X.509 Certificate Policy

For The

Federal Bridge Certification Authority (FBCA)

27 September 2004

Approved by:

_____

Chair, Federal Public Key Infrastructure Policy Authority (FPKIPA)

Revision Page

Document Date	Revision Details
27 September 2004	This FBCA CP updates and replaces the 10 September 2002 version. Text changes are specified in the following FBCA CP Change Proposals (**change proposal number**, title, date): **2003-01**, Clarify FBCA requirements to facilitate cross certification with the Department of Defense, 20 September 2004 **2003-02**, Clarify FBCA requirements to facilitate cross certification with the State of Illinois, 20 September 2004 **2003-03**, FBCA Event Logging, 20 August 2003 **2003-04**, FBCA Token Destruction, 3 September 2003 **2003-05**, FBCA Operational Authority Independent Audit Qualifications, 1 August 2003 **2004-01**, Clarify FBCA requirements for online FBCA internal and border directories, 8 June 2004 **2004-02**, Various editorial changes from CPWG meetings for the HEBCA CP mapping and the DoD ECA CP mapping, 24 September 2004

Table of Contents

1. INTRODUCTION

This Certificate Policy (CP) defines five certificate policies for use by the Federal Bridge Certification Authority (FBCA) to facilitate interoperability between the FBCA and other Entity PKI domains. The five policies represent four different assurance levels (Rudimentary, Basic, Medium, and High) for public key digital certificates, plus one assurance level used strictly for testing purposes (Test). The word "assurance" used in this CP means how well a Relying Party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate. In addition, it also reflects how well the Relying Party can be certain that the individual whose subject name is cited in the certificate is controlling the use of the private key that corresponds to the public key in the certificate, and how securely the system which was used to produce the certificate and (if appropriate) deliver the private key to the subscriber performs its task.

The FBCA supports interoperability among Entity PKI domains in a peer to peer fashion. The FBCA issues certificates only to those CAs designated by the owning Entity (called "Principal CAs"). The FBCA, or a CA that interoperates with 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. The FBCA does not add to and should not subtract from trust relationships existing between the transacting parties as established through the Federal PKI Policy Authority.

At their discretion, entities may elect to interoperate among themselves without using the FBCA. Those entities that elect to do so may nonetheless employ levels of assurance that mimic those set forth in the FBCA CP. 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. When used in the *policyMappings* extension, the Entity may employ the OIDs only after a policy mapping determination is made by the Federal PKI Policy Authority allowing their use.

This FBCA CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 2527, Certificate Policy and Certification Practice Statement 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 party that registers the OID (in this case, the U.S. Government) also publishes the CP, for examination by Relying Parties. Each certificate issued by the FBCA will, in the

policyMappings extension and in whatever other fashion is determined by the FBCA Operational Authority (described in section 1.3.1.2) to be necessary for interoperability, reflect what mappings the Federal PKI Policy Authority determines shall exist between the FBCA CP and the affected Entity CP.

1.1.2 Relationship Between the FBCA CP and the FBCA CPS

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

1.1.3 Relationship Between the FBCA CP and the Entity CP

The levels of assurance of the certificates issued under the FBCA CP are mapped by the Federal PKI Policy Authority to the levels of assurance of the certificates issued by Entity CAs. The policy mappings information is placed into the certificates issued by the FBCA, or otherwise published or used by the FBCA Operational Authority (described in section 1.3.1.2) so as to facilitate interoperability.

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 IDENTIFICATION

There are 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. The OIDs are registered under the id-infosec arc 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-highAssurance	::= fbca-policies 4
id-fpki-certpcy-testAssurance	::= fbca-policies 5

1.3 COMMUNITY AND APPLICABILITY

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 that includes overseeing the operation of the organizations responsible for governing and promoting its use. In particular, this CP is established under the authority of and with the approval of the Federal CIO Council.

1.3.1.2 Federal PKI Policy Authority

The Federal PKI Policy Authority is a group of U.S. Federal Government Agencies (including cabinet-level Departments) established pursuant to the Federal CIO Council. The Federal PKI Policy Authority is responsible for:

- The Federal Bridge Certification Authority (FBCA) Certificate Policy (CP),
- The FBCA Certification Practice Statement (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 Federal PKI Policy Authority), 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 Federal PKI Policy Authority will enter into a Memorandum of Agreement (MOA) with an 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. Thus, the term “MOA” as used in this CP shall always refer to the Memorandum of Agreement cited in this paragraph. 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 FBCA Operational Authority

The FBCA Operational Authority is the organization that operates the FBCA, including issuing FBCA certificates when directed by the Federal PKI Policy Authority, posting those certificates and Certification Authority Revocation Lists (CARLs) into the FBCA repository, and ensuring the continued availability of the repository to all users.

1.3.1.4 FBCA Operational Authority Administrator

The Administrator is the individual within the FBCA Operational Authority who has principal responsibility for overseeing the proper operation of the FBCA including the FBCA repository, and who appoints individuals to the positions of FBCA Operational Authority Officers.

1.3.1.5 FBCA Operational Authority Officers

These officers are the individuals within the FBCA Operational Authority, selected by the Administrator, who operate the FBCA and its repository including executing Federal PKI Policy Authority direction to issue FBCA certificates to Principal CAs or taking other action to effect interoperability between the FBCA and Principal CAs. The roles include FBCA Operational Authority Officer, Auditor, and Operator, all described in later sections of this CP.

1.3.1.6 Entity Principal Certification Authority (Principal CA)

The Principal CA is a CA within a PKI that has been designated to interoperate directly with the FBCA (e.g., through the exchange of cross-certificates), and which issues either end-entity certificates, or cross-certificates (or other means of interoperation) to other Entity or external party CAs, or both. It should be noted that an Entity may request that the FBCA interoperate 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 this term 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 the Entity employs a hierarchical or other PKI architecture.

1.3.1.7 Federal Bridge Certification Authority (FBCA)

The FBCA is the entity operated by the FBCA 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 FBCA 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.

1.3.1.8 Registration Authority (RA)

The RA is the entity that collects and verifies each Subscriber's identity and information that are to be entered into his or her public key certificate. The FBCA 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. The requirements for RAs in Entity PKIs are set forth in the sections below.

1.3.2 Related Authorities

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

1.3.3 End Entities

1.3.3.1 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate, who asserts that it uses its key and certificate in accordance with the certificate policy asserted in the certificate, and who does not itself issue certificates. FBCA Subscribers include only FBCA Operational Authority personnel and, when determined by the Federal PKI Policy Authority, possibly certain network or hardware devices such as firewalls and routers when needed for infrastructure protection. CAs are sometimes technically considered "subscribers" in a PKI. However, the term "Subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

1.3.3.2 Relying Parties

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

1.3.4 Applicability

The sensitivity of the information processed or protected using certificates issued by FBCA or an Entity CA will vary significantly. Entities 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 Entity for each application and is not controlled by this CP. To provide sufficient granularity, this CP specifies security requirements at four increasing, qualitative levels of assurance: Rudimentary, Basic, Medium 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

This CP also defines the Test level of assurance, which is used by the FBCA prototype bridge and CAs when conducting interoperability testing. The production FBCA does not issue certificates with the Test level of assurance.

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

Assurance Level	**Applicability**
Test	This level is used for interoperability testing between the FBCA and Principal CAs. It is solely used for this purpose and conveys no assurance information.
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.
High	This level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

1.3.4.1 Factors in determining usage

The Relying Party must first determine the level of assurance required for an application, and then select the certificate appropriate for meeting the needs of that application. This will be determined by evaluating various risk factors including the value of the information, the threat environment, and the existing protection of the information environment. These determinations are made by the Relying Party and are not controlled by the Federal PKI Policy Authority or the FBCA Operational Authority. Nonetheless, this CP contains some helpful guidance, set forth below, which Relying Parties may consider in making their decisions. Further, Relying Parties should review more detailed guidance governing the use of electronic signatures (which include the use of digital certificates) issued by the Office of Management and Budget implementing the Government Paperwork Elimination Act (Federal Register May 2000: Volume 65, Number 85, Page 25508), as well as more detailed subordinate guidance issued by other agencies pursuant to OMB direction (such as NIST Special Publication 800-25 covering the technical elements of using digital signatures, and electronic record retention guidance such as that provided by the National Archives and Records Administration at www.nara.gov/records/policy/gpea and www.cio.gov/docs/NARA_gpea).

