



**Public**

**X.509 Certification Practice Statement (CPS)**

**For The**

**Federal Bridge Certification Authority (FBCA)**

**7 March 2003**



**Signature Page**

\_\_\_\_\_  
Chair, Federal Public Key Infrastructure Steering Committee

\_\_\_\_\_  
DATE



## Table of Contents

<b>1. INTRODUCTION.....</b>	<b>1</b>
<b>1.1 OVERVIEW.....</b>	<b>2</b>
1.1.1 Certification Practice Statement (CPS).....	2
1.1.2 Relationship Between the FBCA CPS and the FBCA CP.....	2
1.1.3 Relationship Between the FBCA CP and the Agency CP.....	2
1.1.4 Interoperation with CAs External to the Federal Government.....	2
<b>1.2 IDENTIFICATION.....</b>	<b>2</b>
<b>1.3 COMMUNITY AND APPLICABILITY.....</b>	<b>3</b>
1.3.1 PKI Authorities.....	3
1.3.2 Applicability.....	6
<b>1.4 CONTACT DETAILS.....</b>	<b>7</b>
1.4.1 Specification administration organization.....	7
1.4.2 Contact person.....	7
1.4.3 Person determining Certification Practice Statement suitability for the policy.....	7
<b>2. GENERAL PROVISIONS.....</b>	<b>7</b>
<b>2.1 OBLIGATIONS.....</b>	<b>7</b>
2.1.1 CA Obligations.....	7
2.1.2 RA Obligations.....	11
2.1.3 Subscriber Obligations.....	11
2.1.4 Relying Party Obligations.....	11
2.1.5 Repository Obligations.....	12
2.1.6 Requirements for Issuing Certificates to non-US Government Parties.....	12
<b>2.2 LIABILITY.....</b>	<b>12</b>
<b>2.3 FINANCIAL RESPONSIBILITY.....</b>	<b>12</b>
2.3.1 Indemnification by Relying Parties and subscribers.....	13
2.3.2 The FBCA CP does not stipulate a requirement for this section. Fiduciary relationships.....	13
2.3.3 Administrative processes.....	13
<b>2.4 INTERPRETATION AND ENFORCEMENT.....</b>	<b>13</b>
2.4.1 Governing Law.....	13
2.4.2 Severability of Provisions, Survival, Merger, and Notice.....	13
2.4.3 Dispute resolution procedures.....	13
<b>2.5 FEES.....</b>	<b>13</b>
<b>2.6 PUBLICATION AND REPOSITORY.....</b>	<b>13</b>

2.6.1	Publication of CA Information .....	13
2.6.2	Frequency of Publication .....	14
2.6.3	Access controls .....	14
2.6.4	Repositories.....	15
<b>2.7</b>	<b><i>COMPLIANCE AUDIT</i></b> .....	<b>15</b>
2.7.1	Frequency of Entity Compliance Audit .....	15
2.7.2	Identity/Qualifications of Compliance Auditor .....	15
2.7.3	Compliance Auditor’s Relationship to Audited Party .....	16
2.7.4	Topics Covered by Compliance Audit.....	16
2.7.5	Actions taken as a result of deficiency .....	16
2.7.6	Communication of Result .....	17
<b>2.8</b>	<b><i>CONFIDENTIALITY</i></b> .....	<b>17</b>
2.8.1	Types of Information to be Protected .....	17
2.8.2	Information Release Circumstances .....	17
<b>2.9</b>	<b><i>INTELLECTUAL PROPERTY RIGHTS</i></b> .....	<b>18</b>
<b>3.</b>	<b>IDENTIFICATION AND AUTHENTICATION.....</b>	<b>18</b>
<b>3.1</b>	<b><i>INITIAL REGISTRATION</i></b> .....	<b>18</b>
3.1.1	Types of names .....	18
3.1.2	Need for names to be meaningful .....	19
3.1.3	Rules for interpreting various name forms .....	20
3.1.4	Uniqueness of names .....	20
3.1.5	Name claim dispute resolution procedure.....	20
3.1.6	Recognition, authentication and role of trademarks .....	20
3.1.7	Method to prove possession of private key.....	20
3.1.8	Authentication of organization identity Subscriber .....	20
3.1.9	Authentication of Individual Identity Subscriber .....	21
3.1.10	Authentication of Component Identity subscribers .....	21
3.1.11	Authentication of Agency PCAs.....	21
<b>3.2</b>	<b><i>CROSS-CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY</i></b> .....	<b>23</b>
3.2.1	Cross-Certificate Re-key.....	23
3.2.2	Cross-Certificate Renewal .....	24
3.2.3	Cross-Certificate Update.....	24
<b>3.3</b>	<b><i>OBTAINING A NEW CROSS-CERTIFICATE AFTER REVOCATION</i></b> .....	<b>24</b>
<b>3.4</b>	<b><i>REVOCATION REQUEST</i></b> .....	<b>24</b>

<b>4.</b>	<b>OPERATIONAL REQUIREMENTS .....</b>	<b>24</b>
<b>4.1</b>	<b>APPLICATION FOR A CROSS-CERTIFICATE.....</b>	<b>24</b>
4.1.1	Delivery of Agency PCA public key(s) for FBCA cross-certificate issuance.....	25
<b>4.2</b>	<b>CERTIFICATE ISSUANCE.....</b>	<b>25</b>
4.2.1	Delivery of Subscriber's private key to Subscriber.....	26
4.2.2	FBCA public key delivery and use .....	26
<b>4.3</b>	<b>CROSS-CERTIFICATE ACCEPTANCE .....</b>	<b>26</b>
<b>4.4</b>	<b>CERTIFICATE SUSPENSION AND REVOCATION .....</b>	<b>26</b>
4.4.2	Suspension .....	29
4.4.3	Certification Authority Revocation Lists (CARLs) / Certificate Revocation Lists (CRLs)	29
4.4.4	On-line Revocation / Status checking availability.....	30
4.4.5	Other forms of revocation advertisements available .....	30
4.4.6	Checking requirements for other forms of revocation advertisements.....	30
4.4.7	Special requirements related to key compromise .....	30
<b>4.5</b>	<b>SECURITY AUDIT PROCEDURE.....</b>	<b>30</b>
4.5.1	Types of Events Recorded .....	30
4.5.2	Frequency of processing data.....	38
4.5.3	Retention period for security audit data.....	38
4.5.4	Protection of security audit data .....	38
4.5.5	Security Audit data backup procedures .....	39
4.5.6	Security Audit collection system (internal vs. external).....	39
4.5.7	Notification to event-causing subject.....	39
4.5.8	Vulnerability Assessments.....	40
<b>4.6</b>	<b>RECORDS ARCHIVAL.....</b>	<b>40</b>
4.6.1	Types of events archived .....	40
4.6.2	Retention period for archive .....	41
4.6.3	Protection of archive.....	41
4.6.4	Archive backup procedures.....	42
4.6.5	Requirements for time-stamping of records .....	43
4.6.6	Archive collection system.....	43
4.6.7	Procedures to obtain and verify archive information.....	43
<b>4.7</b>	<b>KEY CHANGEOVER.....</b>	<b>43</b>
<b>4.8</b>	<b>COMPROMISE AND DISASTER RECOVERY.....</b>	<b>44</b>
4.8.1	Computing resources, software, and/or data are corrupted.....	44

4.8.2	FBCA signature keys are revoked .....	45
4.8.3	FBCA signature keys are compromised .....	45
4.8.4	Secure Facility impaired after a Natural or Other type of Disaster .....	46
<b>4.9</b>	<b><i>CA TERMINATION</i></b> .....	<b>46</b>
<b>5.</b>	<b>PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS .....</b>	<b>46</b>
<b>5.1</b>	<b><i>PHYSICAL CONTROLS FOR THE FBCA OR AGENCY CA</i></b> .....	<b>46</b>
5.1.1	Site location and construction.....	47
5.1.2	Physical access.....	47
5.1.3	Electrical Power .....	47
5.1.4	Water exposures.....	48
5.1.5	Fire prevention and protection .....	48
5.1.6	Media storage.....	48
5.1.7	Waste disposal .....	48
5.1.8	Off-site backup.....	48
<b>5.2</b>	<b><i>PROCEDURAL CONTROLS FOR THE FBCA AND AGENCY CA</i></b> .....	<b>48</b>
5.2.1	Trusted Roles .....	48
5.2.2	Separation of Roles.....	50
5.2.3	Number of persons required per task .....	50
5.2.4	Identification and authentication for each role .....	51
<b>5.3</b>	<b><i>PERSONNEL CONTROLS</i></b> .....	<b>51</b>
5.3.1	Background, qualifications, experience, and security clearance requirements .....	51
5.3.2	Background check procedures .....	51
5.3.3	Training Requirements.....	51
5.3.4	Retraining frequency and requirements .....	52
5.3.5	Job rotation frequency and sequence .....	52
5.3.6	Sanctions for unauthorized actions .....	52
5.3.7	Contracting personnel requirements .....	52
5.3.8	Documentation supplied to personnel.....	52
<b>6.</b>	<b>TECHNICAL SECURITY CONTROLS .....</b>	<b>52</b>
<b>6.1</b>	<b><i>KEY PAIR GENERATION AND INSTALLATION</i></b> .....	<b>52</b>
6.1.1	FBCA and CA key pair generation.....	52
6.1.2	Private Key Delivery to Subscriber .....	52
6.1.3	Public Key Delivery to Certificate Issuer .....	53

