X.509 Certificate Policy

For The

Federal Bridge Certification Authority (FBCA)

Version 2.1

January 12, 2006

Signature Page

_____   _____

Chair, Federal Public Key Infrastructure Policy Authority   DATE

Revision History

Document Version	Document Date	Revision Details
2.1	12 January 2006	This FBCA CP updates and replaces Version 2.0, dated 13 September 2005. Text changes are specified in the following FBCA CP Change Proposals (**change proposal number**, title, date): **2005-03**, Changes to the FBCA CP to modify audit cycle for consistency with Government certification and accreditation process, 13 December 2005

Table of Contents

1. INTRODUCTION

This Certificate Policy (CP) defines seven certificate policies for use by the Federal Bridge Certification Authority (FBCA) to facilitate interoperability between the FBCA and other Entity PKI domains. The policies represent five different assurance levels (Rudimentary, Basic, Medium, Medium Hardware, and High) for public key certificates. The level of assurance refers to the strength of the binding between the public key and the individual whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.

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 the purview of the Federal PKI Policy Authority 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.

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 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   Certificate Policy (CP)

FBCA certificates contain a registered certificate policy object identifier (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The OID corresponds to a specific level of assurance 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 & the FBCA CPS

The FBCA CP states what assurance can be placed in a certificate issued by the FBCA. The FBCA Certification Practices Statement (CPS) states how the FBCA establishes that assurance.

1.1.3 Relationship between the FBCA CP and the Entity CP

The FPKI Policy Authority maps Entity CP(s) to the five levels of assurance in the FBCA CP. The relationship between these CPs and the FBCA is asserted in CA certificates issued by the FBCA in the *policyMappings* extension.

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 non-Federal entities only when it is beneficial to the Federal Government.

1.2 DOCUMENT IDENTIFICATION

There are seven policies specified at five levels of assurance in this Certificate Policy, which are defined in subsequent sections. Each level of assurance has an Object Identifier (OID), to be asserted in certificates issued by the FBCA. Entity Principal CAs may assert these OIDs in policyMappings extensions of certificates issued to the FBCA. The FBCA policy OIDs are registered in the NIST Computer Security Objects Registry as follows:

fbca-policies OBJECT IDENTIFIER	::= { csor-certpolicy 3 }
csor-certpolicy OBJECT IDENTIFIER	::= { 2 16 840 1 101 3 2 1 }
id-fpki-certpcy-rudimentaryAssurance	::= { fbca-policies 1 }
id-fpki-certpcy-basicAssurance	::= { fbca-policies 2 }
id-fpki-certpcy-mediumAssurance	::= { fbca-policies 3 }
id-fpki-certpcy-mediumHardware	::= { fbca-policies 12 }
id-fpki-certpcy-medium-CBP	::={ fbca-policies 14 }
id-fpki-certpcy-mediumHW-CBP	::={ fbca-policies 15 }
id-fpki-certpcy-highAssurance	::= { fbca-policies 4 }

The High Assurance policy is reserved for government (federal, state, and local) use.

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

The requirements associated with the Medium Hardware policy are identical to those defined for the Medium Assurance policy, with the exception of subscriber cryptographic module requirements (see Section 6.2.1).

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

1.3   PKI ENTITIES
The following are roles relevant to the administration and operation of the FBCA.

1.3.1   PKI Authorities

1.3.1.1 Federal Chief Information Officers Council
The Federal CIO Council comprises the Chief Information Officers of all cabinet level departments and other independent agencies. The Federal CIO Council has established the framework for the interoperable 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 PKI Policy Authority (FPKIPA) is a group of U.S. Federal Government Agencies (including cabinet-level Departments) chartered by the Federal CIO Council. The FPKIPA owns this policy and represents the interest of the Federal CIOs. The FPKIPA is responsible for:

- The FBCA CP,

- The FBCA CPS,

- Accepting applications from Entities desiring to interoperate using the FBCA,

- Determining the mappings between certificates issued by applicant Entity CAs and the levels of assurance set forth 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 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 certificate levels of assurance 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 Operational Authority (FPKI OA)

The FPKI Operational Authority is the organization that operates and maintains the FBCA on behalf of the U.S. Government, subject to the direction of the FPKIPA.

1.3.1.4 FPKI Operational Authority Program Manager

The Program Manager is the individual within the FPKI Operational Authority who has principal responsibility for overseeing the proper operation of the FBCA including the FBCA repository, and selecting the FPKI Operational Authority Staff. The Program Manager is selected by the FPKI Operational Authority and reports to the FPKIPA. The FPKI Operational Authority Program Manager must hold a Top Secret security clearance.

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.

1.3.1.6 Federal Bridge Certification Authority (FBCA)

The FBCA is the entity operated by the FPKI Operational Authority that is authorized by the Federal PKI Policy Authority to create, sign, and issue public key certificates to Principal CAs. As operated by the FPKI Operational Authority, 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.

1.3.2   Registration Authority (RA)

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

1.3.3   Subscribers

A Subscriber is the user or device to whom or to which a certificate is issued. FBCA Subscribers include only FPKI Operational Authority personnel and, when determined by the Federal PKI Policy Authority, network or hardware devices. Note that CAs are sometimes technically considered "subscribers" in a PKI. However, the term "Subscriber" as used in this document does not refer to CAs.

1.3.4   Relying Parties

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

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

1.3.5   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.

1.4   CERTIFICATE USAGE

1.4.1   Appropriate Certificate Uses

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 five increasing, qualitative levels of assurance: Rudimentary, Basic, Medium, 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. 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 appropriate uses for 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.
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..
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 Federal Information Processing Standards, NIST Special Publications and electronic record retention guidance provided by the National Archives and Records Administration).

1.4.2   Prohibited Certificate Uses

No stipulation.

1.5 POLICY ADMINISTRATION

1.5.1   Organization administering the document

The Federal PKI Policy Authority is responsible for all aspects of this CP.

1.5.2   Contact Person

Questions regarding this CP shall be directed to the Chair of the Federal PKI Policy Authority, whose address can be found at http://www.cio.gov/fpkipa.

1.5.3   Person Determining Certification Practices Statement Suitability for the Policy

The Certification Practices Statement must conform to the corresponding Certificate Policy. The Federal PKI Policy Authority is responsible for asserting whether the FBCA CPS conforms to the FBCA 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 be based on an independent compliance auditor's results and recommendations. See Section 8 for further details.