1.4 CONTACT DETAILS

1.4.1 Specification administration organization

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

1.4.2 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.

1.4.3 Person determining Certification Practice Statement suitability for the policy

The Federal PKI Policy Authority shall approve the FBCA CPS. Entities are responsible for determining whether their CA CPSs conform to their CA CPs, and in particular, properly adhere to any policy mappings approved by the Federal PKI Policy Authority between the FBCA CP and the Entity Principal CA CP. Entities will be required to attest to such compliance periodically as established by the Federal PKI Policy Authority. Further, the Federal PKI Policy Authority reserves the right to audit Entity compliance as set forth in this CP and in the MOA between it and the Entity.

2. GENERAL PROVISIONS

2.1 OBLIGATIONS

The obligations described below pertain to the FBCA (and, by implication, the FBCA 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.

2.1.1 CA Obligations

The FBCA is obligated to comply with the requirements of this CP, the approved CPS, and any MOAs agreed upon between the FBCA and an Entity CA.

An Entity CA that issues certificates mapped by the Federal PKI Policy Authority to the FBCA policies defined in this CP for which the Federal PKI Policy Authority has authorized the issuance of an FBCA certificate containing those mappings to the Entity's Principal CA, shall comply with the requirements set forth in the MOA, as well as ensuring compliance with Entity CP requirements.

2.1.2 RA Obligations

An Entity RA who performs registration functions in support of an Entity CA described in 2.1.1 shall also comply with the requirements set forth in the MOA, and shall also include compliance with Entity CP requirements.

2.1.3 Subscriber Obligations

Subscribers who receive certificates from Entity CAs described in 2.1.1 or the FBCA shall also be required to comply with the requirements set forth in the MOA, and in the former case, shall also include compliance with Entity CP requirements.

2.1.4 Relying Party Obligations

The FBCA CP does not specify what steps a Relying Party should take to determine whether to rely upon a certificate. The Relying Party decides, pursuant to its own Entity's policies, what steps to take. The FBCA merely provides the tools needed to perform the trust path creation, validation, and certificate policy mappings which the Relying Party may wish to employ in its determination.

2.1.5 Repository Obligations

The FBCA 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.

2.1.6 Certificate Issuance to Non-US Government Parties

The FBCA may issue end-entity certificates to contractors and parties regulated by Federal agencies, for the convenience of the Government when those parties have a bona fide need to possess a certificate issued by the FBCA, as established by the Federal PKI Policy Authority. In each such case, a Memorandum of Agreement or similar instrument will be executed, and will contain whatever provisions are determined appropriate by the Federal PKI Policy Authority. Such provisions will address the issues delineated below.

2.2 LIABILITY

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 federal government. Any review by the FBCA of a non-federal entity's certificate policy is for the use of the FBCA 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 FBCA is not a substitute for due care and mapping of certificate policies by the non-federal entity.

2.3 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 consummate a transaction. Thus, one Entity may be willing to accept a Basic assurance level certificate for transactions of a financial value for which another Entity would require a High assurance level certificate. This is entirely at the discretion of the Entity as Relying Party and is likely to depend upon several factors in addition to the certificate assurance level (e.g., likelihood of fraud, other procedural controls, Entity-specific policy or statutorily imposed constraints).

2.3.1 Indemnification by Relying Parties and subscribers

No stipulation.

2.3.2 Fiduciary relationships

No stipulation.

2.3.3 Administrative processes

Administrative processes pertaining to this CP shall be determined by the FBCA Operational Authority pursuant to the agreement between it and the Federal PKI Policy Authority for the operation of the FBCA.

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1 Severability of Provisions, Survival, Merger, and Notice

Should it be determined that one section of this CP is incorrect or invalid, the other section of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 8.1

2.4.2 Dispute resolution procedures

The United States Government shall facilitate the resolution between entities when conflicts arise as a result of the use of the FBCA or certifications issued by the FBCA. This CP contemplates that an Entity may, for any reason, decline to accept the Federal PKI Policy Authority's mapping of its or another Entity's CP. In that case, the Entity is free to seek redress from the Federal CIO Council, or to pursue directly an agreement with another Entity concerning reliance on a particular Entity CP and the certificates issued thereunder.

2.5 FEES

The FBCA is currently being funded centrally; however, the FBCA Operational Authority reserves the right to charge a fee to each Entity in order to operate the FBCA. These fees will only be used to fund operation of the FBCA. The Federal PKI Policy Authority must approve the total amount and the fee mechanism.

2.6 PUBLICATION AND REPOSITORY

2.6.1 Publication of CA Information

The FBCA Operational Authority shall publish information concerning the FBCA necessary to support its use and operation. Publication by entities of information pertaining to their CAs shall be set forth in the MOA.

2.6.2 Frequency of Publication

FBCA and Entity certificates are published as specified in this and (for Entity certificates) the Entity CP. Certificate status information is published as specified in this (and for Entity certificates) the Entity CP.

2.6.3 Access controls

The FBCA Operational Authority shall protect any repository information not intended for public dissemination or modification. Public keys 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.

2.6.4 Repositories

See Section 2.1.5. Additionally, as set forth in the respective MOAs, entities who interoperate with the FBCA shall work to make their directories interoperate with the FBCA repository and/or other Entity repositories, and contain the information necessary to support interoperation of the Entity PKI domains that employ the FBCA for this purpose.

2.7 COMPLIANCE AUDIT

Entity CAs must have a compliance audit mechanism in place to ensure that the requirements of their CP/CPS and the provisions of the MOA are being implemented and enforced. The FBCA Operational Authority shall have a similar mechanism in place covering the requirements of this CP, the FBCA CPS and the MOAs signed with Entities.

2.7.1 Frequency of Entity Compliance Audit

The FBCA, Entity Principal CAs and RAs and their subordinate CAs and RAs shall be subject to a periodic compliance audit which is no less frequent than once per year for High and Medium Assurance, and no less than once every two years for Basic Assurance. There is no audit requirement for CAs and RAs operating at the Rudimentary or Test levels 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.

2.7.2 Identity/Qualifications of Compliance Auditor

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 primary responsibility.

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 FBCA Operational Authority shall identify the compliance auditor for the FBCA.

2.7.3 Compliance Auditor's Relationship to Audited Party

For both the FBCA and Entity CAs, the compliance auditor either shall be a private firm which 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.

2.7.4 Topics Covered by Compliance Audit

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.

The compliance audit of the FBCA CA shall verify that the FBCA CA is implementing all provisions of a CPS approved by the FPKI Policy Authority on the basis of meeting the requirements of this Certificate Policy.

In addition, each MOA between the FBCA Policy Authority and Entity PKIs shall provide for a mechanism to confirm that the Entity PKI is correctly implementing the MOA. The FBCA's compliance with MOAs is confirmed by incorporating MOA stipulations in the FBCA CPS, which is audited for compliance in accordance with the stipulations of this section.