6.1.4	FBCA cross-certificates and public key availability and delivery to Agency PCAs	53
6.1.5	Key sizes .....	53
6.1.6	Public key parameters generation .....	53
6.1.7	Parameter quality checking.....	53
6.1.8	Hardware/Software key generation.....	53
6.1.9	Key usage purposes (as per X.509 v3 key usage field) .....	53
<b>6.2</b>	<b><i>PRIVATE KEY PROTECTION</i></b> .....	<b>54</b>
6.2.1	Standards for cryptographic module.....	54
6.2.2	FBCA private key multi-person control .....	54
6.2.3	Key Escrow of FBCA private signature key.....	54
6.2.4	Private Key Backup .....	54
6.2.5	Private Key Archival.....	54
6.2.6	Private key entry into cryptographic module.....	54
6.2.7	Method of activating private keys.....	54
6.2.8	Methods of deactivating private keys .....	55
6.2.9	Method of destroying private signature keys.....	55
<b>6.3</b>	<b><i>GOOD PRACTICES REGARDING KEY-PAIR MANAGEMENT</i></b> .....	<b>55</b>
6.3.1	Public Key Archival.....	55
6.3.2	Usage Periods for the Public and Private Keys .....	55
<b>6.4</b>	<b><i>ACTIVATION DATA</i></b> .....	<b>56</b>
6.4.1	Activation data generation and installation.....	56
6.4.2	Activation data protection.....	56
6.4.3	Other Aspects of Activation Data.....	56
<b>6.5</b>	<b><i>COMPUTER SECURITY CONTROLS</i></b> .....	<b>56</b>
6.5.1	Specific computer security technical requirements .....	56
6.5.2	Computer Security Rating.....	58
<b>6.6</b>	<b><i>LIFE-CYCLE TECHNICAL CONTROLS</i></b> .....	<b>58</b>
6.6.1	System development controls .....	58
6.6.2	Security management controls.....	59
<b>6.7</b>	<b><i>NETWORK SECURITY CONTROLS</i></b> .....	<b>59</b>
<b>6.8</b>	<b><i>CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS</i></b> .....	<b>59</b>
<b>7.</b>	<b><i>CERTIFICATE AND CARL/CRL PROFILES</i></b> .....	<b>59</b>
<b>7.1</b>	<b><i>CERTIFICATE PROFILE</i></b> .....	<b>60</b>
7.1.1	Version numbers .....	69
7.1.2	Certificate Extensions .....	69

7.1.3	Algorithm object identifiers .....	69
7.1.4	Name forms .....	69
7.1.5	Name constraints .....	69
7.1.6	Certificate policy object identifier .....	70
7.1.7	Usage of Policy Constraints extension .....	70
7.1.8	Policy qualifiers syntax and semantics .....	70
7.1.9	Processing semantics for the critical certificate policy extension .....	70
<b>7.2</b>	<b><i>CARL/CRL PROFILE</i></b> .....	<b>70</b>
7.2.1	Version numbers .....	73
7.2.2	CARL and CRL entry extensions .....	73
7.2.3	73	
<b>8.</b>	<b>SPECIFICATION ADMINISTRATION .....</b>	<b>73</b>
<b>8.1</b>	<b><i>SPECIFICATION CHANGE PROCEDURES</i></b> .....	<b>73</b>
<b>8.2</b>	<b><i>PUBLICATION AND NOTIFICATION POLICIES</i></b> .....	<b>74</b>
<b>8.3</b>	<b><i>CPS APPROVAL PROCEDURES</i></b> .....	<b>74</b>
<b>8.4</b>	<b><i>WAIVERS</i></b> .....	<b>74</b>
<b>9.</b>	<b>BIBLIOGRAPHY .....</b>	<b>75</b>
<b>10.</b>	<b>ACRONYMS AND ABBREVIATIONS .....</b>	<b>76</b>
<b>11.</b>	<b>GLOSSARY .....</b>	<b>79</b>

### List of Tables

Table 1.3.1-1.	FBCA Roles .....	3
Table 3.1.11-1.	FBCA Assurance Levels .....	22
Table 3.2.1-1.	Routine Rekey Requirements .....	23
Table 4.5.1-1.	Auditable Events .....	31
Table 5.1.2-1.	FBCA Multiple Person Control Access Matrix.....	<b>Error! Bookmark not defined.</b>

**RECORD OF CHANGES**

CHANGE NUMBER	DATE OF CHANGE	DATE RECEIVED	DATE ENTERED	SIGNATURE OF PERSON ENTERING CHANGE

## 1. INTRODUCTION

The Federal Bridge Certification Authority (FBCA) supports interoperability among Federal Agency PKI domains in a peer-to-peer fashion. The FBCA will issue a certificate (i.e., cross certificates) only to those CAs determined by the owning agency (called “Principal CAs”). The FBCA certificates issued to Agency PCAs 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 (FPKIPA).

At their discretion, agencies may elect to interoperate among themselves without using the FBCA. Those agencies that elect to do so may nonetheless employ levels of assurance that mimic those set forth in the FBCA CP. However, FBCA CP Object Identifiers (OIDs) may be used only by agencies that interoperate with the FBCA. Any use of or reference to this FBCA CPS outside the purview of the FPKIPA is completely at the using party’s risk. Further, unless specifically approved by the FPKIPA, an Agency shall not assert the FBCA CP OIDs in any certificates the Agency CA issues, except in the “policyMappings” field establishing an equivalency between an FBCA OID and an OID in the Agency CA’s CP. When used in the “policyMappings” field, the Agency may employ the OIDs only after a policy mapping determination is made by the FPKIPA allowing their use.

The FBCA CP defines five policies. 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 the FBCA 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.

As with every CA operation, the Certification Practice Statement (CPS) documents the internal practices and procedures executed by the FBCA Operational Authority (OA) to comply with the requirements, policy and procedures set forth in the FBCA CP.

This FBCA CPS 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 CPS shall be interpreted under and governed by applicable Federal law. The United States Government disclaims any liability that may arise from the use of this FBCA CPS.

## **1.1 OVERVIEW**

### **1.1.1 Certification Practice Statement (CPS)**

This Certification Practice Statement (CPS) documents the internal practices and procedures used by the Federal Bridge Certification Authority (FBCA) Operational Authority (OA). It covers the operation of systems and the management of facilities, which include FBCA Membrane CAs and the FBCA repository functionality, used to facilitate Agency CA interoperability with the FBCA and with other Agency PKI domains.

### **1.1.2 Relationship Between the FBCA CPS and the FBCA CP**

The FBCA CP states what assurance can be placed in a certificate issued by the FBCA. The FBCA CPS describes how the FBCA practices and procedures establish that assurance.

### **1.1.3 Relationship Between the FBCA CP and the Agency CP**

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

### **1.1.4 Interoperation with CAs External to the Federal Government**

The FBCA CP current version and this CPS do not provide for interoperability through the FBCA between Federal Agency PKI domains and those of parties who are external to the Federal government and who have no regulatory or contractual relationship with the Federal government.

Nonetheless, it is the ultimate intent of the FPKIPA to make the FBCA available to support interoperability between Federal and non-Federal entities. Moreover, interoperability with entities external to the Federal government for purposes of technical testing may be performed when directed by, and in a fashion determined by, the FPKIPA, employing the "Test" level of assurance. Additionally, certificates issued by the FBCA will ensure that appropriate controls are placed on the acceptance of certificates issued by CAs external to the Federal government, for example through the use of the *nameConstraints* extension.

## **1.2 IDENTIFICATION**

This CPS is referred to as the FBCA CPS.

**1.3 COMMUNITY AND APPLICABILITY**

**1.3.1 PKI Authorities**

The following table summarizes the roles relevant to the administration and operation of the FBCA. These roles are entirely defined in the FBCA CP.

