identity proofing process. Supervised Remote Identity Proofing must meet the criteria specified in NIST SP 800-63A Section 5.3.3 and the related [Conformance Criteria] for NIST SP 800-63A Enrollment and Identity Proofing; and must have the capacity to capture an approved biometric ~~when utilized for PIV-I credential issuance~~.
System ~~Equipment Configuration~~Software Layer	~~A comprehensive accounting of all system hardware and software types and settings.~~A layer of software that manages lower layer hardware and software resources and provides services through well-defined interfaces to the higher layers of software. Examples of system software layers are virtual machines, hypervisors, operating systems, and any containerized architectures.
~~System High~~	~~The highest security level supported by an information system. [NS4009]~~
~~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 cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. ~~[NS4009]~~
Trust List	Collection of Trusted Certificates used by relying parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of ~~an Entity~~a CA in confirming Subscriber identification during the registration process. Trusted agents do not have automated interfaces with certification authorities.
Trusted Certificate	A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".
~~Trusted Timestamp~~	~~A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.~~
~~Trustworthy System~~	~~Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.~~
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. ~~[NS4009]~~
~~Update (a certificate)~~	~~The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.~~
~~Virtual Machine Environment~~	~~An emulation of a computer system (in this case, a CA) that provides the functionality of a physical machine in a platform-independent environment. It consists of a host (virtual machine) and isolation kernel (hypervisor) and provides functionality needed to execute entire operating systems. At this time, allowed VMEs are limited to Hypervisor type virtual environments. Other technology, such as Docker Containers, is not permitted.~~

Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. ~~[FIPS1401~~ [FIPS 140]

~~12. ACKNOWLEDGEMENTS~~

~~The Certificate Policy Working Group developed this CP based on RFC 3647 and the original FBCA Certificate Policy.~~

~~APPENDIX A – PIV-INTEROPERABLE SMART CARD DEFINITION~~

~~The intent of PIV-I is to enable issuers to issue cards that are technically interoperable with Federal PIV Card readers and applications, and that may be trusted for particular purposes through a decision of the relying Federal Agency. Thus, reliance on PIV-I Cards requires compliance with technical specifications and specific trust elements. This appendix defines the specific requirements of a PIV-I Card. It relies heavily on relevant specifications from the National Institute of Standards and Technology (NIST).~~

~~The following requirements shall apply to PIV-I Cards:~~

1. ~~To ensure interoperability with Federal systems, PIV-I Cards shall use a smart card platform that is on GSA's FIPS 201 Evaluation Program Approved Product List (APL) and uses the PIV application identifier (AID).~~
2. ~~PIV-I Cards shall conform to [NIST SP 800-73[5]].~~
3. ~~The mandatory X.509 Certificate for Authentication shall be issued under a policy that is cross certified with the FBCA PIV-I Hardware policy OID.~~
4. ~~All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile].~~
5. ~~PIV-I Cards shall contain an asymmetric X.509 Certificate for Card Authentication that:~~
   - ~~a. conforms to [PIV-I Profile];~~
   - ~~b. conforms to [NIST SP 800-73]; and~~
   - ~~c.a. is issued under the PIV-I Card Authentication policy.~~
6. ~~PIV-I Cards shall contain an electronic representation (as specified in SP 800-73 and SP 800-76) of the Cardholder Facial Image printed on the card.~~
7. ~~The X.509 Certificates for Digital Signature and Key Management described in [NIST SP 800-73] are optional for PIV-I Cards.~~
8. ~~Visual distinction of a PIV-I Card from that of a Federal PIV Card is required to ensure no suggestion of attempting to create a fraudulent Federal PIV Card. Examples of allowable visual distinction includes (but are not limited to):~~
   - ~~a. Printing a phrase such as PIV-Interoperable, [Company credential], [Organization] Local Access Only, or some other phrase that makes it clear this is not a PIV on the front of the card~~
   - ~~b.a. Printing the card horizontal rather than in portrait mode,~~
   - ~~Using a colored background~~

[5] Special attention should be paid to UUID requirements for PIV-I.