2.7.5 Actions taken as a result of deficiency

The Federal PKI Policy Authority may determine that the FBCA or Entity CA is not complying with its obligations set forth in this CP or the respective MOA. When such a determination is made, the Federal PKI Policy Authority may suspend operation of the FBCA, or may direct the FBCA Operational Authority to cease interoperating with the affected Entity Principal CA (e.g., by revoking the certificate that the FBCA had issued to the Entity Principal CA), or may direct that other corrective actions be taken which allow interoperation to continue. When the compliance auditor finds a discrepancy between how the FBCA or Entity CA is designed or is being operated or maintained, and the requirements of this CP, the Entity CP, the MOA, or the applicable CPS, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;

- The compliance auditor shall notify the Entity of the discrepancy. The Entity shall notify the Federal PKI Policy Authority promptly;

- The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this CP and the MOA, 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 decide to halt temporarily operation of the FBCA, to revoke a certificate issued by the FBCA, or take other actions it deems appropriate. The Federal PKI Policy Authority will develop procedures for making and implementing such determinations.

2.7.6 Communication of Result

An Audit Compliance Report, including identification of corrective measures taken or being taken by the Entity or FBCA Operational Authority, shall be provided to the Federal PKI Policy Authority as set forth in section 2.7.1. Additionally, where necessary, the results shall be communicated as set forth in 2.7.5 above.

2.8 CONFIDENTIALITY

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.

2.9 INTELLECTUAL PROPERTY RIGHTS

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

3. IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

3.1.1 Types of names

The FBCA (and where required, Entity CAs) shall be able to generate and sign certificates that contain an X.500 Distinguished Name (DN); the X.500 DN may also contain domain component elements. Certificates issued to Entity CAs and RAs shall use the DN form, and have an assurance level equal to, or greater than, the highest level of assurance of the certificates the CA issues to subscribers or other CAs. Where DNs are required, subscribers shall have them assigned through their organizations, in accordance with a naming authority. Certificates may additionally assert an alternate name form subject to requirements set forth below intended to

ensure name uniqueness. The table below describes the naming requirements that apply to each level of assurance.

Test	To be established in the MOA (will depend upon testing circumstances)
Rudimentary	Non-Null Subject Name, or Null Subject Name if Alternative Subject Name is populated and marked critical
Basic	Non-Null Subject Name, and optional Alternative Subject Name if marked non-critical
Medium	X.500 Distinguished Name, and optional Alternative Subject Name if marked non-critical
High	X.500 Distinguished Name, and optional Alternative Subject Name if marked non-critical

3.1.2 Need for names to be meaningful

The identity certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates must identify the person or object to which they are assigned in a meaningful way.

When DNs are used, it is preferable that the common name represent the subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter). However, at the Rudimentary and Basic assurance levels, a DN for human subscribers may also be a pseudonym (such as a large number) as long as it respects name space uniqueness requirements.

The FBCA shall use DNs in certificates it issues. In the case where one Entity CA certifies another CA within that Entity, the certifying Entity CA must impose restrictions on the name space authorized in the subordinate Entity CA which are at least as restrictive as its own name constraints.

All certificates issued by the FBCA at the Medium 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 FBCA Operational Authority include such constraints for the FBCA certificates issued at the Test, Basic or Rudimentary levels if it deems appropriate.

3.1.3 Rules for interpreting various name forms

Rules for interpreting name forms shall be contained in the applicable certificate profile and are established by the Federal PKI Policy Authority. The authority responsible for Entity CA name space control shall be identified in the respective CP.

3.1.4 Uniqueness of names

Name uniqueness across the FPKI must be enforced. The FBCA, Entity CAs and RAs shall enforce name uniqueness within the X.500 name space which they have been authorized. When name forms other than a DN (e.g., an electronic mail address or DNS name) are used, they too must be allocated such that name uniqueness across the FPKI is ensured.

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?).

3.1.5 Name claim dispute resolution procedure

The Federal PKI Policy Authority shall resolve any name collisions brought to its attention that may affect interoperability using the FBCA.

3.1.6 Recognition, authentication and role of trademarks

No stipulation.

3.1.7 Method to prove possession of private key

In all cases where the party named in a certificate generates its own keys, that party shall be required to prove possession of the private key which corresponds to the public key in the certificate request. For signature keys, this may be done by the entity using its private key to sign a value and providing that value to the 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 directly on the party's hardware or software token, or in a key generator that benignly transfers the key to the party's token, then the party is deemed to be in possession of the private key at the time of generation or transfer. If the party is not in possession of the token when the key is generated, then the token (e.g., a smartcard or a PKCS

#12 encoded message) shall be delivered to the subject via an accountable method (see Section 6.1.2).

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

3.1.8 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 FBCA 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.

3.1.9 Authentication of individual identity

For Subscribers, the FBCA or Entity CA shall ensure that the applicant's identity information is verified and checked in accordance with the applicable CP and CPS. The FBCA, Entity CAs and/or RAs shall ensure that the applicant's identity information and public key are properly bound. Additionally, the FBCA, Entity CAs and/or RAs shall record the process that was followed for issuance of each certificate. Process information shall depend upon the certificate level of assurance and shall be addressed in the FBCA or Entity CPS. The process documentation and authentication requirements shall include the following depending upon the level of assurance (as set forth below):

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the Subscriber (including verification of any roles or authorizations that apply to that certificate) as required by the applicable certificate policy which may be met by establishing how the applicant is known to the verifier as required by this certificate policy;
- A unique identifying number from the ID of the verifier and, if in-person identity proofing is done, from the ID of the applicant;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature. If in-person identity proofing is done, this shall be performed in the presence of the person performing the identity authentication.

For All Levels: If an Applicant is unable to perform face-to-face registration alone (e.g., a network device), the applicant shall 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.

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

Assurance Level	Identification Requirements
Test	To be established in the MOA with the Entity (will depend upon test circumstances)
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 comparison with trusted information in a data base of user-supplied information (obtained and/or checked electronically, through other trusted means (such as the U.S. mail), or in-person); or by attestation of a supervisor, or administrative or information security officer, or a person certified by a state or Federal Entity as being authorized to confirm identities.
Medium	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)

3.1.10 Authentication of component identities

Some computing and communications components (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases, the component must have a human sponsor. The PKI 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 3.1.9.

3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY

3.2.1 Certificate Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtains new keys and re-establishes its identity. Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period.

New certificates will need to be issued to Principal CAs by the FBCA when the FBCA re-keys, and when Principal CAs re-key. Upon re-key of either of these components, the FBCA shall identify and authenticate Principal CAs either by:

(a) Performing the initial registration identification process defined in Section 3.1, or

(b) If it has been less than three years since a Principal CA was identified as required in Section 3.1, using the currently valid certificate issued to the Principal CA by the FBCA.

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

Assurance Level	Routine Rekey Identity Requirements for Subscriber Signature and Encryption Certificates
Test	To be determined in the MOA with the Entity
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	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

3.2.2 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but a new, extended validity period and a new serial number. Certificates may be renewed in order to reduce the size of CRLs. 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. Thus, an Entity CA may choose to create a certificate good for one year, renew it twice (each for a one-year period), then re-key at the end of the third year.

3.2.3 Certificate Update

Updating a certificate means creating a new certificate that has the same or a different key and a different serial number, and that it differs in one or more other fields, from the old certificate. For example, an Entity CA may choose to update a certificate of a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

Further, if an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or other designated agent (as set forth above) in order for an updated certificate having the new name to be issued.

Finally, when a CA updates its private signature key and thus generates a new public key, the CA shall notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed. For self-signed ("root") certificates, such certificates shall be conveyed to users in a secure fashion to preclude malicious substitution attacks.

3.3 OBTAINING A NEW CERTIFICATE 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 3.1 to obtain a new certificate. This applies to Entity CAs.

3.4 REVOCATION REQUEST

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.

4. OPERATIONAL REQUIREMENTS

4.1 APPLICATION FOR A CERTIFICATE

This paragraph applies to entities seeking FBCA certificates for their Principal CAs. The Federal PKI Policy Authority shall establish procedures for entities to use in applying for a certificate from the FBCA and then publish those procedures. 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 applicant Entity, shall instruct the FBCA Operational Authority to issue the certificate to the Entity. The Entity Principal CA shall have a distinguished name as defined in X.509, and that shall be placed in the certificate subject name field. The common names asserted in the FBCA issued certificates shall be the official names of the Entity affiliated with the cross-certified CA, or an officially recognized acronym (such as FBI, DEA, DOJ) meeting the requirement of a DN.