**Table 1.3.1-1. FBCA Roles**

<b>FBCA Role</b>	<b>Description</b>
Federal Chief Information Officers Council	<p>The Federal CIO Council comprises the Chief Information Officers of all cabinet level departments and other independent agencies. The Federal CIO Council has established the framework for the interoperable Federal PKI, and that includes overseeing the operation of the organizations responsible for governing and promoting its use. In particular, the FBCA CP and CPS are established under the authority of and with the approval of the Federal CIO Council.</p>
Federal PKI Policy Authority (FPKIPA)	<p>The FPKIPA is a group of U.S. Federal Government Agencies (including cabinet-level Departments) established pursuant to the Federal CIO Council. The FPKIPA includes representatives of the Agencies that execute a MOA with the FBCA. The FPKIPA is responsible for:</p> <ul style="list-style-type: none"> <li>• The Federal Bridge Certification Authority (FBCA) Certificate Policy (CP),</li> <li>• The FBCA Certification Practice Statement (CPS),</li> <li>• Accepting applications from Agencies desiring to interoperate using the FBCA,</li> <li>• Determining the mappings between certificates issued by applicant Agency CAs and the levels of assurance set forth in the FBCA CP (which will include objective and subjective evaluation of the respective CP contents and any other facts deemed relevant by the FPKIPA), and</li> <li>• After an Agency is authorized to interoperate using the FBCA, ensuring continued conformance of that Agency with applicable requirements as a condition for allowing continued interoperability using the FBCA.</li> </ul>
FBCA Operational	The FBCA Operational Authority (OA) is the organization that

<b>FBCA Role</b>	<b>Description</b>
Authority (FBCA OA)	operates the FBCA, including issuing FBCA certificates when directed by the FPKIPA, posting those certificates and Certification Authority Revocation Lists (CARLs) into the FBCA repository, and ensuring the continued availability of the repository to all users.
FBCA OA Administrator	The Administrator is the individual within the FBCA OA 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 OA Officers.
FBCA OA Officers	These officers are the individuals within the FBCA OA, selected by the Administrator, who operate the FBCA and its repository including executing FPKIPA direction to issue FBCA certificates to Agency PCAs or taking other action to effect interoperability between the FBCA and Agency PCAs. The roles include FBCA OA Officer, Auditor, and Operator, all described in the FBCA CPS, section 5.2.1.
Agency Principal Certification Authority (CA)	The Agency PCA is an entity within an Agency 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 to Agency users, or certificates or cross-certificates (or other means of interoperation) to other Agency or external party CAs, or both. It should be noted that an Agency might request that the FBCA interoperate with more than one CA within the Agency; that is, an Agency may have more than one Principal CA. The use of this term shall encompass any CA under the control of the Agency that has a certificate issued to it by the Agency PCA or any CA subordinate to the Principal CA, whether or not the Agency employs a hierarchical or other PKI architecture.
Federal Bridge Certification Authority (FBCA)	<p>The FBCA is the entity operated by the FBCA OA that is authorized by the FPKIPA to create, sign, and issue public key certificates to Agency PCAs. As operated by the FBCA OA, the FBCA is responsible for all aspects of the issuance and management of a certificate including:</p> <ul style="list-style-type: none"> <li>• Control over the registration process,</li> <li>• The identification and authentication process,</li> <li>• The certificate manufacturing process,</li> </ul>

FBCA Role	Description
	<ul style="list-style-type: none"> <li>• Publication of certificates,</li> <li>• Revocation of certificates,</li> <li>• Re-key of FBCA signing material, and</li> <li>• Ensuring that all aspects of the FBCA services and FBCA operations and infrastructure related to certificates issued under the FBCA CP are performed in accordance with the requirements, representations, and warranties of the FBCA CP.</li> </ul>
Registration Authority (RA)	<p>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 OA acts as the RA for the FBCA, and performs its function in accordance with a CPS approved by the FPKIPA. .</p>
Related Authorities	<p>The FBCA operating under the FBCA CP will require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The FBCA CPS identifies the parties responsible for providing such services, and the mechanisms used to support these services.</p>
End Entities	<p>Subscribers</p> <p>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 it issue certificates. FBCA Subscribers include only FBCA OA personnel and, when determined by the FPKIPA, possibly certain network or hardware devices such as firewalls and routers when needed for infrastructure protection. CAs is sometimes technically considered “subscribers” to 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.</p> <p>Relying Parties</p> <p>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</p>

<b>FBCA Role</b>	<b>Description</b>
	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.

The FPKIPA will enter into a Memorandum of Agreement (MOA) (see section 2.1.3.1 in this CPS) with an Agency setting forth the respective responsibilities and obligations of both parties, and the mappings between the certificate levels of assurance contained in the FBCA CP and those in the Agency CP.

**1.3.2 Applicability**

The FBCA does not issue certificates to end-entity subscribers as defined in section 1.3.1; the FBCA only issues certificates to Agency PCAs (cross-certificates) and issues CRLs and CARLs relating to those certificates.

As a key critical infrastructure component, the FBCA OA operates the FBCA at system high level of assurance. The FBCA issues at least one certificate that asserts mapping to the high assurance level, so the FBCA is operated at that level. As described in the FBCA CP, that level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk. Note that the data in such transactions NEVER traverses the FBCA infrastructure component.

The FBCA is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to Federal statues and regulations. Each Agency specific MOA will identify the level(s) of assurance associated with that Agency

**1.3.2.1 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 FPKIPA or the FBCA OA.

The FBCA CP contains some helpful guidance, 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).

## ***1.4 CONTACT DETAILS***

### **1.4.1 Specification administration organization**

The FPKIPA is responsible for the maintenance and all aspects of this CPS.

### **1.4.2 Contact person**

Direct all questions regarding this CPS to the Chair of the FPKIPA, whose address can be found at <http://www.cio.gov/fpkipa>.

### **1.4.3 Person determining Certification Practice Statement suitability for the policy**

The FPKIPA is responsible for determining suitability of this CPS for the FBCA CP.

## **2. GENERAL PROVISIONS**

### ***2.1 OBLIGATIONS***

The FBCA OA will abide with the obligations defined in the FBCA CP, by following the procedures defined in this CPS.

#### **2.1.1 CA Obligations**

The FBCA OA, which operates the FBCA CAs, will abide with the obligations defined in the FBCA CP, by following the procedures defined in this CPS.

##### ***2.1.1.1 Sample FBCA Memorandum of Agreement (MOA)***

The latest draft of the MOA template can be downloaded from the FBCA web site at <http://www.cio.gov/fpkipa/documents/moa.htm>

### **DRAFT FBCA MOA**

**This document is for internal review only and has not been approved by the Department of Justice or accepted by the Federal PKI Steering Committee or Federal PKI Policy Authority**

Memorandum of Agreement

I. Introduction

- A. A. This Agreement is entered into by the Federal Public Key Infrastructure (PKI) Policy Authority and \_\_\_\_\_ ("Agency").
- B. B. This Memorandum of Agreement ("MOA") details the agreement between the Agency and the Federal PKI Policy Authority covering interoperability between the Agency Principal Certification Authority (CA) and the Federal Bridge Certification Authority (FBCA). Specifically, it sets forth the rights, responsibilities and reservations of both parties governing Agency's interoperation with the FBCA.

II. Background

The FBCA is designed to provide a mechanism for agencies employing agency-specific PKI domains to interoperate efficiently. The FBCA allows agencies to create and process trust paths between agency-specific PKI domains, so that digital certificates issued by CAs in one domain can be honored with an appropriate level of trust in a different domain. The FBCA will act as a non-hierarchical "hub." An Agency PCA receives permission to interoperate with the FBCA under terms and conditions described in this document. This system will allow every CA that interoperates with the FBCA the possibility of interoperating with all participating agencies using the FBCA-issued certificates, in an environment of trust and reliability. This is accomplished through the use of policy mapping, which is how certificates issued in different agency PKIs meet one another's standards for authentication, integrity of data, non-repudiation, and encryption of data. Policy mappings between the Agency PCA and the FBCA are proposed by the Agency and approved by the Federal PKI Policy Authority, and then placed in the certificate issued by the FBCA to the Agency PCAs. When the Agency is determining whether to rely on a certificate issued by another agency or party, however, it is not required to use the mapping expressed in the FBCA certificates. The Agency, at its sole discretion, may choose to use a separate mapping for certain transactions or for all transactions.

III. Scope

- A. This Agreement is enforceable only by the parties and is binding upon the parties, by and through their officials, agents, employees, and successors. No person or entity is intended to be a third party beneficiary of the provisions of this Agreement for purposes of any civil, criminal, or administrative action, and accordingly, no person or entity may assert any claim or right as a beneficiary or protected class under this Agreement in any civil, criminal, or administrative action. Similarly, this Agreement does not authorize, nor shall it be construed to authorize, access to any documents by persons or entities not a party to this Agreement.
- B. The Agency's Application for Interoperability with the Federal Bridge Certification Authority ("Application") is incorporated into this document by reference. That Application includes the Agency's Certificate Policy and Certification Practices Statement which form part of the Application.
- C. The FBCA Certificate Policy is incorporated into this document by reference.

- D. The FBCA Certification Practices Statement is incorporated into this document by reference.
- E. This Agreement shall constitute the entire integrated Agreement of the parties. No prior or contemporaneous communications, oral or written, or prior drafts shall be relevant or admissible for purposes of determining the meaning of any provisions herein in any litigation or any other proceeding.
- F. F. If, at any time, either party to this Agreement desires to modify it for any reason, that party shall notify the other party in writing of the proposed modification and the reasons for it. No modification shall occur unless there is written acceptance by both Parties.

#### IV. Rights and Obligations of the Parties

This section details the rights and responsibilities of the parties. It describes what the Federal PKI Policy Authority will provide to the Agency and what the Agency agrees to do in return.