For non-Federally issued PIV-I, images or logos on a PIV-I Card shall not be placed entirely within Zone 11F, *Agency Seal*, as defined by [FIPS 201].

9.1. The PIV-I Card physical topography shall include, at a minimum, the following items on the front of the card:

a. Cardholder facial image;

b.a. Cardholder full name;

c. Organizational Affiliation, if exists; otherwise the issuer of the card; and

d. Card expiration date.

10.1. PIV-I Cards shall have an expiration date not to exceed 6 years of issuance.

11.1. Expiration of the PIV-I Card should not be later than expiration of PIV-I Content Signing certificate on the card.

12. The digital signature certificate that is used to sign objects on the PIV-I Card (e.g., CHUID, Security Object) shall contain a policy OID that has been mapped to the FBCA PIV-I Content Signing policy OID. The PIV-I Content Signing certificate shall conform to [PIV-I Profile].

13. The PIV-I Content Signing certificate and corresponding private key shall be managed within a trusted Card Management System as defined by Appendix B.

14. At issuance, the RA shall activate and release the PIV-I Card to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.1.

15.1. PIV-I Cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or update, the card management system shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73]. When cards are personalized, card management keys shall be set to be specific to each PIV-I Card. That is, each PIV-I Card shall contain a unique card management key. Card management keys shall meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [SP800-78]

APPENDIX B – CARD MANAGEMENT SYSTEM REQUIREMENTS

PIV-I Cards are issued and managed through information systems called Card Management Systems (CMSs). The complexity and use of these trusted systems may vary. Nevertheless, Entity CAs have a responsibility to ensure a certain level of security from the CMSs that manage the token on which their certificates reside, and to which they issue certificates for the purpose of signing PIV-I Cards. This appendix provides additional requirements to those found above that apply to CMSs that are trusted under this Certificate Policy.

The Card Management Master Key shall be maintained in a FIPS 140-2 Level 2 Cryptographic Module and conform to [NIST SP 800-78] requirements. Diversification operations shall also occur on the Hardware Security Module (HSM). Use of these keys requires PIV-I Hardware or commensurate. Activation of the Card Management Master Key shall require strong authentication of Trusted Roles. Card management shall be configured such that only the authorized CMS can manage issued cards.

The PIV-I identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV-I credential without the cooperation of another authorized person.

Individual personnel shall be specifically designated to the four Trusted Roles defined in Section 5.2.1. Trusted Role eligibility and Rules for separation of duties follow the requirements for Medium assurance in Section 5.

All personnel who perform duties with respect to the operation of the CMS shall receive comprehensive training. Any significant change to CMS operations shall have a training (awareness) plan, and the execution of such plan shall be documented.

Audit log files shall be generated for all events relating to the security of the CMS shall be treated the same as those generated by the CA (see Sections 5.4 and 5.5).

A formal configuration management methodology shall be used for installation and ongoing maintenance of the CMS. Any modifications and upgrades to the CMS shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the CMS.

The CMS shall have document incident handling procedures that are approved by the head of the organization responsible for operating the CMS. If the CMS is compromised, all certificates issued to the CMS shall be revoked, if applicable. The damage caused by the CMS compromise shall be assessed and all Subscriber certificates that may have been compromised shall be revoked, and Subscribers shall be notified of such revocation. The CMS shall be re-established.

All Trusted Roles who operate a CMS shall be allowed access only when authenticated using a method commensurate with PIV-I Hardware.

The computer security functions listed below are required for the CMS:

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

- ~~manage privileges of users to limit users to their assigned roles;~~
- ~~generate and archive audit records for all transactions; (see Section 5.4)~~
- ~~enforce domain integrity boundaries for security-critical processes; and~~

~~support recovery from key or system failure.~~