Requests by an Entity for an FBCA certificate to be issued to one or more of its Entity Principal CAs shall be submitted to the Federal PKI Policy Authority using a procedure and application form developed by the Federal PKI Policy Authority and made available to all entities. The application shall be accompanied by a CP and a CPS written to the format of the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [RFC2527]. Additionally, the application shall propose a mapping between the levels of assurance expressed in the Entity's CP, and those in the FBCA.

The Federal PKI Policy Authority will evaluate the application in accordance with procedures that it will develop and publish, and make a determination regarding whether or not to issue the requested certificate(s), and what policy mappings to express in the certificate(s). The Federal PKI Policy Authority and the applicant Entity will then enter into a MOA setting forth their respective responsibilities, and the Federal PKI Policy Authority will direct the FBCA Operational Authority to issue the certificate(s). 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.

4.1.1 Delivery of public key for certificate issuance

Public keys must be delivered for certificate issuance in a way that binds the applicant Entity's verified identification to the public key. For all levels of assurance, this binding may be accomplished using cryptography. If cryptography is used, it must be at least as strong as that employed in certificate issuance. Additionally, for Medium and Basic Assurance, this binding may also be accomplished using non-cryptographic physical and procedural mechanisms. These mechanisms may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a hardware or software cryptographic module to a certificate issuer for local key generation at the point of certificate issuance or request. For Rudimentary Assurance, no trusted delivery mechanism is required. For Test Assurance, the mechanism shall be set forth in the MOA. In all cases, the method used for public key delivery shall be set forth in a CPS.

In those cases where public/private key pairs are generated by the FBCA or Entity CA on behalf of the Subscriber, the FBCA or Entity CA (respectively) shall implement secure mechanisms to ensure that the token on which the public/private key pair is held is securely sent to the proper Subscriber. The FBCA or Entity CA (respectively) shall also implement procedures to ensure that the token is not activated by an unauthorized entity.

4.2 CERTIFICATE ISSUANCE

Upon receiving a request for a certificate, the Entity CA or RA shall respond in accordance with the requirements set forth in its CP and CPS.

The certificate request may contain an already built ("to-be-signed") certificate. This certificate will not be signed until the process set forth in the CP and CPS has been met.

While the Subscriber may do most of the data entry, it is still the responsibility of the RA to verify that the information is correct and accurate. This may be accomplished through a system approach linking trusted databases containing personnel information, other equivalent authenticated mechanisms, or through personal contact with the Subscriber's sponsoring organization. If databases are used to confirm Subscriber information, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance of the certificate being sought.

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

4.2.1 Delivery of Subscriber's private key to Subscriber

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

deliver the private key. If the key is generated elsewhere, then the module must be delivered to the Subscriber. Accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it. The Subscriber shall acknowledge receipt of the module. Under no circumstances shall anyone other than the Subscriber have substantive knowledge of or control over private signing keys after generation of the key. 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. Hardware tokens containing FBCA or Entity CA private signature keys may be backed-up in accordance with security audit requirements defined Section 4.5.1.

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. In these cases:

- An 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).

4.2.2 FBCA public key delivery and use

The public key of the FBCA must be available for certification trust paths to be created and verified. That key will appear in the form of a cross-certificate issued by an Entity Principal CA to the FBCA. In order to extract the key from that certificate with confidence that it has not been altered, the Entity Principal CA must ensure that its users have its self-signed root certificate in a trustworthy fashion. Such a self-signed root certificate is sometimes called a Trusted Certificate. Acceptable methods for Trusted Certificate delivery include but are not limited to:

- The CA loading a Trusted Certificate onto tokens delivered to Relying Parties via secure mechanisms;

- Secure distribution of Trusted Certificates through secure out-of-band mechanisms;

- Comparison of certificate hashes or fingerprints against Trusted Certificate hashes or fingerprints made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and

- Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.

4.3 CERTIFICATE ACCEPTANCE

The MOA shall set forth responsibilities of respective Entities and the Federal PKI Policy Authority before the Federal PKI Policy Authority authorizes issuance of an FBCA certificate to the Entity Principal CA. Once that certificate has been issued, its acceptance by the Entity commences interoperability with the FBCA and thus triggers its obligations under the MOA and hence this CP.

For Medium 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. For Rudimentary Assurance level, there are no requirements. For Test Assurance level, the requirements shall be as set forth in the MOA.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Circumstances for revocation of a certificate issued by the FBCA or Entity CA

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

- The first circumstance is when the Federal 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

- Chair, Federal PKI Steering Committee, or

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

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

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.

4.4.1.1 Who can request revocation of a certificate issued by the FBCA or Entity CA

An FBCA certificate may be revoked upon direction of the Federal PKI Policy Authority or upon an authenticated request by a previously 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).

The process for requesting revocation of a Subscriber certificate issued by an Entity CA shall be set forth in the Entity CP or CPS. Revocation normally will proceed once:

- An Entity receives sufficient evidence of compromise or loss of the subscriber's corresponding private key,

- An authenticated request is made to the Entity by the holder of the private key, or

- Someone in his or her supervisory chain, or an officially designated administrative or information security officer, makes an authenticated request for revocation.

4.4.1.2 Procedure for revocation request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). Only the Federal PKI Policy Authority or a previously delegated official of the Agency responsible for the Principal CA may direct the Operational Authority to revoke certificates issued by the FBCA. Note that an Entity Principal CA may always revoke the certificate it has issued to the FBCA, thus terminating interoperability with the FBCA without any Federal PKI Policy Authority action.

Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties. In particular, if the revocation is being requested for reason of key compromise or suspected fraudulent use, then the Subscriber's or the RA's revocation request must so indicate. If a RA performs this on behalf of a Subscriber, a formal, signed

message format known to the CA shall be employed. All requests shall be authenticated; for signed requests from the certificate subject, or from an RA, verification of the signature is sufficient.

Upon receipt of a revocation request involving an FBCA certificate, the FBCA 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 FBCA Operational Authority to revoke the certificate by placing its serial number and other identifying information on a CARL/CRL and then post the CARL/CRL in the FBCA repository, in addition to any other revocation mechanisms used. Practice Note: Entity CAs may use OCSP to distribute status information instead of CARL/CRL.

For PKI implementations using 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 hardware tokens are zeroized or destroyed, revocation of the associated certificates is recommended.

4.4.1.3 Revocation of a Certificate Issued by the FBCA

Revocation of an FBCA certificate shall be accomplished by the generation and publication into the FBCA repository of status information that cites the certificate as revoked, and identifies the certificate being revoked and the reason for the revocation in accordance with *CARL/CRL Issue Frequency,* Section 4.4.3.1. Further, and separate from the publication of the status information, prompt oral or electronic notification shall be given by the FBCA Operational Authority to previously designated officials in all entities having a Principal CA with which the FBCA interoperates.

4.4.1.4 Revocation of a Certificate Issued by an Entity CA

Revocation shall take effect upon the publication of status information (identifying the reason for the revocation, which may include loss, compromise, or termination of employment) within the time limits as specified in Section 4.4.3 (starting from the time the request is authenticated or sufficient evidence of compromise or loss is received). Information about a revoked certificate

shall remain in the status information until the certificate expires. A certificate may be omitted from CRLs issued after it expires.

4.4.1.5 Revocation Request Grace Period

There is no revocation grace period for the FBCA. Grace periods for Entity CAs shall be set forth in their respective CPs or CPSs.

4.4.2 Suspension

Suspension shall not be used by the FBCA.