- A. Responsibilities of the Federal PKI Policy Authority. By entering into this agreement, the Federal PKI Policy Authority agrees that it will do the following:
  - 1. Oversee and ensure proper performance of, through the FBCA Operational Authority, the operation and maintenance of the FBCA and the FBCA Directory in accordance with the FBCA CP and CPS.
  - 2. Promptly advise the Agency in the event of any material problem or inability to operate the FBCA in accordance with the FBCA CP or CPS, or in the event that the Federal PKI Policy Authority becomes aware of a material non-compliance on the part of any other party that interoperates with the FBCA or takes any action to terminate or limit such other party's interoperability with the FBCA. Any such notification will occur as follows:
    - a. The Administrator of the FBCA Operational Authority, or the Chair of the Federal PKI Policy Authority, shall notify \_\_\_\_\_ at the Agency (telephone number: \_\_\_\_\_; e-mail address: \_\_\_\_\_).
    - b. Notification will be done by telephone, by digitally signed e-mail, or any other mechanism agreed upon by the parties separate from this agreement but documented in official correspondence between the parties, signed by the Chair of the Federal PKI Policy Authority and \_\_\_\_\_ at the Agency.
- B. Rights of the Federal PKI Policy Authority. By entering into this agreement, the Agency grants the Federal PKI Policy Authority the rights set forth in the FBCA CP, including appropriate access to Agency information such as CA audit results and operational information.
- C. Responsibilities of the Agency. By entering into this agreement, the Agency agrees that it will comply with the applicable requirements of the FBCA CP and its own CP and CPS governing operation of the Agency PKI. In particular, the

agency will develop a matrix which delineates each requirement it must meet pursuant to this MOA, and will supply that matrix along with an attestation to the Federal PKI Policy Authority that all of the requirements are being met, no later than 90 days after the date that this MOA goes into effect. Agency responsibilities to the Federal PKI Policy Authority include:

- 1. Responding within a reasonable time to any requests for information by the Federal PKI Policy Authority or the FBCA Operational Authority.
- 2. Maintaining compliance with the requirements of this MOA, or notifying the Federal PKI Policy Authority promptly in the event of an actual or expected material nonconformance.
- 3. Notifying the Federal PKI Policy Authority in the event of any material change to the information in its Application.
- 4. Ensuring compliance audits are performed and the results reported to the Federal PKI Policy Authority as required in the FBCA CP.

V. Certificate Policy Mapping

The mapping between the Agency's certificate levels of assurance and the FBCA's certificate levels of assurance shall be as detailed in the table below. This information shall be expressed in the policyMappings extension of the certificate issued by the FBCA to the Agency PCA.

<b>FBCA Certificate Level of Assurance</b>	<b>Agency Certificate Level of Assurance</b>
Test	
Rudimentary	
Basic	
Medium	
High	

VI. Liability

Each party to this agreement shall hold the other harmless with respect to any liability arising out of the operation of the FBCA or the Agency PKI.

VII. Special Considerations

<Here is where any provisions specific to the case at hand would be added.>

VIII. Termination of the MOA

This MOA may be terminated under two circumstances:

- A. At the discretion of the Federal PKI Policy Authority. Should the agency not comply with its obligations under the FBCA CP, Agency CP, this MOA, or should an Agency fail an audit, this MOA and the certificate issued by the FBCA to the Agency may be revoked at the sole discretion of the Federal PKI Policy Authority, upon written notification being provided to the Agency and in accordance with procedures published by the Federal PKI Policy Authority.

B. At the request of the Agency. The certificate issued by the FBCA to the Agency PCA may be revoked upon an authenticated request to the Administrator of the FBCA Operational Authority or the Chair of the Federal PKI Policy Authority, by a designated official of the Agency responsible for the Principal CA. This official is \_\_\_\_\_ .

IX. Termination of FBCA Operation.

In the event that the Federal PKI Policy Authority decides to terminate the operation of the FBCA, certificates signed by the FBCA shall be revoked and the Federal PKI Policy Authority shall advise agencies who 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.

X. Date of Effect.

This MOA shall enter into effect upon the signatures of both parties.

FOR THE Federal PKI Policy Authority:

FOR THE AGENCY:

\_\_\_\_\_  
Chair, Federal PKI Policy Authority  
Date: \_\_\_\_\_

\_\_\_\_\_  
XXXX  
Date: \_\_\_\_\_

**2.1.2 RA Obligations**

The FBCA OA is the RA for the FBCA and is responsible for controlling the registration process, including collecting and verifying the information to be entered into the certificates issued by the FBCA. .

**2.1.3 Subscriber Obligations**

The only potential FBCA subscribers identified are the FBCA OA Administrator and the FBCA OA Officers. There are no other FBCA subscribers. The FBCA, however does not issue certificates to end-entity subscribers, rather it merely issues cross-certificates with Agency PCAs, which are not technically deemed as end-entity subscribers.

**2.1.4 Relying Party Obligations**

The Relying Party decides, pursuant to its own agency'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 OA operates and uses a variety of mechanisms for posting information into a repository as required by the FBCA CP. The mechanisms supported and operated include:

- Configuring and maintaining a separate repository (X.500, Lightweight Directory Access Protocol (LDAP) and/or Database) for each FBCA CA,
- Maintaining a separate online X.500 Directory Service System that will support LDAP v2 or better, as directed by the FPKIPA, which allows authorized access and retrieval of the certificate information, including all cross-certificates and the status of all cross-certificates issued by the FBCA, and
- Providing administrative access control mechanisms when needed to protect repository information as described in later sections.

The FPKIPA will be maintaining a web server (see section 2.6.4) to post FBCA for official use only (FOUO) documentation, including the CP, CPS, and FPKIPA procedural documents.

### **2.1.6 Requirements for Issuing Certificates to non-US Government Parties**

The FBCA may issue certificates to parties other than agencies, officers and employees of the U.S. Government, such as 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 FPKIPA. In each such case, a Memorandum of Agreement or similar instrument will be executed, and will contain whatever provisions are determined appropriate by the FPKIPA.

## ***2.2 LIABILITY***

The United States Government disclaims any liability that may arise from use of any certificate issued by the FBCA, or the Federal PKI Policy Authority's determination to revoke a certificate issued by the FBCA. In no event will the U.S. Government be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued by the FBCA

## ***2.3 FINANCIAL RESPONSIBILITY***

Agencies, acting as Relying Parties, are responsible for determining what financial limits, if any, they wish to impose for certificates used to consummate a transaction. This is entirely at the discretion of the Agency 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, agency-specific policy or statutorily imposed constraints).

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

The FBCA is not financially responsible for any losses incurred from using its services.

### **2.3.1 Indemnification by Relying Parties and subscribers**

### **2.3.2 The FBCA CP does not stipulate a requirement for this section. Fiduciary relationships**

No fiduciary is intended or should be deemed to arise out of any provision of this CPS.

### **2.3.3 Administrative processes**

Administrative processes set forth by this CPS are determined by the FBCA OA pursuant to the agreement between it and the FPKIPA for the operation of the FBCA.

## ***2.4 INTERPRETATION AND ENFORCEMENT***

### **2.4.1 Governing Law**

The laws of the United States of America govern the practices described in this CPS.

### **2.4.2 Severability of Provisions, Survival, Merger, and Notice**

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

### **2.4.3 Dispute resolution procedures**

The FPKIPA will resolve any disputes associated with the use of the FBCA or certificates issued by the FBCA.

## ***2.5 FEES***

The FBCA OA will determine the fees, if any, for FBCA services, as approved by the FPKIPA.

## ***2.6 PUBLICATION AND REPOSITORY***

### **2.6.1 Publication of CA Information**

The FBCA OA will deliver this CPS to the FPKIPA and any relevant authority in the Federal government. It will make this CPS available on the FBCA web site described in

section 2.6.4. The FBCA OA will publish information concerning the FBCA necessary to support its use and operation, including:

- The cross certificates it issues;
- The CRLs and CARLs it issues;
- The Certificate for its certificate signing key;
- This CPS; and
- The FBCA CP, and any waivers granted by the FPKIPA.

Information, clearly “about critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a)(i), §3544(A)(1)(a)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3545(f), as well as GSA Orders 1800.3C (draft) and PBS 3490.1, is omitted in the publicly universally available version of this document. The complete CPS document is available upon request to authorized organizations with a need to know.

### **2.6.2 Frequency of Publication**

Certificates are published following certificate issuance as specified in section 4.2. The CRL is published as specified in section 4.4.

### **2.6.3 Access controls**

The web site publishing this CPS enables a read-only access to the FBCA CPS. Only authorized personnel have access to modify the CPS. The procedure for updating the documents on the web server consists of an out-of-band mechanism.

The FBCA directory resides behind a firewall. The public anonymous read access to its information is enabled. Only authorized FBCA OA personnel can update the information stored in this server. Access controls are set by administrative function and assigned roles/responsibilities, and enforced using password-based authenticated subject identity.

The FBCA CA application(s) generating the cross certificates with the Agency PCAs is (are) stand alone, secured, unconnected and physically separate from any external network. The procedures for issuing and updating the cross certificates, CRLs, and CARLs generated by these CA Applications requires multi-person access controls. The updating of the FBCA repository consists of a manual out-of-band transfer via floppy diskette. Each CA within the FBCA is enabled to issue and revoke cross-certificates to Agency PCAs and to generate periodic CARLs/CRLs. The number of CAs within the FBCA system is determined by the FPKIPA.

#### 2.6.4 Repositories

The FBCA includes an X.500 Directory Service that will support, as directed by the FPKIPA, LDAP V2 operations for the purpose of publishing Agency PCAs cross-certificates, the possible FBCA CA(s) self-signed certificates, CRLs and CARLs.

The FBCA also provides a web site to publish other FBCA information, including this CPS and the FBCA CP Access to the CPS is granted only to the Agencies in the Federal government as authorized by the FPKIPA. .