1.5.4   CPS Approval Procedures

The FPKI Operational Authority shall submit the FBCA CPS and the results of a compliance analysis study to the FPKI PA for approval. The FPKI PA shall vote to accept or reject the CPS and accompanying analysis. If rejected, the FPKI Operational Authority shall resolve the identified discrepancies and resubmit to the FPKI PA.

1.6 DEFINITIONS AND ACRONYMS

See Sections 11 and 12.

2. PUBLICATION & REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The FPKI Operational Authority 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 FPKI Operational Authority 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 also accessible through the Lightweight Directory Access Protocol,

- Availability of the information as required by the certificate information posting and retrieval stipulations of this CP, and

- Access control mechanisms when needed to protect repository information as described in later sections.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 Publication of Certificates and Certificate Status

The FPKI Operational Authority shall publish all CA certificates issued by or to the FBCA and all CRLs issued by the FBCA in the FBCA repository.

At a minimum, the Entity repositories shall contain all CA certificates issued by or to the Entity PKI and CRLs issued by the Entity PKI.

2.2.2 Publication of CA Information

The FPKI Operational Authority shall publish information concerning the FBCA necessary to support its use and operation. The FBCA CP shall be publicly available on the FPKI PA website (see http://www.cio.gov/fpkipa). The FBCA CPS will not be published; a redacted version of the CPS will be publicly available from the FPKI PA website (see http://www.cio.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 FPKI Operational Authority; for more information see the FBCA website (see http://www.cio.gov/fbca).

2.3   FREQUENCY OF PUBLICATION

This CP and any subsequent changes shall be made publicly available within one week of approval.

2.4   ACCESS CONTROLS ON REPOSITORIES

The FPKI Operational Authority shall protect any repository information not intended for public dissemination or modification. Certificates and certificate status information in the FBCA repository shall be publicly available through the Internet.

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.

3. IDENTIFICATION & AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

The FBCA shall only generate and sign certificates that 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 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 the naming requirements that apply to each level of assurance.

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
High	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical

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.

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.

3.1.3 Anonymity or Pseudonymity of Subscribers

The FBCA shall 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 certificates issued by Entity CAs may contain a pseudonym (such as a large number) as long as name space uniqueness requirements are met.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation for the FBCA.

Entity CAs must specify 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.)

3.1.5 Uniqueness of Names

Name uniqueness must be enforced by the FBCA and Entity CAs.

The Federal PKI Policy Authority is responsible for ensuring name uniqueness in certificates issued by the FBCA.

> Practice Note: The FBCA considers it good practice for entities to include the following information in the Entity's CPS:
> - What name forms shall be used, and
> - How they will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (e.g., if "Joe Smith" leaves a CA's community of Subscribers, and a new, different "Joe Smith" enters the community of Subscribers, how will these two people be provided unique names?).

3.1.6 Recognition, Authentication, & Role of Trademarks

The FPKIPA shall resolve 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.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

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

In the case where a key is generated by 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 proof of possession is not required.

3.2.2 Authentication of Organization Identity

Requests for FBCA or Entity CA certificates in the name of an organization shall include the organization name, address, and documentation of the existence of the organization. The FPKI Operational Authority or Entity RA shall 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.

3.2.3 Authentication of Individual Identity

3.2.3.1 Authentication of Human Subscribers

For Subscribers, the FPKI Operational Authority or Entity CA, and/or associated RAs shall 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 upon the certificate level of assurance and shall be addressed in the FBCA or Entity CPS. The documentation and authentication requirements shall vary depending upon the level of assurance.

The FPKI Operational Authority, Entity CAs and/or RAs shall record the information set forth below for issuance of each certificate:

- The identity of the person performing the identification;

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

- If in-person identity proofing is done, a unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);

- The date of the verification; and

- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

For All Levels: If an applicant is unable to perform face-to-face 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. 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.

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 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 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)
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)

3.2.3.2 Authentication of Human Subscribers For Group Certificates

Normally, a certificate shall be issued to a single Subscriber. For cases where there are several entities acting in one capacity, and where non-repudiation for transactions is not desired, a certificate may be issued that corresponds to a private key that is shared by multiple Subscribers. The FPKI Operational Authority, Entities and/or RAs shall 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:

- The Information Systems Security Office or equivalent shall be responsible for ensuring control of the private key, including maintaining a list of Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time.

- The subjectName DN must not imply that the subject is a single individual, e.g. by inclusion of a human name form;

- The list of those holding the shared private key must be provided to, and retained by, the 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).

3.2.3.3 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 providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name)

- Equipment public keys

- Equipment authorizations and attributes (if any are to be included in the certificate)

- Contact information to enable the CA or RA to communicate with the sponsor when required

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

- Verification of digitally signed messages sent from the sponsor (using certificates of equivalent or greater assurance than that being requested).

- In person 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, information that is not verified shall not be included in certificates.

3.2.5   Validation of Authority

For cross-certification, the FPKI Operational Authority shall validate the representative's authorization to act in the name of the organization.

3.2.6   Criteria for Interoperation

The FPKIPA shall determine the criteria for cross-certification with the FBCA. See also Section 1.1.5 and the U.S. Government Public Key Infrastructure Cross-Certification Methodology and Criteria. (see http://www.cio.gov/fbca)

3.3   IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1   Identification and Authentication for Routine Re-key

In the event that a 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.

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

Assurance Level	Routine Re-key Identity Requirements for Subscriber Signature and Encryption Certificates
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 be reestablished through initial registration process at least once every 15 years from the time of initial registration.
Medium (all policies)	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration.
High	Identity may be established through use of current signature key, except that identity shall be established through initial registration 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.)

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

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

4. CERTIFICATE LIFE-CYCLE

4.1 APPLICATION

This section specifies requirements for initial application for certificate issuance.

Entities seeking to cross-certify with the FBCA shall fulfill the application requirements as specified in the U.S. Government Public Key Infrastructure Cross-Certification Criteria and Methodology. The Federal PKI Policy Authority shall act on the application and, upon making a determination to issue a certificate and entering into the MOA with the Entity, shall authorize the FPKI Operational Authority to issue the cross-certificate to the Entity.

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

4.1.1 Submission of Certificate Application

For the FBCA, the certificate application shall 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.

4.1.2 Enrollment Process and Responsibilities

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 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, this CP makes no stipulations regarding enrollment process and responsibilities.

4.2 CERTIFICATE APPLICATION PROCESSING

Information in certificate applications must be verified as accurate before certificates are issued. Entity CPs shall 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 performed by the FPKI Operational Authority.

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.

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

4.2.3   Time to Process Certificate Applications

No stipulation.