4.4.3 Certification Authority Revocation Lists / Certificate Revocation Lists

All Entity CAs shall issue Certification Authority Revocation Lists (CARLs) and Certificate Revocation Lists (CRL). To the extent practical, the contents of CARLs and CRLs shall be checked before issuance to ensure that all information is correct. This may be done using software which scans the CARLs and CRLs looking for any evidence of an improperly manufactured CARL or CRL.

4.4.3.1 CARL/CRL Issuance Frequency

CARLs and CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below. The FBCA shall ensure that superseded certificate status information is removed from the repository upon posting of the latest certificate status information.

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote (laptop) operation. Entities shall coordinate with the repositories to which they post certificate status information to reduce latency between creation and availability. Superseded certificate status information shall be removed from the repository system upon posting of the latest certificate status information.

The following table provides CARL/CRL issuance requirements.

Assurance Level	CARL/CRL Issuance Frequency for Entity CAs (Routine)	CARL/CRL Issuance for Entity CAs (Loss or Compromise of Private Key)
Test	As set forth in MOA	As set forth in MOA
Rudimentary	Not Applicable	Not Applicable
Basic	Entity determined	Within 24 Hours of Notification

Assurance Level	CARL/CRL Issuance Frequency for Entity CAs (Routine)	CARL/CRL Issuance for Entity CAs (Loss or Compromise of Private Key)
Medium	At Least Once Each Day	Within 18 Hours of Notification
High	At Least Once Each Day	Within 6 Hours of Notification

4.4.3.2 CARL/CRL Checking requirements

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.

4.4.4 On-line Revocation / Status checking availability

In addition to CARL/CRLs, Entity CAs and Relying Party client software may optionally support on-line status checking. 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 4.4.3.1. Client software using on-line status checking need not obtain or process CARL/CRLs. The Federal PKI Policy Authority will determine when and under what circumstances the FBCA Operational Authority will provide on-line status checking of FBCA certificates.

4.4.5 Other forms of revocation advertisements available

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

4.4.6 Checking requirements for other forms of revocation advertisements

No stipulation.

4.4.7 Special requirements related to key compromise

In the event of an Entity Principal CA private key compromise or loss, a CARL shall be published at the earliest feasible time by the FBCA Operational Authority. Entity CAs operating at the High Assurance level and using reason codes must have the ability to transition any reason code to key compromise.

4.5 SECURITY AUDIT PROCEDURE

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 4.6.2.

4.5.1 Types of Events Recorded

Detailed audit requirements are listed in the table below. All security auditing capabilities of the FBCA or Entity CA operating system and PKI CA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically 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 when executing the FBCA or Entity CA's signing process
- A success or failure indicator when performing certificate revocation
- The identity of the entity and/or operator (of the FBCA or Entity CA) that caused the event.

Auditable Event	Rudimentary	Basic	Medium	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
IDENTIFICATION AND AUTHENTICATION				
Successful and unsuccessful attempts to assume a role		X	X	X
Change in the value of maximum authentication attempts		X	X	X

Auditable Event	Rudimentary	Basic	Medium	High
Maximum number of unsuccessful 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
KEY GENERATION				
Whenever the FBCA or Entity 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 FBCA or Entity 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
PRIVATE KEY EXPORT				
The export of private keys (keys used for a single session or message are excluded)	X	X	X	X

Auditable Event	Rudimentary	Basic	Medium	High
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
FBCA OR ENTITY CA CONFIGURATION				
Any security-relevant changes to the configuration of the FBCA or Entity CA		X	X	X
ACCOUNT ADMINISTRATION				
Roles and users are added or deleted	X	X	X	X
The access control privileges of a user account or a role are modified	X	X	X	X
CERTIFICATE PROFILE MANAGEMENT				
All changes to the certificate profile	X	X	X	X
REVOCATION PROFILE MANAGEMENT				
All changes to the revocation profile		X	X	X

Auditable Event	Rudimentary	Basic	Medium	High
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT				
All changes to the certificate revocation list profile		X	X	X
MISCELLANEOUS				
Installation of the Operating System		X	X	X
Installation of the FBCA or Entity 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 FBCA or Entity CA Apps		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 FBCA or Entity CA internal database		X	X	X
Restoring FBCA or Entity 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 FBCA or Entity CA internal database			X	X
All certificate compromise notification requests		X	X	X
Loading tokens with certificates			X	X

Auditable Event	Rudimentary	Basic	Medium	High
Shipment of Tokens			X	X
Zeroizing tokens		X	X	X
Rekey of the FBCA or Entity 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 FBCA or Entity CA			X	X
Access to the FBCA or Entity CA server			X	X
Known or suspected violations of physical security		X	X	X
ANOMALIES				
Software Error conditions		X	X	X
Software check integrity failures		X	X	X
Receipt of improper messages			X	X
Misrouted messages			X	X
Network attacks (suspected or confirmed)		X	X	X
Equipment failure	X	X	X	X

Auditable Event	Rudimentary	Basic	Medium	High
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

4.5.2 Frequency of processing data

Audit logs shall be reviewed in accordance to the table below. The FBCA OA shall explain all significant events in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

Assurance Level	Review Audit Log
Test	As set forth in the MOA
Rudimentary	Only required for cause
Basic	Only required for cause
Medium	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

Assurance Level	Review Audit Log
	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.

4.5.3 Retention period for security audit data

Audit logs shall be retained onsite for at least two months 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.

4.5.4 Protection of security audit data

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

- only authorized people have read access to the logs;
- only authorized people may archive audit logs; and,
- audit logs are not modified.

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). Audit logs shall be moved to a safe, secure storage location separate from the FBCA 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.

4.5.5 Security Audit data 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 in accordance with the CPS on a monthly basis.

4.5.6 Security Audit collection system (internal vs. external)

The audit log collection system may or may not be external to the FBCA or Entity CA system. Audit processes shall be invoked at system startup, and cease only at system 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 FBCA Operational

Authority Administrator (or comparable Entity authority) shall determine whether to suspend FBCA operation (or Entity CA operation respectively) until the problem is remedied.

4.5.7 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.

4.5.8 Vulnerability Assessments

The Operational Authority will perform routine self assessments of security controls.

4.6 RECORDS ARCHIVAL

4.6.1 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 (requirements for Test Assurance shall be set forth in the MOA):

Data To Be Archived	Rudimentary	Basic	Medium	High
FBCA or Entity 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

Data To Be Archived	Rudimentary	Basic	Medium	High
Documentation of receipt of tokens		X	X	X
All certificates issued or published	X	X	X	X
Record of FBCA or Entity CA Re-key	X	X	X	X
All CARLs and 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

4.6.2 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
Test	As set forth in MOA
Rudimentary	7 Years & 6 Months
Basic	7 Years & 6 Months
Medium	10 Years & 6 Months
High	20 Years & 6 Months

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 FBCA 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.

4.6.3 Protection of archive

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

4.6.4 Archive backup procedures

No stipulation.

4.6.5 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.

4.6.6 Archive collection system (internal or external)

No stipulation.

4.6.7 Procedures to obtain and verify archive information

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

4.7 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, certificate 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 contain certificates signed with that key, then the old key must be retained and protected.

The FBCA's signing key shall have a validity period of one-half the lifetime of its corresponding certificate. The certificate lifetime will not be more than six years.

Entities may select signing key validity periods for their CAs that differ from the values that do not correspond to one-half the validity period of the corresponding certificate. In selecting the signing key validity period, entities shall consider the length of the signing key, how it is protected and controlled, whether their PKI is in a hierarchical or mesh arrangement, and other factors.

4.8 COMPROMISE AND DISASTER RECOVERY

4.8.1 Computing resources, software, and/or data are corrupted

If FBCA or Entity CA equipment is damaged or rendered inoperative, but the FBCA or Entity CA signature keys are not destroyed, FBCA or Entity CA operation shall be reestablished as quickly as possible, giving priority to the ability to generate certificate status information.