Purpose	Uniform Resource Locator (URL)
X.500 LDAP V2 or better Directory	ldap://fbca_directory.fbca.gov
FBCA CPS Website	<a href="http://www.cio.gov/fpkipa">http://www.cio.gov/fpkipa</a>
FBCA CP Website	<a href="http://www.cio.gov/fpkipa">http://www.cio.gov/fpkipa</a>
FBCA Interoperability Guidelines	<a href="http://www.cio.gov/fpkipa">http://www.cio.gov/fpkipa</a>

## 2.7 COMPLIANCE AUDIT

### 2.7.1 Frequency of Entity Compliance Audit

The FBCA OA will arrange initially and annually for independent inspections and compliance audits to validate that the FBCA is operating in accordance with the security practices and procedures described in this CPS. Results of the compliance audit will be provided to the FPKIPA.

### 2.7.2 Identity/Qualifications of Compliance Auditor

The FBCA compliance audits will be provided by an independent auditor as agreed between the FPKIPA and FBCA OA, which has demonstrated a proven track record in one or more of the following areas:

- Specialization in EDP security audit
- Knowledge and experience with Compliance Audits and PKI

- Independence from the organization being audited
- Understanding of the Federal certification and accreditation process required by OMB A-130 and the Government Information Security Reform Act (GISRA, P.L. 106-398)

The FPKI PA has chosen the following organization to conduct the compliance audit:

Name of the Auditor Organization: KPMG

The selected auditor will verify and validate through document reviews and demonstrations that the FBCA complies with the FBCA CP and requirements that the FPKIPA imposes on the issuance and management of FBCA certificates.

### **2.7.3 Compliance Auditor's Relationship to Audited Party**

As required by GISRA (P.L. 106-398), the selected FBCA compliance auditor is a contractor that is independent from FBCA OA, FPKI PA, and FPKI Steering Committee. This contractor provides an unbiased, independent evaluation and is one whose primary responsibility is the performance of EDP Compliance Audits.

### **2.7.4 Topics Covered by Compliance Audit**

The compliance audit will address all aspects of the FBCA operation. The scope of the compliance audit includes all practices described in this CPS and other FPKIPA requirements.

### **2.7.5 Actions taken as a result of deficiency**

The FBCA compliance auditor will notify within 24 hours the FBCA OA and FPKIPA of the results of the compliance audit by e-mail and/or out-of-band writing.

Once notified, the FPKIPA and FBCA OA will have 10 business days to review the results and the recommendations from the compliance audit to determine the action to be taken.

Based on the findings of the FBCA compliance auditor, the possible courses of actions include:

- Correction of deficiencies prior to implementing full operation of the FBCA or within another time period as determined by the FPKIKPA and FBCA OA
- Suspension of full operation of the FBCA (this alternative will execute the emergency procedure described in section 4.1.1.2 for revocation of certificates),
- Execute other corrective actions through procedures developed and published by the FPKIPA.

In the event of deficiencies on the part of the Agency PCA, the FPKIPA may direct the FBCA OA to suspend interoperations with that Agency PCA by revoking cross-certificates issued to that Agency (this alternative will execute the revocation procedure described in section 4.1.1.2), or

### **2.7.6 Communication of Result**

The selected compliance auditor will communicate results of a compliance audit of the FBCA to the FBCA OA and FPKIPA within 24 hours by a signed e-mail an/or in writing. The results will be provided as a written report. The report will contain a summary table of topics covered, areas in which FBCA was found to be non-compliant, a brief description of the problem(s) for each area of non-compliance, and possible remedies for each area. The report will also contain the detailed results of the compliance audit for all topics covered, including the topics in which the FBCA passed and the topics in which the FBCA failed. Notification of compliance audit failure, the topics of failure, reason(s) for failure, and possible remedies will be provided within 24 hours, upon the conclusion of the compliance audit, in a written form (signed e-mail and/or out of band letter) to the FBCA OA and to the FPKIPA. A comprehensive report may be provided later.

## **2.8 CONFIDENTIALITY**

FBCA information not requiring protection is publicly available. Federal PKI Policy Authority access to Agency information is addressed in the MOA with that Agency. Public access to Agency information is determined by the respective Agency.

### **2.8.1 Types of Information to be Protected**

The following information collected from the Agency PCAs will be kept confidential: MOAs, FBCA CAs passwords and private signature keys, information on the agency sponsor identity card that is not required to be made public (e.g., driver license number, passport number, social security number, etc.) and agency registration information

Information stored on the FBCA workstations is protected by password.

### **2.8.2 Information Release Circumstances**

The FBCA will disclose confidential information to any third party when required by this CPS, FBCA CP, by law, government rule or regulation, or order of a court of competent jurisdiction. Any request for release of information will be authenticated. The authentication will consist of validating the identity of the requester using two forms of photo identifications. The individual's authority to obtain the information will be validated using at least one of the following means:

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

Court orders and IG requests must be approved by specific Agency General Counsel

## ***2.9 INTELLECTUAL PROPERTY RIGHTS***

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

## **3. IDENTIFICATION AND AUTHENTICATION**

This section contains the practices the FBCA OA follows in identifying and Agency PCAs and sponsors involved in the cross certification request process.

### ***3.1 INITIAL REGISTRATION***

An Agency registration to the FBCA service is initiated by applying to the FPKIPA to obtain a cross-certificate from the FBCA to the Agency PCA. This application is done using a form supplied by the FPKIPA (available on its web site, <http://www.cio.gov/fpkipa> that must be filled in by the completed and signed by an authorized official of the Agency (as established on the form). The application contains how the Agency proposes to map the certificate levels of assurance present in the Agency's CP to the levels expressed in the FBCA CP, and how the Agency's certificate profile conforms to the Federal Certificate Profile (available at the FPKIPA web site cited above). The application also describes how the applicant Agency's PKI has been independently audited to ensure conformance by the applicant to its own CP and CPS.

The FPKIPA will evaluate the application and either will accept the policy mapping proposed by the applicant or propose an alternative mapping. If the applicant accepts the alternative mapping, the FPKIPA will execute with the applicant a Memorandum of Agreement (MOA) that reflects the respective responsibilities of the FPKIPA and the Agency along with the policy mappings. After the MOA is signed by the parties, the FPKIPA notifies the FBCA OA to initiate the process for issuing cross-certificates to the Agency PCA and establishing interoperability with the FBCA directory.

#### **3.1.1 Types of names**

The FBCA generates and signs certificates where the issuer DN consists of a set of the following X.520 naming elements: C; O; OU; and CN. Certificates may additionally

assert an alternate name form subject to requirements set forth below which are intended to ensure name uniqueness.

The FBCA generates and signs certificates where the subject DN contains X.520 naming elements (at least C, O, and OU), the domain component naming element (dc), or a combination of the two.

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

The certificates issued to Agency PCAs have an assurance level equal to the highest level of assurance contained in the policy mappings as agreed between the FPKIPA and the Agency PCA.

**3.1.2 Need for names to be meaningful**

The FBCA operates CAs from multiple vendors in order to support the generation and publication of cross-certificates with Agency PCAs using various CA products. The certificates issued by the FBCA CAs contain the relative distinguished name (RDN) of C=US, O=U.S. Government, OU=FBCA, OU= <CA product name>. As an example cross-certificates issued from an Entrust FBCA CA to an Entrust Agency PCA will contain the RDN C=US/O=U.S. Government/OU=FBCA/OU=Entrust.

The FBCA CAs operating under this CPS issue and sign certificates with subject names from within the name-space C=US, O=U.S. Government. For example, the Agency PCA RDN for a certificate issued to the Agency PCA for NIST could be C=US, O=U.S. Government, OU=NIST, OU=Experimental CA1.

Additionally, the FBCA CAs operating under this CPS may issue and sign certificates with subject names from other name spaces as directed explicitly by the FPKIPA.

The FBCA issues all the Medium or High Assurance levels certificates with name constraints asserted limiting the name space of the Agency PCAs to that appropriate for their domains. Additionally, the FPKIPA may require that such constraints be

implemented for the certificates issued at the Test, Basic or Rudimentary levels if it deems appropriate.

### **3.1.3 Rules for interpreting various name forms**

The FBCA certificate profile established by the FPKIPA contains the rules for interpreting name forms. The FBCA certificate profile supports the DN, RFC822, and DCN name forms. The FBCA certificate profile can be found in the FBCA Interoperability Guidelines, which are posted at the FBCA web site (see Section 2.6.4)

### **3.1.4 Uniqueness of names**

The FPKI PA manages the name uniqueness across the FBCA.. Names, whether X.500 DNs or other name forms, will be assigned by the FPKIPA and made unique. Additionally, the CAs in the FBCA membrane are configured to require name uniqueness when issuing cross-certificates to Agency PCAs.

### **3.1.5 Name claim dispute resolution procedure**

Naming collisions that affect interoperability with the FBCA will be brought to the attention of the FPKIPA for resolution. The FBCA OA will revoke and re-issue all affected certificates as directed by the FPKIPA.

### **3.1.6 Recognition, authentication and role of trademarks**

No stipulation.

### **3.1.7 Method to prove possession of private key**

The FBCA OA verifies that a cross-certificate applicant possesses the private key corresponding to the public key submitted with the application in accordance with section 4.2. All transactions involved in cross-certificate issuance are recorded as part of the security audit data, as described in section 4.5.1. Since the FBCA CAs are at all times off-line, these messages are exchanged using an out-of-band mechanism as described in section 4.2.