4.3   ISSUANCE

4.3.1   CA Actions during Certificate Issuance

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

Entity CAs shall verify the source of a certificate request before issuance.

4.3.2   Notification to Subscriber 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.cio.gov/fbca/tech_requirements.htm)

For Entity CAs, no stipulation

4.4   ACCEPTANCE

4.4.1   Conduct constituting certificate acceptance

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

4.4.2   Publication of the Certificate by the CA

As specified in 2.2.1, all CA certificates shall be published in FBCA or Entity repositories.

This specification makes no 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 FPKI PA shall be notified upon issuance of new inter-organizational CA cross-certificates.

> Practice Note: The process for notifying the FPKIPA shall be 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 protect their private keys from access by other parties. For Rudimentary assurance, no stipulation.

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 CRLs specifying the current status of all unexpired FBCA certificates. It is recommended that relying parties process and comply with this information whenever using FBCA issued certificates in a transaction.

4.6 CERTIFICATE RENEWAL

Certificate renewal consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate including the public key. Frequent renewal of certificates may assist in reducing the size of CRLs.

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.

4.6.2 Who may request Renewal

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

For Entity CAs, no stipulation.

4.6.3   Processing Certificate Renewal Requests

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

For Entity CAs, no stipulation.

4.6.4   Notification of new certificate issuance to Subscriber

The FPKI Operational Authority shall notify Entity CAs upon issuance of new certificates.

For Entity CAs, no stipulation.

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.

4.6.6   Publication of the Renewal certificate by the CA

As specified in 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 FPKI Operational Authority shall inform the FPKIPA of any certificate issuance.

For Entity CAs, no stipulation.

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.

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

4.7.1   Circumstance for Certificate Re-key

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

For Entity CAs, no stipulation.

4.7.2   Who may request certification of a new public key

The FPKI Operational Authority may request certification of a new public key for currently cross-certified Entity Principal CAs.

For Entity CAs, no stipulation.

4.7.3   Processing certificate Re-keying requests

Before performing re-key, the FPKI Operational Authority shall identify and authenticate Principal CAs 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, no stipulation.

4.7.4   Notification of new certificate issuance to Subscriber

The FPKI Operational Authority shall notify Entity CAs upon issuance of new certificates.

For Entity CAs, no stipulation.

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.

4.7.6   Publication of the Re-keyed certificate by the CA

As specified in 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 FPKI Operational Authority shall inform the FPKIPA of any certificate issuance.

For Entity CAs, no stipulation.

4.8   MODIFICATION

Certificate modification consists of creating new certificates with subject information (e.g., a name or email address) that differs 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, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.8.1   Circumstance for Certificate Modification

For the FBCA, certificate modification is performed if the Entity CA changes its name.

For Entity CAs, no stipulation.

4.8.2   Who may request Certificate Modification

The FPKI Operational Authority or the Entity Principal CA may request certificate modification for currently cross-certified Entity Principal CAs.

For Entity CAs, no stipulation.

4.8.3   Processing Certificate Modification Requests

The FPKI Operational Authority shall perform certificate modification at the direction of the FPKI PA. The FPKI Operational Authority 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.

4.8.4   Notification of new certificate issuance to Subscriber

The FPKI Operational Authority shall notify Entity CAs upon issuance of new certificates.

For Entity CAs, no stipulation.

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.

4.8.6   Publication of the modified certificate by the CA

As specified in 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 FPKI Operational Authority shall inform the FPKIPA of any certificate issuance.

For Entity CAs, no stipulation.

4.9 CERTIFICATE REVOCATION & 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, Medium Hardware, Medium, and Basic Assurance, all CAs shall publish CRLs.

4.9.1 Circumstances for Revocation

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

- The first circumstance is when the Federal PKI Policy Authority requests an FBCA-issued certificate be revoked. This will be the normal mechanism for revocation in cases where the Federal PKI Policy Authority 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 Operational Authority 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, Federal PKI Policy Authority, or

    - Other personnel as designated by the Chair, Federal PKI Policy Authority.

The Federal PKI Policy Authority shall meet as soon as practicable to review the emergency revocation.

Entity CAs that implement certificate revocation shall, at a minimum, revoke certificates for the reason of key compromise upon receipt of an authenticated request from an appropriate entity. Other circumstances for certificate revocation may be supported by Entity CAs.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

4.9.2　Who Can Request Revocation

An FBCA certificate may be revoked upon direction of the Federal PKI Policy Authority 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).

Entity CAs that implement certificate revocation shall, at a minimum, accept revocation requests from subscribers. Requests for certificate revocation from other parties may be supported by Entity CAs. Note that an Entity Principal CA may always revoke the certificate it has issued to the FBCA without any Federal PKI Policy Authority action.

4.9.3　Procedure for Revocation Request

Upon receipt of a revocation request involving an FBCA-issued certificate, the FPKI Operational Authority shall authenticate the request and apprise the Federal PKI Policy Authority. The Federal PKI Policy Authority 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 Federal PKI Policy Authority shall direct the FPKI Operational Authority to revoke the certificate. The FPKI Operational Authority shall give prompt oral or electronic notification to previously designated officials in all entities having a Principal CA with which the FBCA interoperates.

Entity CAs that implement certificate revocation shall 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, revocation is optional if all the following conditions are met:

- the revocation request was not for key compromise;
- the hardware token 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.

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

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.

For Entity CAs, no stipulation.

4.9.5   Time within which CA must Process the Revocation Request

For the FBCA, all revocation requests must be processed within six hours of receipt of request.

For Entity CAs, revocation request processing time shall be as specified below:

Assurance Level	Processing Time for Revocation Requests
Rudimentary	No stipulation
Basic	Within 24 hours of receipt of request
Medium (all policies)	Within 18 hours of receipt of request
High	Within six hours of receipt of request

4.9.6   Revocation Checking Requirements for Relying Parties

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, the interval between CRLs shall not exceed 24 hours. In the case of revocation of a certificate, the FBCA shall issue an emergency CRL within six hours.

For Entity CAs, see the table below for issuing frequency of routine and emergency CRLs. For Basic, Medium, Medium Hardware, and High, Emergency CRLs shall be issued whenever a CA certificate is revoked, or any certificate is revoked because of key compromise. CRLs may be issued more frequently than specified below.