4.8.2 FBCA or Entity CA signature keys are revoked

If the FBCA or Entity CA cannot issue a CARL/CRL prior to the time specified in the next update field of its currently valid CARL/CRL, then the Federal PKI Policy Authority and all of its members shall be securely notified at the earliest feasible time in a fashion set forth in the MOA. This will allow member entities to protect their interests as Relying Parties. The Federal PKI Policy Authority shall determine whether to revoke the FBCA certificate issued to the Entity CA. The FBCA or Entity Principal CA shall reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS. The FBCA 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.

4.8.3 FBCA or Entity CA signature keys are compromised

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 securely notified at the earliest feasible time (so that entities may issue CARLs revoking any cross-certificates issued to the FBCA);

- 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 FBCA 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.

4.8.4 Secure Facility impaired after a Natural or Other type of Disaster

In the case of a disaster whereby the FBCA installation is physically damaged and all copies of the FBCA signature key are destroyed as a result, the Federal PKI Policy Authority and all of its member entities shall be securely notified at the earliest feasible time, and the Federal PKI Policy Authority shall take whatever action it deems appropriate.

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

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.

4.9 CA 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 FBCA shall provide archived data to a Federal PKI Policy Authority approved 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.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS FOR THE FBCA OR ENTITY CA

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.

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.

5.1.1 Site location and 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

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

These 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 intended to:

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

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

- Be manually or electronically monitored 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

Physical security requirements pertaining to CAs at the Test Assurance level shall be as set forth in the MOA.

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

A security check of the facility housing the 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.

5.1.3 Electrical Power

The FBCA and Entity CAs (operating at the Basic Assurance level or higher) shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and 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). Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the FBCA and Entity CAs.

5.1.7 Waste disposal

No stipulation.

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, described in the respective CPS. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an offsite location (separate from the FBCA and 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 and Entity CA.

5.2 PROCEDURAL CONTROLS FOR THE FBCA AND ENTITY CA

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 FBCA may encompass CA products from several vendors, and Entity CAs may also use products from different vendors. Entities are encouraged to closely examine products before selecting them, and to evaluate those products against the Entity's mission requirements (including the potential for covert investigation of internal matters), and then to consider the roles set forth below to ensure that Entity security functions are met. This is particularly important because different commercial products support somewhat different roles, and use different mechanisms for registering or enrolling subscribers and issuing certificates. The requirements of this policy are therefore drawn in terms or four, somewhat abstract, roles (Note: the information derives from the Certificate Issuing and Management Components Protection Profile being developed by NIST.) :

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 view and maintain audit logs.
4. *Operator* – authorized to perform system backup and recovery.

5.2.1.1 Administrator

The administrator role is responsible for:

- installation, configuration, and maintenance of the 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;
- 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 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.

The separation of roles for the FBCA and Entity CAs shall be as follows:

Assurance Level	**Role Separation Rules**
Test	As set forth in the MOA.
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	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, but any individual may assume the Operator role. The CA system shall identify and authenticate its users and shall ensure that no user identity can: • Assume both the Administrator and Officer roles • Assume both the Administrator and Auditor roles • Assume both the Auditor and Officer roles. No individual shall have more than one identity.

The FBCA shall operate at the High Assurance level.

5.2.3 Number of persons required per task

To best ensure the integrity of the FBCA equipment and operation, no individual will be assigned more than one trusted role. The separation provides a set of checks and balances over the FBCA operation.

Under no circumstances shall an FBCA auditor perform the functions of another FBCA role.

The requirements of this section apply to Entity CAs operating at the high level.

5.2.4 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.

5.3 PERSONNEL CONTROLS

5.3.1 Background, qualifications, experience, and 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 FBCA Operational Authority.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and must be U.S. citizens. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA shall be set forth in the Entity CA CPS.

FBCA Operational Authority personnel shall hold TOP SECRET security clearances. Entity CA personnel may hold security clearances if deemed appropriate by their respective Entity.

5.3.2 Background check procedures

Entity background check procedures shall be described in the CPS and shall demonstrate that Entity requirements set forth in Section 5.3.1 are met.

5.3.3 Training Requirements

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

- CA/RA security principles and mechanisms
- All PKI software versions in use on the CA system
- All PKI duties they are expected to perform
- Disaster recovery and business continuity procedures.

5.3.4 Retraining frequency and 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.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

The Federal PKI Policy Authority or Entity CA Policy Authority shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the FBCA or its repository not authorized in this CP, the FBCA CPS, or other procedures published by the FBCA Operational Authority.

5.3.7 Contracting personnel requirements

Contractor personnel employed to perform functions pertaining to the FBCA or an Entity CA shall meet applicable requirements set forth in the FBCA CP or Entity CP as determined by the FBCA Operational Authority or the corresponding Entity.

5.3.8 Documentation supplied to personnel

The FBCA and Entity CA shall make available to its CA and RA personnel the certificate policies it supports, relevant parts of the CPS, and any relevant statutes, policies or contracts. Documentation shall be maintained identifying all personnel who received training and the level of training completed.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 FBCA and CA key pair generation

Cryptographic keying material for certificates issued by the FBCA or Entity CAs shall be generated in FIPS 140 validated cryptographic modules. 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 or Medium), or Security Level 3 (for High). Requirements for Test Assurance shall be set forth in the MOA.

The FBCA and Entity CAs must document their key generation procedure in their CPSs, and generate auditable evidence that the documented 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. For High and Medium Assurance the process shall be validated by an independent third party.

6.1.2 Private Key Delivery to Subscriber

The Entity CA generates its own key pair and therefore does not need private key delivery. Entity CA Subscribers will usually generate their own signature keys and thus will not require delivery; where signature keys are generated by the Entity CA, they will be delivered in accordance with the requirements of this CP and the applicable Entity CP/CPS. For encryption keys, delivery of the private key to the Subscriber (or, if the Subscriber generates the encryption

key pair, delivery by the Subscriber to the Entity) shall be in accordance with the requirements of this CP and the applicable Entity CP/CPS.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys shall be delivered to the certificate issuer in an authenticated manner set forth in the CA CPS. This is usually via a certificate electronic request message from an RA, but it may also be done through other secure electronic mechanisms. Further, it may be accomplished via secure non-electronic means. These means may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a token to a certificate issuer for local key generation at the point of certificate issuance or request. If off-line means are used, they shall include identity checking as set forth in this CP and shall also ensure that proof of possession of the corresponding private key is accomplished.

6.1.4 FBCA certificates and public key availability and delivery to Principal CAs

The FBCA shall post the certificates it issues in the FBCA repository. An Entity Principal CA will also be required to issue a certificate to the FBCA and post it to the FBCA repository concurrent with the issuance of an FBCA certificate to the Entity Principal CA. A copy of the FBCA public key shall then be available in an Entity Principal CA certificate, which facilitates trust path validation. For an Entity Principal CA to issue cross-certificates to the FBCA, the FBCA shall transport its public key to the Entity Principal CA in a secure, out-of-band fashion to effect certificate issuance.

6.1.5 Key sizes

All FIPS-approved signature algorithms shall be considered acceptable. If the Federal PKI Policy Authority determines that the security of a particular algorithm may be compromised, it may require the FBCA and Entity CAs to revoke the affected certificates (in the latter case, in order to support continued compliance with the MOA).

All certificates issued by the FBCA shall use at least 1024 bit RSA or DSA, with Secure Hash Algorithm version 1 (SHA-1) (or better), in accordance with FIPS 186. Certificates issued by Entity CAs shall use at least 1024 bit RSA or DSA, with SHA-1 (or better), in accordance with FIPS 186. Use by the FBCA or an Entity of SSL 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.

6.1.6 Public key parameters generation

Public key parameters prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186.

6.1.7 Parameter quality checking

Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186 or a more stringent test if specified by the Federal PKI Policy Authority.