### **3.1.8 Authentication of organization identity Subscriber**

No stipulation. The FBCA will not issue certificates to organizational subscribers.

The FBCA will issue certificates (i.e., cross certificates) only to Agency PCAs as directed by the FPKIPA. The FPKIPA will authenticate the organization identity as part of the application and MOU processes, as described in section 3.1.11.

### **3.1.9 Authentication of Individual Identity Subscriber**

The FBCA does not issue certificates to any individual. The FBCA OA Administrator and the officers do not have FBCA-issued certificates for their activity.

All data relating to authentication of Agency PCAs is recorded in accordance with section 4.5.1, and archived in accordance with section 4.6.

### **3.1.10 Authentication of Component Identity subscribers**

The FBCA will not issue certificates to FBCA components. No stipulation.

### **3.1.11 Authentication of Agency PCAs**

Agency PCAs are established by the Agency PCA applicant's agency.

Following the completion of the MOU between the FPKIPA and the Agency PCA, the authorized official of the Agency PCA will designate (sponsor) the individual(s) responsible for completing interoperability with the FBCA (i.e., generating cross-certificate requests, establishing directory interoperability). The Agency PCA will provide the FBCA OA with a written document signed by an authorized official of the Agency PCA that provides identity information of the designated individual(s).

The designated Agency PCA responsible individual(s) will complete and sign a registration document and the FBCA OA will verify the information based on the requirements for the level of assurance of the certificate being issued to the Agency PCA.

FBCA OA records the process that was followed for issuance of each certificate. The process documentation and authentication requirements includes 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 Agency PCA responsible individual as required by the level of assurance;
- A unique identifying number from the ID of the verifier and, if in-person identity proofing is done, from the ID of the individual;
- The date and time of the verification;
- A declaration of identity signed by the applicant using a handwritten signature. If in-person identity proofing is done, this is performed in the presence of the person performing the identity authentication or a trusted agent (i.e., notary public).

**For All Levels:** The trusted person will present information sufficient for registration at the level of the certificate being requested. The table below summarizes the identification requirements for each level of assurance.

**Table 3.1.11-1. FBCA Assurance Levels**

Assurance Level	Identification Requirements
Test	To be established in the MOA with the Agency (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 appearance 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 agency as being authorized to confirm identities (such as notaries public) who uses a stamp, seal or other mechanism to authenticate their identity confirmation
Medium	<p>Identity established by in-person appearance before the Registration Authority, Trusted Agent or an entity certified by a State or Federal agency as being authorized to confirm identities (such as notaries public) who uses a stamp, seal or other mechanism to authenticate their identity confirmation; information provided shall be checked to ensure legitimacy</p> <p>Credentials required are either one Federal Government-issued Picture ID, or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License)</p>
High	<p>Identity established by in-person appearance before the Registration Authority or Trusted Agent; information provided shall be checked to ensure legitimacy</p> <p>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)</p>

### 3.2 CROSS-CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY

#### 3.2.1 Cross-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. FBCA cross-certificates issued under this CPS to Agency PCAs will have three-year maximum validity period for authentication certificates.

New cross-certificates will need to be issued to Agency PCAs by the FBCA when the FBCA re-keys (every one-half of the FBCA CA self-signed certificate validity period), and when Agency PCAs re-key. Upon Agency PCAs re-key, the FBCA OA will identify and authenticate the Agency PCAs either by:

- (a) Performing the initial registration identification process defined in Section 3.1, or
- (b) If it has been less than one-half of the certificate validity period since an Agency PCA was identified as required in Section 3.1, using the currently valid certificate issued to the Agency PCA by the FBCA.

Agency PCAs designated responsible individuals identify themselves for the purpose of re-keying as required in table below.

**Table 3.2.1-1. Routine Rekey Requirements**

<b>Assurance Level</b>	<b>Routine Rekey Identity Requirements for Subscriber Signature and Encryption Certificates</b>
Test	To be determined in the MOA with the Agency
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

Assurance Level	Routine Rekey Identity Requirements for Subscriber Signature and Encryption Certificates
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 Cross-Certificate Renewal

No Stipulation. The FBCA does not renew cross certificates.

### 3.2.3 Cross-Certificate Update

No stipulation. The FBCA does not update cross certificates.

### 3.3 *OBTAINING A NEW CROSS-CERTIFICATE AFTER REVOCATION*

In the event of cross-certificate revocation, issuance of a new cross-certificate always requires an initial registration process per Section 3.1 above.

### 3.4 *REVOCATION REQUEST*

Revocation requests are authenticated and processed as described in section 4.4.

## 4. OPERATIONAL REQUIREMENTS

### 4.1 *APPLICATION FOR A CROSS-CERTIFICATE*

The procedures developed, approved and published (on the FBCA web site) by the FPKI PA for agencies to use in applying for a certificate from the FBCA for one or more Agency PCAs are as follows:

1. The candidate agency completes an application using a form supplied by the Federal PKIPA (available on its web site, <http://www.cio.gov/fpkipa>), which is signed by an authorized official of the agency (as established on the form). The application contains how the agency proposes to map the certificate levels of assurance present in the Agency PCA CP to the levels expressed in the FBCA CP, and how the Agency certificate profile conforms to the FBCA certificate profile (available at the web site cited above). The application also describes how the applicant Agency PKI has been independently audited to ensure conformance by the applicant to its own CP and CPS. The Agency application will include the Agency CP and CPS written to the format of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC2527].

2. The FPKIPA acts on the application and makes a determination as to whether to issue a certificate and enter into the MOA with the applicant Agency.
3. The FPKIPA instructs the FBCA OA to issue the certificate to the Agency PCA.
4. The FPKIPA also instructs each established Agency PCA to provide the FBCA OA with a memo (on the Agency PCA site letterhead) designating a primary and alternate POC. The Agency PCA authorized official signs this memo. The memo contains the Agency PCA Distinguished Name (DN).. The memo also contains the name of the electronic file, which contains the certificate request (PKCS #10 format message). The three items: letter, floppy diskette, and backup floppy diskette are put in a sealed envelope and securely delivered to the FBCA OA (i.e., in-person, registered mail, courier).
5. Upon issuance, each certificate issued by the FBCA is manually checked to ensure each field and extension is properly populated with the correct information, before the certificate is delivered to the Agency PCA and before it is posted in the repository.

#### **4.1.1 Delivery of Agency PCA public key(s) for FBCA cross-certificate issuance**

Agency PCA public keys are delivered to the FBCA electronically in a digitally signed certificate request (i.e., using PKCS #10) message to the FBCA OA via secure non-electronic means (e.g., floppy disk delivered by registered mail or courier). Identity checking and proof of possession of the private key is accomplished as described in this CPS in section 3.1.11 and 4.2 respectively.

#### **4.2 CERTIFICATE ISSUANCE**

The FBCA OA issues cross-certificates to the Agency PCA by the following procedure:

1. Upon receiving a signed request message (PKCS#10 message) from the Agency PCA, the designated CA software verifies the signature to prove possession of the private key. Then the designated FBCA CA will sign and issue a cross-certificate to the Agency PCA.
2. The certificate issued by the FBCA CA will be delivered to the Agency PCA in a signed response message (PKCS#10), via secure non-electronic means (e.g., floppy disk delivered by registered mail or courier).
3. Each certificate issued by the FBCA is manually checked to ensure each field and extension is properly populated with the correct information, before the certificate is delivered to the Agency PCA.
4. The FBCA CA will generate a digitally signed certificate request message and deliver it to the Agency PCA in a PKCS#10 certificate request message, via

secure non-electronic means (e.g., floppy disk delivered by registered mail or courier).

5. The Agency PCA will sign and issue a certificate to the FBCA CA and deliver it to the FBCA in a signed response message (PKCS#10), via secure non-electronic means (e.g., floppy disk delivered by registered mail or courier)..
6. The FBCA OA will post both certificates (cross-certificates) in the FBCA repository individually or as a single cross-certificate pair.

#### **4.2.1 Delivery of Subscriber's private key to Subscriber**

The FBCA does not generate subscriber private keys.

#### **4.2.2 FBCA public key delivery and use**

The FBCA incorporates CA products from different vendors to enable cross-certification with CA platforms implemented by Agency PCAs.

The FBCA CA products public keys are delivered to the Agency PCA(s) as described in section 4.2 above.

### ***4.3 CROSS-CERTIFICATE ACCEPTANCE***

The MOA sets forth responsibilities of respective Agencies and the FPKIPA before the FPKIPA authorizes issuance of an FBCA cross certificate to the Agency PCA. Once that a cross-certificate has been issued, its acceptance by the Agency PCA commences interoperability with the FBCA via completion of directory chaining between the Agency PCA directory and the FBCA directory. This triggers its obligations under the MOA and this CPS.

### ***4.4 CERTIFICATE SUSPENSION AND REVOCATION***

- Circumstances for revocation of a cross-certificate issued by the FBCA

There are three circumstances where certificates issued by the FBCA can be revoked:

1. When the Federal Policy authority requests that an FBCA-issued certificate be revoked. This will be the normal mechanism for revocation in cases where the FBCA PA determines that an Agency PKI does not meet the FPKI policy requirements or certification of the Agency PKI is no longer in the best interest of the federal government.