Table 1 Entity CA CRL issuance Frequency

Assurance Level	Maximum Interval for Routine CRL Issuance	Maximum Interval for Emergency CRL Issuance
Rudimentary	No stipulation	No stipulation
Basic	24 hours	24 hours after notification
Medium (all policies)	24 hours	18 hours after notification
High	24 hours	Six hours after notification

For Entity Principal CAs that only issue CA certificates and are operated in an off-line manner, routine CRLs may be issued less frequently than specified above. However, the interval between routine CRL issuance shall not exceed 31 days. Such CAs must meet the requirements specified above for issuing Emergency CRLs. (Note: such CAs will also be required to notify the FPKI Operational Authority upon Emergency CRL issuance. This requirement will be included in the MOA between the FPKIPA and the Entity.)

4.9.8   Maximum Latency of CRLs

No stipulation. (See Section 4.9.7).

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.

4.9.10   On-line Revocation Checking Requirements

No stipulation.

4.9.11   Other Forms of Revocation Advertisements Available

Any alternate forms used to disseminate revocation information shall be implemented in a manner consistent with the security and latency requirements for the implementation of CRLs and on-line revocation and status checking.

4.9.12   Special Requirements Related To Key Compromise

In the event of an Entity Principal CA private key compromise or loss, a CRL shall be published at the earliest feasible time by the FPKI Operational Authority.

For Entity CAs, no stipulation.

4.9.13   Circumstances for Suspension

Suspension shall not be used by the FBCA.

For Entity CAs, no stipulation.

4.9.14   Who can Request Suspension

For Entity CAs, no stipulation.

4.9.15   Procedure for Suspension Request

For Entity CAs, no stipulation.

4.9.16   Limits on Suspension Period

For Entity CAs, no stipulation.

4.10 CERTIFICATE STATUS SERVICES

No stipulation.

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

No stipulation.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

No stipulation.

4.12 KEY ESCROW & 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.

4.12.1 Key Escrow and Recovery Policy and Practices

For the FBCA, no stipulation.

Entity CAs that support key recovery shall identify the document describing the key recovery policy in the applicable CP.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

For the FBCA, no stipulation.

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

5. FACILITY MANAGEMENT & OPERATIONS CONTROLS

5.1 PHYSICAL CONTROLS

The FBCA and Entity CAs shall impose physical security requirements that provide similar levels of protection as those specified below. All the physical control requirements apply equally to the FBCA and Entity CAs.

5.1.1 Site Location & Construction

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

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

The FBCA and Entity CA equipment shall always be protected from unauthorized access. The security mechanisms shall 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 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 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 system

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

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

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

5.1.2.2 Physical Access for RA Equipment

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

5.1.3 Power and Air Conditioning

The FBCA and Entity CAs (operating at the Basic Assurance level or higher) shall have backup capability sufficient to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. In addition, the FBCA directories (containing FBCA issued certificates and CRLs) shall be provided with Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power.

5.1.4 Water Exposures

No stipulation.

5.1.5 Fire Prevention & Protection

No stipulation.

5.1.6 Media Storage

FBCA and Entity CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic).

5.1.7 Waste Disposal

Sensitive waste material shall be disposed of in a secure fashion.

5.1.8 Off-Site backup

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

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 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. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The requirements of this policy are defined in terms of four roles. (Note: the information derives from the Certificate Issuing and Management Components (CIMC) Protection Profile.)

1. *Administrator* – authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.

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

3. *Auditor* – authorized to maintain audit logs.

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

Some roles may be combined. The roles required for each level of assurance are identified in Section 5.2.4.

The following subsections provide a detailed description of the responsibilities for each role.

5.2.1.1 Administrator

The administrator role is responsible for:

- Installation, configuration, and maintenance of the CA;
- Establishing and maintaining CA system accounts;
- Configuring certificate profiles or templates and audit parameters, and;
- Generating and backing up CA keys.

Administrators do not issue certificates to subscribers.

5.2.1.2 Officer

The officer role is responsible for issuing certificates, that is:

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

5.2.1.3 Auditor

The auditor role is responsible for:

- Reviewing, maintaining, and archiving audit logs;
- Performing or overseeing internal compliance audits to ensure that the FBCA or Entity CA is operating in accordance with its CPS;

5.2.1.4 Operator

The operator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

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, Medium Hardware, or High Levels of Assurance for the following tasks:

- CA key generation;
- CA signing key activation;
- CA private key backup.

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

Multiparty control shall not be achieved using personnel that serve in the Auditor Trusted Role.

5.2.3 Identification and Authentication for Each Role

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

5.2.4 Separation of Roles

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

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

Assurance Level	Role Separation Rules
Rudimentary	No stipulation.
Basic	Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role, however, no one individual shall assume both the Officer and Administrator roles. This may be enforced procedurally. No individual shall be assigned more than one identity.
Medium (all policies)	Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role; however, individuals who assume an Officer role may not assume an Administrator or Auditor role. The CA system shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role or an Auditor and an Officer role. No individual shall be assigned more than one identity.
High	Individual CA personnel shall 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 system shall identify and authenticate its users and shall enforce these roles. No individual shall have more than one CA operational identity.

The FBCA shall operate at the High Assurance level.

5.3 PERSONNEL CONTROLS

5.3.1 Background, Qualifications, Experience, & Security 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 Federal PKI Policy Authority and the FPKI Operational Authority.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity. For the FBCA and Federal Agency PKIs, regardless of the assurance level, and for state and local government PKIs operated in the U.S. at High Assurance, all trusted roles are required to be held by U.S. citizens. For PKIs operated at Medium Assurance and Medium Hardware, all trusted roles must be held by citizens of the country where the CA is located. For PKIs operated at Medium-CBP and Medium Hardware-CBP, there is no citizenship requirement specified.

> Practice Note: For PKIs operated at Medium Assurance and Medium Hardware on behalf of multinational governmental organizations, all trusted roles must be held by citizens of the member countries.

Where an entity PKI operated at Medium or Medium Hardware Assurance is affiliated with RAs operated overseas, RA personnel holding trusted roles may be local citizens of the country where the RA is located or of the country where the CA is located.

FPKI Operational Authority personnel acting in trusted roles shall hold TOP SECRET security clearances.

5.3.2 Background Check Procedures

FPKI Operational Authority personnel acting in trusted roles shall, at a minimum, undergo procedures necessary to be cleared at the TOP SECRET level

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

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

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

Adjudication of the background investigation shall be performed by a competent adjudication authority using a process consistent with Executive Order 12968 August 1995, or equivalent.

> 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 or Entity CA shall 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 security principles and mechanisms;
- All PKI software versions in use on the CA system.