6.1.8 Hardware/Software Subscriber key generation

For subscribers, software or hardware shall be used to generate pseudo-random numbers, key pairs and symmetric keys, as set forth in the table below. Any pseudo-random numbers used for key generation material shall be generated by a FIPS approved method.

Assurance Level	Key Generation Mechanism
Test	As set forth in the MOA
Rudimentary	Software or Hardware
Basic	Software or Hardware
Medium	Software or Hardware
High	Hardware only

6.1.9 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. In particular, certificates to be used for digital signatures (including authentication) shall set the *digitalsignature* and *nonrepudiation* bits. Certificates to be used for data encryption shall set the *dataencryption* bit. FBCA certificates shall set two key usage bits: *cRLSign* and *CertSign*. This restriction is not intended to prohibit use of protocols (like the Secure Sockets Layer) that provide authenticated connections using key management certificates.

Test, Rudimentary, Basic and Medium Assurance Level certificates may include a single key for use with encryption and signature in support of legacy Secure Multipurpose Internet Mail Extensions (S/MIME) 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 data encryption and one for digital signature and authentication.

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for cryptographic module

The relevant standard for cryptographic modules is FIPS PUB 140-1, *Security Requirements for Cryptographic Modules*. The Federal PKI Policy Authority may determine that other comparable validation, certification, or verification standards are sufficient. These standards will be published by the Federal PKI Policy Authority. Cryptographic modules shall be validated to the FIPS 140-1 level identified in this section, or validated, certified, or verified to requirements published by the Federal PKI Policy Authority. Additionally, the Federal PKI Policy Authority reserves the right to review technical documentation associated with any cryptomodules under consideration for use by the FBCA.

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

Assurance Level	Latest version of FIPS 140 series	Federal Bridge Certification Authority	Certification Authority	Subscriber	Registration Authority
Test	MOA	MOA	MOA	MOA	MOA
Rudimentary	N/A	Level 3 (Hardware)	Level 1 (Hardware or Software)	N/A	Level 1 (Hardware or Software)
Basic	Required	Level 3 (Hardware)	Level 2 (Hardware or Software)	Level 1 (Hardware or Software)	Level 1 (Hardware or Software)
Medium	Required	Level 3 (Hardware)	Level 2 (Hardware)	Level 1 (Hardware or Software)	Level 2 (Hardware)
High	Required	Level 3 (Hardware)	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

6.2.2 FBCA private key multi-person control

Use of the FBCA private signing key shall require action by multiple persons as set forth in Section 5 of this CP.

6.2.3 Key Escrow of FBCA and Entity CA private signature key

Under no circumstances shall the FBCA or an Entity CA signature keys used to support non-repudiation services be escrowed by a third party.

6.2.3.1 Escrow of Entity 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.

6.2.4 Private Key Backup

6.2.4.1 Backup of FBCA and Entity CA private signature key

If backed up, the FBCA and Entity CA private signature keys shall be backed up under the same multi-person control as the original signature key. A controlled copy or copies of the CA signature key may be stored at various FBCA or Entity CA locations, as long as all copies of the signature key are controlled, accounted for and protected from unauthorized access. These multiple copies may be kept at the FBCA or CA backup location under the same multiple person access rules and storage requirements that apply to operational and backup signature keys. Procedures for FBCA private signature key backup shall be included in the FBCA CPS.

6.2.4.2 Backup of subscriber private signature key

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the FBCA mediumAssurance, basicAssurance, or rudimentaryAssurance policies (or an entity policy which maps to these policies) may be backed up or copied, but must be held in the Subscriber's control.

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the FBCA highAssurance policy, or an entity policy which maps to the FBCA highAssurance policy may not be backed up or copied.

6.2.5 Private Key Archival

Private signature keys shall not be escrowed or archived.

6.2.6 Private key entry into 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.

6.2.7 Method of activating private keys

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).

6.2.8 Methods of deactivating private keys

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. 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.

6.2.9 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.

6.3 GOOD PRACTICES REGARDING KEY-PAIR MANAGEMENT

It is technically possible to use the same key-pair for both digital signature and confidentiality. However, this CP discourages that condition for Rudimentary, Basic and Medium, except to support legacy applications as defined in Section 6.1.9. A single dual-use key pair is prohibited for High assurance implementations, where one key-pair shall be used for digital signature/authentication, and a separate key-pair shall be used for confidentiality.

A subscriber's key-pair that is used for digital signatures shall never be escrowed, archived or backed up, because a subscriber can repudiate a transaction if there is a copy of his or her digital signature private key in existence.

For information that is encrypted, the subscriber shall use his or her private encryption (confidentiality) key to decrypt the information. If that private key is lost or destroyed, or if the subscriber departs the Entity without relinquishing the private key, or acts maliciously, there is no way to decrypt the information. Thus, for business continuity reasons, an Entity must be able to escrow, backup or archive private keys used for decrypting files and e-mails, while not escrowing, backing up or archiving key-pairs used for authentication. This means that two separate key pairs need to be employed.

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2 Usage Periods for the Public and Private Keys

The FBCA private signing keys will be used to sign certificates for not more than one-half of the certificate lifetime. The certificate lifetime will be valid for not more than 6 years.

6.4 ACTIVATION DATA

6.4.1 Activation data generation and installation

The activation data used to unlock FBCA, Entity CA or subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. For Rudimentary, Basic, and Medium assurance levels, activation data may be user selected. For the High assurance level, it shall either entail the use of biometric data or satisfy the policy enforced at/by the cryptographic module. Where passwords are used as activation data, the password data shall be generated in conformance with FIPS-112. 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. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation data protection

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

The following computer security 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

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

6.5.2 Computer Security Rating

No Stipulation.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System development controls

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

- Use software that has been designed and developed under a formal, documented development methodology.
- Hardware and software procured to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- Hardware and software developed specifically for the CA shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the CA physical location.

- 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 and RA equipment. Only applications required to perform the operation of the CA shall be obtained from sources authorized by local policy. RA hardware and software shall be scanned for malicious code on first use and periodically thereafter.

- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and 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 FBCA Operational Authority at least weekly (e.g., in conjunction with CARL publication).

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 NETWORK SECURITY CONTROLS

The FBCA and FBCA Internal Directory shall be connected within the Bridge membrane. The Bridge membrane will be connected with the FBCA Border directory through a firewall. The FBCA Border Directory shall be connected to the Internet and provide continuous service (except, when necessary, for brief periods of maintenance or backup). Information will be transported from the Internal Directory to the Border directory using automatic mechanisms, and all such information will be digitally signed (certificates and CARLs). The firewall will restrict connections to those initiated by the Internet directory to the Border directory. The FBCA Border Directory shall be protected by a network guard, firewall or filtering router to guard against denial of service and intrusion attacks.

Entity CAs shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of guards, firewalls and filtering routers. Unused network ports and services shall be turned off. Any network software present shall be necessary to the functioning of the Entity CA.

The FBCA or Entity CPS shall define the network protocols and mechanisms required for the operation of the FBCA Border Directory or Entity CA. Any boundary control devices used to

protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Requirements for cryptographic modules are as stated above in Section 6.2

7. CERTIFICATE AND CARL/CRL PROFILES

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

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles. These profiles are written to prescribe an appropriate amount of control over an infrastructure, yet be flexible enough to meet the needs of the various CAs and communities. Certificates issued by the FBCA shall comply with *Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile* [FPKI-Prof]. Certificates issued by Entity PKI's operating at High and Medium shall comply with FPKI-Prof. Certificates issued by Entity PKI's operating at Basic and Rudimentary shall comply with RFC2459. Whenever private extensions are used, they shall be identified in a CPS. Critical private extensions shall be interoperable in their intended community of use.