2. When the FBCA Operational Authority receives an authenticated request from a previously designated official of the Agency responsible for the Principal CA (such official or official shall be identified in the MOA as authorized to make such a request.
3. When the FBCA Operational Authority 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:
  - a. Chair of the FPKI Policy Authority
  - b. Chair of the FPKI Steering Committee
  - c. Directory of the FBCA Operational Authority
  - d. As designated by the FPKI Policy Authority

The FPKI PA shall meet as soon as practical to review the emergency revocation.

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

The FBCA OA posts the CRL and/or CARL to the FBCA repository (see section 2.6.4) within 6 hours of notification. Certificates are removed from the CRL and/or CARL after the expiration date of the cross-certificate; however the revoked certificate must appear on at least one published CRL and/or CARL.

#### ***4.4.1.1 Who can request revocation of a cross-certificate issued by the FBCA or Agency CA***

An FBCA cross-certificate to an Agency PCA is revoked (1) upon direction of the FPKIPA, or (2) upon an authenticated request by a previously designated authorized official of the Agency PCA (such official or officials are established in the MOA as authorized to make such a request) (3) when the FBCA Operational Authority personnel determine that an emergency has occurred that may impact the integrity of the certificates issued by the FBCA (see section 4.4.1).

#### ***4.4.1.2 Procedure for revocation request***

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

1. An authorized official of the Agency PCA, or the FPKI PA, drafts an authenticated request to revoke a certificate. The individual then notifies the

request to the FBCA OA Administrative/Help desk via phone as well as submits the request via signed e-mail to the FBCA OA identifying the certificate to be revoked, explaining the reason for revocation.

2. Upon receipt of a signed revocation request, the FBCA OA authenticates the request by verifying the digital signature and/or making direct contact (call back or challenge/response telephone conversation) with the Agency PCA POC (or the FPKI PA).
3. In the event the request to revoke originates from the Agency PCA, the FBCA OA apprises the FPKIPA of the request for revocation.
4. The FPKIPA evaluates and verifies the need for revocation expressed in the authenticated request. If the revocation request appears to be valid, the FPKIPA will direct the FBCA OA to proceed with revocation.
5. The FBCA OA will revoke the certificate, which automatically generates and adds a CRL entry for that certificate within 6 hours of notification of approval by the FPKIPA.
6. The FBCA OA manually posts the new CARL/CRL in the FBCA repository within 6 hours of notification of approval by the FPKIPA.
7. The Agency PCA also revokes the certificate issued to the FBCA and generates and posts a new CARL/CRL.

The FBCA OA may affect revocation of a certificate prior to notification and approval of the FPKIPA as set forth in emergency revocation procedures consisting of the following steps:

1. Notify all identified POCs in the emergency list of FBCA (i.e., FPKI Steering Committee POC, FPKI OA POC, Agency PCA POCs, CP/CPS WG POC). This can be done by either:
  - a. Telephone (using one of call-back or challenge/response protocols)
  - b. Signed FAX
  - c. Signed e-mail
2. Revoke the cross-certificate and post the new CRL/CARL
3. Once the incident has been investigated and documented, issue a new cross-certificate to replace the one that has been revoked, as directed by the FPKIPA.

#### ***4.4.1.3 Revocation of a Cross-Certificate Issued by the FBCA***

Revocation of an FBCA cross-certificate is accomplished by the generation and publication into the FBCA repository of status information citing the cross-certificate as revoked and the reason for the revocation, within 6 hours of notification of approval by the FPKIPA or in accordance with emergency procedures provided in section 4.4.1.2.

Further, and separate from the publication of the status information, prompt oral and/or electronic notification is given by the FBCA OA to all Agency PCA POCs..

#### ***4.4.1.4 Revocation of a Cross-Certificate Issued by the Agency PCA***

Revocation takes effect upon the publication of status information (including the reason for the revocation, which may include loss, compromise) for the cross-certificate issued to the FBCA. Information about a revoked cross-certificate remains in the status information until the cross-certificate expires and for one additional CARL issued after it expires.

#### ***4.4.1.5 Revocation Request Grace Period***

There is no revocation grace period for the FBCA.

### **4.4.2 Suspension**

Suspension will not be used by the FBCA.

### **4.4.3 Certification Authority Revocation Lists (CARLs) / Certificate Revocation Lists (CRLs)**

The FBCA OA issues Certification Authority Revocation Lists (CARLs) and Certificate Revocation Lists (CRLs) in accordance with the CARL/CRL profile provided in the FBCA Interoperability Guidelines. The contents of CARLs and CRLs are checked before posting to the FBCA repository to ensure that all information is correct by using mechanisms provided by the CA software or third-party software

#### ***4.4.3.1 CARL/CRL Issuance Frequency***

CARLs and CRLs are issued daily, even if there are no changes to be made, to ensure timeliness of information. Certificate status information is posted within 6 hours of notification of approval of revocation or immediately in accordance with emergency revocation procedures provided in section 4.4.1.2. The current CARL/CRL will be removed and replaced with the updated CARL/CRL.

#### ***4.4.3. CARL/CRL Checking Requirements***

The FBCA repository currently supports CRL/CARL access via X.500 chaining to provide certificate status information (i.e., X.500 DSP). The FBCA plans to support Lightweight Directory Access Protocol (LDAP) CRL/CARL checking in the future

#### **4.4.4 On-line Revocation / Status checking availability**

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

#### **4.4.5 Other forms of revocation advertisements available**

The FBCA does not support any other forms of revocation advertisements.

#### **4.4.6 Checking requirements for other forms of revocation advertisements**

The emergency revocation procedures are delineated in section 4.4.1.2.

#### **4.4.7 Special requirements related to key compromise**

In the event of an Agency PCA private key compromise or loss, a CARL/CRL is published by the FBCA OA within 6 hours of notification of approval by the FPKI PA or within 24 hours, in accordance with procedures described in section 4.4.1.2.

### **4.5 SECURITY AUDIT PROCEDURE**

The FBCA OA generates audit log files for all events relating to the security of the FBCA. Where possible, the security audit logs are automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism is used, depending on the audited event. All security audit logs, both electronic and non-electronic, are retained and made available during compliance audits. The security audit logs for each auditable event defined in this section are maintained in accordance with *Retention period for archive*, Section 4.6.2.

#### **4.5.1 Types of Events Recorded**

Security auditing capabilities of the FBCA repository, the FBCA operating system, and CA applications have been enabled for logging the types of events specified in the table below. The table indicates whether the auditable event is logged automatically by the application/operating system, or it is logged manually in a logbook as prescribed by applicable procedures. At a minimum, each audit record includes the following (either recorded automatically or manually for each auditable event):

- The type of event
- The date and time the event occurred
- A success or failure indicator when executing the FBCA or Agency 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 Agency CA) that caused the event.
- A message from any source requesting an action by the FBCA or Agency CA is an auditable event. The message must include message date and time, source, destination and contents.

The FBCA OA staff has verified (i.e., obtained vendor statements and conducted direct testing) that the equipment and application software purchased indeed supports capturing audit logs for the events specified in the table below.

**Table 4.5.1-1. Auditable Events**

Auditable Event	FBCA Directories		FBCA CAs	
	Manual / Procedural	Automatic	Manual / Procedural	Automatic
<b>SECURITY AUDIT</b>				
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	✓		✓	
Any attempt to delete or modify the Audit logs	✓ After a deletion following any archive operation	✓ After a modification following any archive operation		✓
<b>IDENTIFICATION AND AUTHENTICATION</b>				
Successful and unsuccessful attempts to assume a role		✓		✓
Change in the value of maximum authentication attempts	✓		✓	
Maximum number of unsuccessful authentication attempts during user login		✓		✓

Auditable Event	FBCA Directories		FBCA CAs	
	Manual / Procedural	Automatic	Manual / Procedural	Automatic
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	The account is immediately re-activated			
An Administrator changes the type of authenticator, e.g., from password to biometrics	✓		✓	
<b>KEY GENERATION</b>				
Whenever the FBCA-CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	Applies to CA only	Applies to CA only	✓	✓
<b>PRIVATE KEY LOAD AND STORAGE</b>				
The loading of Component private keys	Applies to CA only	Applies to CA only	✓	✓
All access to certificate subject private keys retained within the FBCA CA for key recovery purposes	Applies to CA only	Applies to CA only	✓	✓
<b>TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE</b>				
All changes to the trusted public keys, including additions and deletions	Applies to CA only	Applies to CA only	✓	✓

Auditable Event	FBCA Directories		FBCA CAs	
	Manual / Procedural	Automatic	Manual / Procedural	Automatic
<b>PRIVATE KEY EXPORT</b>				
The export of private-keys (keys used for a single session or message are excluded)	Applies to CA only	Applies to CA only	✓	✓
<b>CERTIFICATE REGISTRATION</b>				
All certificate requests	Applies to CA only	Applies to CA only	✓	✓
<b>CERTIFICATE REVOCATION</b>				
All certificate revocation requests	Applies to CA only	Applies to CA only	✓	✓
<b>CERTIFICATE STATUS CHANGE APPROVAL</b>				
The approval or rejection of a certificate status change request	Applies to CA only	Applies to CA only	✓	
<b>FBCA CA CONFIGURATION</b>				
Any security-relevant changes to the configuration of the FBCA CA	Applies to CA only	Applies to CA only	✓	✓
<b>ACCOUNT ADMINISTRATION</b>				
Roles and users are added or deleted	✓		✓	✓