Documentation shall 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 & Requirements

Individuals responsible for PKI roles shall be aware of changes in the FBCA and Entity CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall 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 be maintained identifying all personnel who received training and the level of training completed.

5.3.5 Job Rotation Frequency & Sequence

For the FBCA, any job rotation frequency and sequencing procedures shall provide for continuity and integrity of the FBCA services.

For Entity CAs, no stipulation.

5.3.6 Sanctions for Unauthorized Actions

The FPKI Operational Authority shall take appropriate actions where personnel have performed actions involving the FBCA or its repository not authorized in this CP, the FBCA CPS, or other procedures published by the FPKI Operational Authority.

For Entity CAs, no stipulation.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to the FBCA or an Entity CA shall meet the personnel requirements set forth in the FBCA CP or Entity CP, as applicable.

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 be provided to the personnel filling that role.

5.4 AUDIT LOGGING PROCEDURES

Audit log files shall be generated for all events relating to the security of the FBCA or Entity CAs. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with *Retention period for archive*, Section 5.5.2.

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

- The type of event,

- The date and time the event occurred,

- A success or failure indicator, 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.

Auditable Event	Rudimentary	Basic	Medium (all policies)	High
SECURITY AUDIT				
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

Auditable Event	Rudimentary	Basic	Medium (all policies)	High
KEY GENERATION				
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 purposes	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

Auditable Event	Rudimentary	Basic	Medium (all policies)	High
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

Auditable Event	Rudimentary	Basic	Medium (all policies)	High
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

Auditable Event	Rudimentary	Basic	Medium (all policies)	High
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

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 logs. Actions taken as a result of these reviews shall be documented.

For the FBCA, the FPKI Operational Authority shall explain all significant events in an audit log summary.

Assurance Level	Review Audit Log
Rudimentary	Only required for cause
Basic	Only required for cause
Medium (all policies)	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
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.

5.4.4 Protection of Audit Logs

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

- Only personnel assigned to trusted roles have read access to the logs;

- Only authorized people may archive audit logs; and,

- Audit logs are not modified.

The entity performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from 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 a safe, secure location separate from the CA equipment.

> 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 and audit summaries shall be backed up at least monthly. A copy of the audit log shall be sent off-site on a monthly basis.

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. Automated audit processes shall be invoked at system or application startup, and cease only at system or application shutdown. Should it become apparent that 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 FPKI Operational Authority Administrator (or comparable Entity authority) shall determine whether to suspend FBCA operation (or Entity CA operation respectively) until the problem is remedied.

5.4.7 Notification to Event-Causing Subject

This CP imposes no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event.

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 perform routine assessments for evidence of malicious activity.

5.5 RECORDS ARCHIVE

5.5.1 Types of Events Archived

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

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

Data To Be Archived	Rudimentary	Basic	Medium (all policies)	High
CA accreditation (if applicable)	X	X	X	X
Certification Practice Statement	X	X	X	X
Contractual obligations	X	X	X	X
System and equipment configuration	X	X	X	X
Modifications and updates to system or configuration	X	X	X	X
Certificate requests	X	X	X	X
Revocation requests		X	X	X
Subscriber identity Authentication data as per Section 3.1.9		X	X	X
Documentation of receipt and acceptance of certificates		X	X	X
Documentation of receipt of tokens		X	X	X
All certificates issued or published	X	X	X	X
Record of CA Re-key	X	X	X	X

Data To Be Archived	Rudimentary	Basic	Medium (all policies)	High
All CRLs issued and/or published		X	X	X
All Audit Logs	X	X	X	X
Other data or applications to verify archive contents		X	X	X
Documentation required by compliance auditors		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.

Assurance Level	Minimum Retention Period
Rudimentary	7 Years & 6 Months
Basic	7 Years & 6 Months
Medium (all policies)	10 Years & 6 Months
High	20 Years & 6 Months

5.5.3 Protection of Archive

No unauthorized user shall be permitted to write to or delete the archive. For the FBCA, archived records may be moved to another medium when authorized by the FPKI Operational Authority Administrator. Archive media shall be stored in a safe, secure storage facility separate from the FBCA or Entity CA itself.

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 Federal PKI Policy Authority for the FBCA (or Entity for the Entity CA).

Prior to the end of the archive retention period, the FPKI Operational Authority shall provide archived data and the applications necessary to read the archives to a Federal PKI

Policy Authority approved archival facility, which shall retain the applications necessary to read this archived data.

5.5.4 Archive Backup Procedures

The CPS or a referenced document shall describe how archive records are backed up, and how the archive backups are managed.

5.5.5 Requirements for Time-Stamping of Records

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

5.5.6 Archive Collection System (internal or external)

No stipulation.

5.5.7 Procedures to Obtain & Verify Archive Information

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

The contents of the archive shall not be released except as determined by the Federal PKI Policy Authority for the FBCA (or Entity for the Entity CA) or as required by law. 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 signing key, that key may be changed often; 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 certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs that cover certificates signed with that key, then the old key must be retained and protected.

For the FBCA, key changeover procedures will establish key rollover certificates where a certificate containing the old public key will be signed by the new private key, and a certificate containing the new public key will be signed by the old private key.

Entity CAs either must establish key rollover certificates as described above or must obtain a new CA certificate for the new public key from the issuers of their current certificates.

> 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 & DISASTER RECOVERY

5.7.1   Incident and Compromise Handling Procedures

The members of the Federal PKI Policy Authority shall be notified if any of the following cases occur:

- suspected or detected compromise of the FBCA systems;

- physical or electronic attempts to penetrate FBCA systems;

- denial of service attacks on FBCA components;

- any incident preventing the FBCA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

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

The FPKI Operational Authority shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the FBCA CPS.

Entity CAs shall provide notice as required by the applicable MOA.

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 shall respond as follows:

- If the CA signature keys are not destroyed, CA operation shall be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in 4.9.7, Table 1.

- If the CA signature keys are destroyed, CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

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):

- The Federal PKI Policy Authority and all of its member entities shall be notified so that entities may issue CRLs revoking any cross-certificates issued to the compromised CA;

- A new FBCA or Entity CA key pair shall be generated by the FBCA or Entity CA in accordance with procedures set forth in the FBCA or Entity CPS; and

- New FBCA or Entity CA certificates shall be issued to Entities also in accordance with the FBCA or Entity CPS.

The FPKI Operational Authority or Entity CA governing body shall also investigate and report to the Federal PKI Policy Authority what caused the compromise or loss, and what measures have been taken to preclude recurrence.