7.1.3 Algorithm object identifiers

Certificates issued under this CP shall use the following OIDs for signatures:

id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

Certificates under this CP will use the following OIDs for identifying the algorithm for which the subject key was generated:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

7.1.4 Name forms

Where required as set forth above, the subject and issuer fields of the base certificate shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by [RFC2459].

7.1.5 Name constraints

FBCA shall assert name constraints in certificates issued to PCA's appropriate for the PKI being certified.

7.1.6 Certificate policy object identifier

Certificates issued under this CP shall assert the OID appropriate to the level of assurance with which it was issued.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

Certificates issued under this CP shall not contain policy qualifiers.

7.1.9 Processing semantics for the critical certificate policy extension

Processing semantics for the critical certificate policy extension used by the FBCA shall conform to [FPKI-PROF].

7.2 CARL/CRL PROFILE

7.2.1 Version numbers

The FBCA shall issue X.509 version two (2) CARLs/CRLs. Entity CAs shall also issue X509 version two (2) CARLs/CRLs.

7.2.2 CARL and CRL entry extensions

Detailed CARL/CRL profiles addressing the use of each extension shall conform to [FPKI-PROF].

8. SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

The Federal PKI Policy Authority shall review this CP at least once every year. The Federal PKI Policy Authority shall maintain and publish a Certificate Policy Plan that describes anticipated changes to this CP. Errors, updates, or suggested changes to this CP shall be communicated to every Entity Principal CA and Subscriber. Such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

All policy changes under consideration by the Federal PKI Policy Authority shall be disseminated to interested parties. All interested parties shall provide their comments to the Federal PKI Policy Authority in a fashion to be prescribed by the Federal PKI Policy Authority.

In evaluating the need for changes to this CP and the Object Identifiers it contains, the Federal PKI Policy Authority will be guided by the language of RFC 2527 which states (in section 4.8.1):

> *It will occasionally be necessary to change certificate policies and Certification Practice Statements. Some of these changes will not materially reduce the assurance that a certificate policy or its implementation provides, and will be judged by the policy administrator as not changing the acceptability of certificates asserting the policy for the purposes for which they have been used. Such changes to certificate policies and Certification Practice Statements need not require a change in the certificate policy Object Identifier or the CPS pointer (URL). Other changes to a specification will change the acceptability of certificates for specific purposes, and these changes will require changes to the certificate policy Object Identifier or CPS pointer (URL).*

8.2 PUBLICATION AND NOTIFICATION POLICIES

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

8.3 CPS APPROVAL PROCEDURES

The term certification practice statement (CPS) is defined in the Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework as: "A statement of the practices, which a Certification Authority employs in issuing certificates." It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management. It shall be more detailed than the corresponding certificate policy described above. The FBCA CPS, which is contained in a separate document published by the FBCA Operational Authority and approved by the Federal PKI Policy Authority, specifies how the FBCA CP and any Memoranda of Agreements that the Federal PKI Policy Authority has approved will be implemented to ensure compliance with their provisions.

8.4 WAIVERS

The Federal PKI Policy Authority will develop and publish procedures pertaining to this area.

9. 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.

FIPS 112 — Password Usage, 1985-05-30 http://csrs.nist.gov/fips/

FIPS 140-1 — Security Requirements for Cryptographic Modules, 1994-01 http://csrs.nist.gov/fips/fips1401.htm

FIPS 186 — Digital Signature Standard, 1994-05-19 http://csrs.nist.gov/fips/fips186.pdf

FOIACT — 5 U.S.C. 552, Freedom of Information Act. Http://www4.law.cornell.edu/uscode/5/552.html

FPKI-Prof — Federal PKI X.509 Certificate and CRL Extensions Profile http://csrc.nist.gov/pki/twg/y2000/papers/twg-00-18.xls

ISO9594-8 — Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997. ftp://ftp.bull.com/pub/OSIdirectory/ITU/97x509final.doc

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. Http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html

RFC 2510 Certificate Management Protocol, Adams and Farrell, March 1999.

RFC 2527 Certificate Policy and Certificate Practices Framework, Chokhani and Ford, March 1999.

Security Requirements for Certificate Issuing and Management Components, 3 November 1999, Draft

Digital Signatures, W. Ford

United States Department of Defense X.509 Certificate Policy, Version 5.0, 13 December 1999

10. ACRONYMS AND 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
FBCA Operational Authority	Federal Bridge Certification Authority Operational Authority
FED-STD	Federal Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKI	Federal Public Key Infrastructure
FPKI-Prof	Federal PKI 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 Federal PKI Policy Authority allowing interoperation between the FBCA and Entity Principal CA)
NIST	National Institute of Standards and Technology
NSA	National Security Agency
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

11. 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).
Agency	For purposes of this CP only, agency is defined as any instrumentality of the federal government, executive, legislative, or judicial branch.
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 Federal PKI Policy Authority 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	An authority trusted by one or more users to issue and manage X.509

(CA)	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 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, such as a subscriber's postal address, that is not

Information	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.
Component Private Key	Private key associated with a function of the certificate issuing equipment, as opposed to being associated as opposed to being associated with an operator or administrator.
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	For purposes of this CP, Entity is any person, organization, corporation, or government (state, local, federal, or foreign) operating, or directing the operation of, one or more CAs.
Entity CA	A CA that acts on behalf of an Entity, and is under the operational control of an Entity.
Federal Bridge Certification Authority (FBCA)	The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer to peer interoperability among Entity Principal Certification Authorities.
Federal Bridge Certification Authority Membrane	The Federal Bridge Certification Authority Membrane consists of a collection of Public Key Infrastructure components including a variety of Certification Authority PKI products, Databases, CA specific Directories, Border Directory, Firewalls, Routers, Randomizers, etc.
FBCA Operational Authority	The Federal Bridge Certification Authority 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 Federal PKI Policy Authority is a federal government body responsible for setting, implementing, and administering policy decisions regarding 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 Federal PKI Policy Authority 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 four 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 Federal PKI Policy Authority.
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 applicable law and 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.
Secret Key	A “shared secret” used in symmetric cryptography, wherein users are authenticated based on a password, Personal Identification Number (PIN), or other information shared between the user and the remote host or server. A single key is shared between two parties: the sender, to encrypt a transmission, and the recipient, to decrypt the transmission, with the shared key being generated with an algorithm agreed to beforehand by the transacting parties.
Server	A system entity that provides a service in response to requests from clients.
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]
Token	Hardware or software that contains or can be used to generate cryptographic keys. Examples of hardware tokens include smart cards and memory cards. Software tokens include both software cryptographic modules that store or generate keys and storage devices or messages that contain keys (e.g., PKCS #12 messages).
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]

12. ACKNOWLEDGEMENTS

While a large number of people identified below participated in the review and development of this Certificate Policy, we would like to specially thank Mr. Richard Guida, Chair of the Federal Public Key Infrastructure Steering Committee, and Mr. Joseph Mettle of the National Security Agency (NSA).

Peter Alterman NIH

Roger Bezdek Treasury

Michelle Borzillo	FDIC
Bill Burr	NIST
Stanley Choffrey	GSA
Russell Davis	FDIC
Dave Fillingham	NSA
Richard Guida	Treasury
Donald Hagerling	Treasury
Michael Henry	PEC
Michael Jenkins	NSA
William Kelly	Treasury
Kathy Lyons-Burke	NIST
Gene McDowell	NOAA
Joseph Mettle	NSA/Treasury
Gary Moore	Entrust
Tim Polk	NIST
Michael Power	GOC
John Purcell	Treasury
Paul Rogers	CIAO
Marion A. Royal	GSA
Shauna Russell	DoD
Sharon Shank	DOE
Kathy Sharp	USDA
Denise Silverberg	Treasury
Judith Spencer	GSA

Johnny Sumners	Treasury
David Sweigert	GD-CS
Shahira Tadross	DOJ/EOUSA
Martin Tevelow	BAH
Peter Weiss	OMB