5.7.4 Business Continuity Capabilities after a Disaster

The FBCA directory system shall be deployed so as to provide 24 hour, 365 day per year availability. The FPKI Operational Authority shall implement features to provide high levels of directory reliability.

The FPKI Operational Authority 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 FPKI Operational Authority or Entity Principal CA shall at the earliest feasible time securely advise the Federal PKI Policy Authority and all of its member entities in the event of a disaster where the FBCA or Entity Principal CA installation is physically damaged and all copies of the FBCA or Entity Principal CA signature keys 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 and the Federal PKI Policy Authority shall advise entities that have entered into MOAs with the Federal PKI Policy Authority that FBCA operation has terminated so they may revoke certificates they have issued to the FBCA. Prior to FBCA termination, the FPKI Operational Authority shall provide all archived 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.

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

6. TECHNICAL SECURITY CONTROLS

6.1   KEY PAIR GENERATION & 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 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 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 5.2.2.

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 the process shall be validated by an independent third party.

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 be performed using a FIPS approved method or equivalent international standard.

At the High and Medium Hardware assurance levels, subscriber key generation must be performed using a hardware cryptographic module. For all other assurance levels, either software or hardware cryptographic modules may be used for key generation.

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 not retain any copy of the key after delivery of the private key to the Subscriber.

- The private key must be protected from activation, compromise, or modification during the delivery process.

- The Subscriber shall acknowledge receipt of the private key(s).

- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers.
    - For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it.
    - For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.
    - For shared key applications, organizational identities, and network devices, see also Section 3.2.

The 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, 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 bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate.

For 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 certificates shall be conveyed to relying parties in a secure fashion to preclude substitution attacks.

> 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 not required.

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

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

6.1.5 Key Sizes

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

For CAs that distribute self-signed certificates to relying parties, the CA's subject public keys in such certificates shall be at least 2048 bits for RSA, or at least 224 bits for ECDSA.

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. Certificates that expire after 12/31/08 shall be generated with at least 2048 bit RSA key, or at least 224 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. Signatures on certificates and CRLs that are issued after 12/31/08 shall be generated using, at a minimum, SHA-256.

End-entity certificates that expire before 12/31/08 shall contain public keys that are at least 1024 bit for RSA, DSA, or Diffie-Hellman, or 160 bits for elliptic curve algorithms. End-entity certificates that expire on or after 12/31/08 shall contain public keys that are at least 2048 bit for RSA or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys through 12/31/08. Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 2048 bit RSA or equivalent for the asymmetric keys after 12/31/08.

6.1.6 Public Key Parameters Generation and Quality Checking

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

Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186; additional tests may be specified by the Federal PKI Policy Authority.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

Public keys that are bound into certificates shall 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 to be used for digital signatures (including authentication) shall set the *digitalSignature* and/or *nonRepudiation* bits. Certificates to be used for key or data encryption shall set the *keyEncipherment* and/or *dataEncipherment* bits. Certificates to be used for key agreement shall set the *keyAgreement* 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 be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CP. Such dual-use certificates shall never assert the non-repudiation key usage bit, and shall not be used for authenticating data that will be verified on the basis of the dual-use certificate at a future time. 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.

6.2 PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards & Controls

The relevant standard for cryptographic modules is FIPS PUB 140, *Security Requirements for Cryptographic Modules*.

Cryptographic modules shall be validated to the FIPS 140 level identified in this section. Additionally, the Federal PKI Policy Authority 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	Subscriber	RA
Rudimentary	Level 1 (Hardware or Software)	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)
Medium Hardware	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
High	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

6.2.2 Private Key Multi-Person Control

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

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

6.2.3 Private Key Escrow

6.2.3.1 Escrow of FBCA and Entity CA private signature key

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

6.2.3.2 Escrow of CA encryption keys

The FBCA shall not perform any encryption key recovery functions involving encryption keys issued to Entity CAs. However, if encryption key pairs need to be issued by the 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 not be escrowed.

No stipulation with respect to escrow of subscriber private encryption keys.

6.2.4 Private Key Backup

6.2.4.1 Backup of FBCA & Entity CA Private Signature Key

FBCA private signature keys shall be backed up under multi-person control, as specified in Section 5.2.2.

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

No more than a single copy of the signature key shall be stored at the FBCA or Entity CA location. Additional copies may exist off-site provided that accountability for them is maintained.

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, Subscriber private signature keys may be backed up or copied, but must be held in the Subscriber's control.

6.2.5 Private Key Archival

Private signature keys shall not be archived.

For private encryption keys (key management or key transport), no stipulation.

6.2.6 Private Key Transfer into or from a Cryptographic Module

FBCA and Entity CA private keys shall be generated by and remain in a cryptographic module. The CA private keys may be backed up in accordance with Section 6.2.4.1.

For Subscriber private keys, no stipulation.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation.

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.

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. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.9 Methods of Deactivating Private Keys

After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. Hardware cryptographic modules shall be removed and stored in a secure container when not in use.

If cryptographic modules are used to store subscriber private keys, then the cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access.

6.2.10 Method of Destroying Subscriber Private Signature Keys

Subscriber 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 should not be 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.

6.3.2   Certificate Operational Periods/Key Usage Periods

The usage period for an FBCA key pair is a maximum of six years. The FBCA private key may be used to generate certificates for the first half of the usage period (3 years), and the public key may be used to validate certificates for the entire usage period. If the FBCA private key is used to sign CRLs, it may be used to sign CRLs for the entire usage period.

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

6.4   ACTIVATION DATA

6.4.1   Activation Data Generation & Installation

The activation data used to unlock FBCA, Entity CA or subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.   Where the FBCA or an Entity CA uses passwords as activation data for the CA signing key, at a minimum the activation data shall be changed upon CA re-key.

6.4.2   Activation Data Protection

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

- memorized
- biometric in nature, or
- recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module.

The protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CP or CPS.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

For the FBCA, 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 and its ancillary parts shall include the following functionality:

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

For Entity CAs, 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:

- 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.

6.5.2 Computer Security Rating

No Stipulation.

6.6 LIFE-CYCLE SECURITY CONTROLS

6.6.1 System Development Controls

The System Development Controls for the FBCA and Entity CAs at the Basic Assurance level and above are as follows:

- For commercial off-the-shelf software, the software shall be designed and developed under a formal, documented development methodology.

- For hardware and software developed specifically for a particular CA, the applicant shall demonstrate that security requirements were achieved through a combination of software verification & validation, structured development approach, and controlled development environment.

- Where open source software has been utilized, the applicant shall demonstrate that security requirements were achieved through software verification & validation and structured development/life-cycle management.

- Hardware and software procured to operate the CA shall be purchased and shipped in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).

- The CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications; hardware devices, network connections, or component software installed which are not part of the CA operation.

- Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Hardware and software shall be scanned for malicious code on first use and periodically thereafter.

- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the FBCA or Entity CA system as well as any modifications and upgrades shall be documented and controlled. There shall 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 be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. For the FBCA, the integrity of the software shall be verified by the FPKI Operational Authority at least weekly (e.g., in conjunction with CRL publication).

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 NETWORK SECURITY CONTROLS

Network security controls shall be employed to protect the FBCA and the FBCA Internal Directory. Networking equipment shall turn off unused network ports and services. Any network software installed on the FBCA equipment shall be necessary to the functioning of the FBCA.

The FBCA Border Directory 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 Border directory or FBCA local area network shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

Entity CAs and directories shall employ appropriate network security controls. Networking equipment shall turn off unused network ports and services. Any network software present shall be necessary to the functioning of the equipment.

6.8 TIME STAMPING

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

7. CERTIFICATE, 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 (populate version field with integer "2").

7.1.2 Certificate Extensions

For all CAs, use of standard certificate extensions shall comply with [RFC 3280].

Certificates issued by the FBCA shall comply with *Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile* [FPKI-Prof]. Certificates issued by Federal Entity CAs operating at High, Medium Hardware, and/or Medium Assurance shall comply with [FPKI-Prof].

Certificates issued by the FBCA shall not include critical private extensions.

CA 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 community of use is not impaired.

7.1.3 Algorithm Object Identifiers

Certificates issued by the FBCA and Entity CAs shall identify the signature algorithm using one of the following OIDs:

id-dsa-with-sha1	{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3 }
sha-1WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }
sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
id-RSASSA-PSS	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10 }
ecdsa-with-SHA1	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) 1 }

ecdsa-with-SHA224	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1 }
ecdsa-with-SH256	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2 }
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }
ecdsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 }

Where certificates are signed using RSA with PSS padding, the 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 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 }
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }

Certificates issued by the FBCA and Entity CAs shall identify the cryptographic algorithm associated with the subject public key using one of the following OIDs:

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

Where non-CA certificates issued on behalf of federal agencies contain an elliptic curve public key, the parameters shall be specified as one of the following named curves:

ansip192r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 1 }
ansit163k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 1 }

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

7.1.4 Name Forms

Where required as set forth in Section 3.1.1, the subject and issuer fields of the base certificate shall be populated with an X.500 Distinguished Name. Distinguished names shall be composed of standard attribute types, such as those identified in [RFC3280].

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 Principal CAs to that appropriate for their domains. Additionally, the Federal PKI Policy Authority may require that the FPKI Operational Authority include such constraints for the FBCA 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 shall include a certificate policies extension asserting the OID(s) appropriate to the level of assurance with which it was issued. See Section 1.2 for specific OIDs.

For Entity CAs, no stipulation.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax & Semantics

Certificates issued by the FBCA shall not contain policy qualifiers. Certificates issued by Entity PKIs may contain policy qualifiers identified in [RFC 3280].

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Not applicable; certificates issued by the FBCA do not include a critical certificate policies extension.

7.2   CRL PROFILE

7.2.1 Version Numbers

The FBCA shall 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 Entry Extensions

For the FBCA, CRL extensions shall conform to [FPKI-PROF].

7.3   OCSP PROFILE

No stipulation.

8. COMPLIANCE AUDIT & OTHER ASSESSMENTS

The FPKI Operational Authority shall 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 shall have a compliance audit mechanism in place to ensure that the requirements of their CP/CPS are being implemented and enforced.

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

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

The FBCA, Entity Principal CAs and RAs and their subordinate CAs and RAs shall be subject to a periodic compliance audit at least once per year for High, Medium Hardware, and Medium Assurance, and at least once every two years for Basic Assurance.

For entity PKIs operated by federal agencies and entity PKIs operated under federal contract, alternative reviews may be substituted for full compliance audits under exceptional circumstances. The conditions that permit an alternative review are as follows:

(1) If no changes to policies, procedures, or operations have occurred during the previous year, an assertion to that effect, signed by the cognizant executive (CIO or equivalent), is acceptable in lieu of a full compliance audit.

(2) If no significant changes to policies, procedures, or operations have occurred during the previous year, a delta compliance audit is acceptable in lieu of a full compliance audit.

(3) However, a full compliance audit (see section 8.4) must be completed every third year regardless.

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

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

The FBCA and Entity Principal CAs 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 Federal PKI Policy Authority

has the right to require aperiodic compliance audits of Entity Principal CAs (and, when needed, their subordinate CAs) that interoperate with the FBCA under this CP. The Federal PKI Policy Authority shall state the reason for any aperiodic compliance audit.

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 Federal PKI Policy Authority 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 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 FPKI Operational Authority shall 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 be a private firm, that is independent from the entity being audited, or it shall 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.

The Federal PKI Policy Authority shall determine whether a compliance auditor meets this requirement.

8.4   TOPICS COVERED BY ASSESSMENT

The compliance audit of the FBCA shall verify that the FPKI Operational Authority is implementing all provisions of a CPS approved by the FPKI Policy Authority consistent with this CP. The audit shall also verify that the FPKI Operational Authority is implementing the relevant provisions of the MOAs between the FPKI Policy Authority and each Entity PKI.

The purpose of a compliance audit of an Entity PKI shall be to verify that an entity subject to the requirements of an Entity CP is complying with the requirements of those documents, as well as any MOAs between the Entity PKI and any other PKI.

A full compliance audit for the FBCA or an Entity PKI covers all aspects within the scope identified above.

Where permitted by section 8.1, the FBCA or Entity PKI may perform a delta compliance audit in lieu of the full compliance audit. A delta compliance audit covers all changes to

policies, procedures, or operations that have occurred during the previous year. The following topics must be addressed in a delta compliance audit even if no changes have occurred since the last full compliance audit:

(1) Personnel controls;
(2) Separation of Duties;
(3) Audit review frequency and scope;
(4) Types of events recorded in physical and electronic audit logs;
(5) Protection of physical and electronic audit data;
(6) Physical security controls; and
(7) Backup and Archive generation and storage.

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 be performed:

- The compliance auditor shall document the discrepancy and provide a copy to the FPKI Operational Authority;

- The FPKI Operational Authority will provide a copy of the discrepancy documentation to the Federal PKI Policy Authority Chair;

- The FPKI Operational Authority will report findings and corrective action to the Federal PKI Policy Authority;

- The FPKI Operational Authority shall 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 Federal PKI Policy Authority may direct the FPKI Operational Authority 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 be performed:

- The compliance auditor shall document the discrepancy;

- The compliance auditor shall notify the responsible party promptly;

- The Entity PKI shall 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 proceed to make such notifications and take such actions without delay.

When the Federal PKI Policy Authority receives a report of audit deficiency from an Entity PKI, the Federal PKI Policy Authority may direct the FPKI Operational Authority to take additional actions to protect the level of trust in the infrastructure.

8.6   COMMUNICATION OF RESULTS

Upon completion, an Audit Compliance Report letter shall be provided to the Federal PKI Policy Authority. The report shall identify the versions of the CP and CPS used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in Section 8.5 above.

9. OTHER BUSINESS & LEGAL MATTERS

9.1 FEES

The Federal PKI Policy Authority reserves the right to charge a fee to each Entity in order to support operations of the FBCA.

9.1.1 Certificate Issuance/Renewal Fees

No Stipulation.

9.1.2 Certificate Access Fees

No Stipulation.

9.1.3 Revocation or Status Information Access Fee

No Stipulation.

9.1.4 Fees for other Services

No Stipulation.

9.1.5 Refund Policy

No Stipulation.

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 determine what financial limits, if any, they wish to impose for certificates used to complete a transaction.

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance/warranty Coverage for End-Entities

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

FBCA information not requiring protection shall be made publicly available. Federal PKI Policy Authority 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.

9.3.2 Information not within the scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

No stipulation.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

The FPKI Operational Authority shall conduct a Privacy Impact Assessment. If deemed necessary, the FPKI Operational Authority shall have a Privacy Plan to protect personally identifying information from unauthorized disclosure. The Federal PKI Policy Authority shall approve the Privacy Plan.

For Entity CAs, no stipulation.

9.4.2 Information treated as Private

The FBCA shall protect all subscriber personally identifying information from unauthorized disclosure. The FBCA shall also protect personally identifying information for Entity personnel collected to support cross-certification and MOA requirements from unauthorized disclosure.

For Entity CAs, no stipulation.

9.4.3 Information not deemed Private

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

9.4.4 Responsibility to Protect Private Information

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

9.4.5 Notice and Consent to use Private Information

The FPKI Operational Authority 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 FPKI Operational Authority shall 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 be processed according to 41 CFR 105-60.605.

9.4.7 Other Information Disclosure Circumstances

None.

9.5 INTELLECTUAL PROPERTY RIGHTS

The FPKI Operational Authority will not knowingly violate intellectual property rights held by others.

9.6 REPRESENTATIONS & WARRANTIES

The obligations described below pertain to the FBCA (and, by implication, the FPKI Operational Authority), and to Principal or other 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 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 Federal PKI Policy Authority 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 MOA.

9.6.1 CA Representations and Warranties

FBCA certificates are issued and revoked at the sole discretion of the Federal PKI Policy Authority. 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 Federal PKI Policy Authority of a non-federal entity's certificate policy is for the use of the Federal PKI Policy Authority 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 Federal PKI Policy Authority is not a substitute for due care and mapping of certificate policies by the non-federal entity.

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscriber Representations and Warranties

For Medium, Medium Hardware, and High Assurance levels, a Subscriber shall be required to sign a document containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. For Basic Assurance level, the Subscriber shall 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 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 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 Representations and Warranties

None.

9.6.5 Representations and Warranties of other Participants

None.

9.7   DISCLAIMERS OF WARRANTIES

No stipulation.

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 & TERMINATION

9.10.1 Term

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

9.10.2 Termination

Termination of this CP is at the discretion of the FPKI Policy Authority.

9.10.3 Effect of Termination and Survival

None.

9.11 INDIVIDUAL NOTICES & COMMUNICATIONS WITH PARTICIPANTS

None.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The Federal PKI Policy Authority shall review this CP at least once every year. Corrections, updates, or suggested changes to this CP shall 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

This CP and any subsequent changes shall be made publicly available.

9.12.3 Circumstances under which OID must be changed

OIDs will be changed if the FPKI Policy Authority 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 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 be governed by law (statute, case law or regulation) under which the Entity operates.

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

9.15 COMPLIANCE WITH APPLICABLE LAW

No stipulation.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

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

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 OTHER PROVISIONS

No stipulation.

10. BIBLIOGRAPHY

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

ABADSG   Digital Signature Guidelines, 1996-08-01.
http://www.abanet.org/scitech/ec/isc/dsgfree.html.

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

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.

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.

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

CA	Certification Authority
CARL	Certificate Authority Revocation List
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FPKI OA	Federal Public Key Infrastructure Operational 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
GPEA	Government Paperwork Elimination Act of 1998
IETF	Internet Engineering Task Force

ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
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)
NIST	National Institute of Standards and Technology
NSA	National Security Entity
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
TSDM	Trusted Software Development Methodology
UPS	Uninterrupted Power Supply

URL   Uniform Resource Locator

U.S.C.   United States Code

WWW   World Wide Web

12. 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).

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.

Attribute Authority — An entity, recognized by the FPKIPA or comparable Entity body as having the authority to verify the association of attributes to an identity.

Audit — Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]

Audit Data — Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]

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 certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
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 it has issued that are revoked prior to their stated expiration date.
Certificate Status Authority	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.
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	A certificate used to establish a trust relationship between two Certification Authorities.
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. [FIPS1401]
Cryptoperiod	Time span during which each key setting remains in effect. [NS4009]

Data Integrity	Assurance that the data are unchanged from creation to reception.
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.
Employee	Any person employed by an Entity as defined above.
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	Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.
Entity CA	A CA that acts on behalf of an Entity, and is under the operational control of an Entity.
FBCA Operational Authority (FPKI OA)	The Federal Public Key Infrastructure Operational Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.
Federal Public Key Infrastructure Policy Authority (FPKI PA)	The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding interEntity PKI interoperability that uses the FBCA.

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.
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, 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 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 key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.

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	Information that is important to the support of deployed and contingency forces.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	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 are used to uniquely identify each of the seven policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).

Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
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)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, 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 made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.

Relying Party	A person or Entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
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.
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 or network device

Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
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 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.
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]

13. ACKNOWLEDGEMENTS

The Certificate Policy Working Group developed this CP based on RFC 3647 and the original FBCA Certificate Policy.