Auditable Event	FBCA Directories		FBCA CAs	
	Manual / Procedural	Automatic	Manual / Procedural	Automatic
The access control privileges of a user account or a role are modified	✓		✓	✓
<b>CERTIFICATE PROFILE MANAGEMENT</b>				
All changes to the certificate profile	Cert Profile not captured in Directory	Cert Profile not captured in Directory	✓	
<b>REVOCACTION PROFILE MANAGEMENT</b>				
All changes to the revocation profile	Revocation Profile not captured in Directory	Revocation Profile not captured in Directory	✓	
<b>CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT</b>				
All changes to the certificate revocation list profile	Certificate Revocation List Profile not captured in Directory	Certificate Revocation List Profile not captured in Directory	✓	
<b>MISCELLANEOUS</b>				
<i>Installation of the Operating System</i>	✓		✓	

Auditable Event	FBCA Directories		FBCA CAs	
	Manual / Procedural	Automatic	Manual / Procedural	Automatic
<i>Installation of the FBCA CA</i>	Applies to CA only	Applies to CA only	✓	✓
<i>Installing hardware cryptographic modules</i>	Applies to CA only	Applies to CA only	✓	✓
<i>Removing hardware cryptographic modules</i>	Applies to CA only	Applies to CA only	✓	
<i>Destruction of cryptographic modules</i>	Applies to CA only	Applies to CA only	✓	
<i>System Startup</i>	✓		✓	
<i>Logon Attempts to FBCA CA Apps</i>	Applies to CA only	Applies to CA only		✓
<i>Receipt of Hardware / Software</i>	✓		✓	
<i>Attempts to set passwords</i>	✓			✓
<i>Attempts to modify passwords</i>	✓			✓
<i>Backing up FBCA-CA internal database</i>	Applies to CA only	Applies to CA only		✓
<i>Restoring FBCA CA internal database</i>	Applies to CA only	Applies to CA only		✓
<i>File manipulation (e.g., creation, renaming, moving)</i>		✓		✓
<i>Posting of any material to a repository</i>		✓		✓
<i>Access to FBCA CA-internal database</i>	Applies to CA only	Applies to CA only	✓	✓
<i>All certificate compromise notification requests</i>	Applies to CA only	Applies to CA only	✓	

Auditable Event	FBCA Directories		FBCA CAs	
	Manual / Procedural	Automatic	Manual / Procedural	Automatic
<i>Loading tokens with certificates</i>	Applies to CA only	Applies to CA only	✓	
<i>Shipment of Tokens</i>	Applies to CA only	Applies to CA only	✓	
<i>Zeroizing tokens</i>	Applies to CA only	Applies to CA only	✓	
<i>Rekey of the FBCA CA</i>	Applies to CA only	Applies to CA	✓	
<i>Configuration changes to the CA server involving:</i>	Applies to CA only	Applies to CA only	✓	
<i>Hardware</i>	Applies to CA only	Applies to CA only	✓	
<i>Software</i>	Applies to CA only	Applies to CA only	✓	
<i>Operating System</i>	Applies to CA only	Applies to CA only	✓	✓
<i>Patches</i>	Applies to CA only	Applies to CA only	✓	✓
<i>Security Profiles</i>	Applies to CA only	Applies to CA only	✓	✓
<b>PHYSICAL ACCESS / SITE SECURITY</b>				
<i>Personnel Access to room housing FBCA CA</i>	✓	✓	✓	✓
<i>Access to the FBCA CA server</i>	Applies to CA only	Applies to CA only	✓	✓

Auditable Event	FBCA Directories		FBCA CAs	
	Manual / Procedural	Automatic	Manual / Procedural	Automatic
<i>Known or suspected violations of physical security</i>	✓	✓	✓	✓
<b>ANOMALIES</b>				
<i>Software Error conditions</i>	✓	✓	✓	✓
<i>Software check integrity failures</i>	✓	✓	✓	✓
<i>Receipt of improper messages</i>	✓	✓	CA is stand alone	CA is stand alone
<i>Misrouted messages</i>	✓	✓	CA is stand alone	CA is stand alone
<i>Network attacks (suspected or confirmed)</i>	✓	✓	CA is stand alone	CA is stand alone
<i>Equipment failure</i>	✓	✓	✓	✓
<i>Electrical power outages</i>	✓	✓	✓	✓
<i>Uninterruptible Power Supply (UPS) failure</i>	✓	✓	✓	✓
<i>Obvious and significant network service or access failures</i>	✓	✓	CA is stand alone	CA is stand alone
<i>Violations of Certificate Policy</i>	✓	Certain Violations as documented by this table	✓	Certain Violations as documented by this table
<i>Violations of Certification Practice Statement</i>	✓	Certain Violations as documented by this table	✓	Certain Violations as documented by this table

Auditable Event	FBCA Directories		FBCA CAs	
	Manual / Procedural	Automatic	Manual / Procedural	Automatic
<i>Resetting Operating System clock</i>	✓		✓	

**4.5.2 Frequency of processing data**

The FBCA AO Auditor reviews audit logs at least once per month as defined in section 5.2. The FBCA OA Auditor will examine 100% of security audit data generated by the FBCA since the last review. All security alerts and irregularities are explained in an audit log summary. The FBCA OA Auditor 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 are documented.

**4.5.3 Retention period for security audit data**

Audit logs are retained offsite at the interim storage area for three months. The FBCA OA System Administrator removes audit logs from the FBCA and gives them to the FBCA OA Auditor neither of whom commands the FBCA CA signature key(s).

**4.5.4 Protection of security audit data**

The compliance audit process is not, done by, or under the control of, the FBCA OA. The FBCA OA Auditor performs routine review of security audit logs. The procedure for protecting security audit data is as follows:

1. Security audit logs are automatically time stamped upon creation
2. The only authorized people having read access to the logs include the FBCA OA Administrator, Security Officer, Auditor, Operator, and others possibly designated by the FPKIPA ;
3. Only the FBCA OA Auditor is authorized to archive audit logs.
4. Audit logs are deleted only under procedural multi-person control.
5. Audit logs are protected under multi-person control and cannot be modified without detection.

Daily audit logs are generated on time stamped digital tape media and are protected from deletion and/or modification prior to the end of the audit log retention period. See

sections 4.5.5, 4.5.6, 4.6, and 5.0 for descriptions of physical and procedural controls for protection of the data.

#### **4.5.5 Security Audit data backup procedures**

##### FBCA Directory:

Audit logs and audit summaries are incrementally backed up daily via time stamped digital tape media. Full backups are performed weekly (i.e., on a fixed week day) and monthly (i.e., on a fixed day of the month) via digital tape media. Weekly and monthly backups are stored in secure container in a separate building from the FBCA facility. Monthly backups are moved to the archive location quarterly. The weekly and daily backup tapes are securely erased and reused after three months. Additionally, backups are performed at the hot site location to ensure continuity; shadowing the primary directory and performing weekly backups accomplish this.

##### FBCA CAs:

Full backups are performed weekly (i.e., on a fixed week day) and monthly (i.e., on a fixed day of the month) via digital tape media. Weekly and monthly backups are stored in secure container in a separate building from the FBCA facility. Monthly backups are moved to the archive location quarterly. The weekly backup tapes are securely erased and reused after three months.

Manual audit logs will be collected weekly and stored in a secure container in a separate building from the FBCA facility. These audit logs are moved to the archive location quarterly.

#### **4.5.6 Security Audit collection system (internal vs. external)**

The audit log collection system is internal to the FBCA components (see section 4.5.1). Audit processes are 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 OA will determine whether to suspend FBCA operation until the problem is remedied. Section 4.5.1 describes the collection procedures (manual or automatic) for the auditable events. Section 4.5.5 describes the protection procedures for backing up audited data that has been collected.

#### **4.5.7 Notification to event-causing subject**

The FBCA OA will notify the FPKIPA regarding any events requiring suspension of FBCA operation due to compromise of the security audit collection system.

#### **4.5.8 Vulnerability Assessments**

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

The Mitretek Systems Security Center will perform vulnerability assessments as part of security compliance audits as specified by the FPKIPA.

The FBCA OA provides a report of the analysis of the results of vulnerability assessments, specifically indicating security vulnerabilities identified and correction procedures of those vulnerabilities.

### **4.6 RECORDS ARCHIVAL**

#### **4.6.1 Types of events archived**

The FBCA OA Auditor produces archive records on a quarterly basis. The records are stored on a removable storage medium (i.e., paper, tape, CD-ROM). The archive records include data received from the certificates and CRLs it generated, certificate requests and certificate revocation requests it received.

At initialization, the FBCA system equipment configuration files are archived, as well as the CPS and any contractual agreements to which the FBCA OA is bound. During FBCA operation, the following data are recorded for archive

- FBCA certification and accreditation
- Certification Practice Statement
- Contractual obligations
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- Revocation requests
- Subscriber identity Authentication data as per Section 3.1.9
- Documentation of receipt and acceptance of certificates
- Documentation of receipt of tokens
- All certificates issued or published

- Record of Re-key
- All CARLs and CRLs issued and/or published
- All Audit Logs
- Other data or applications to verify archive contents
- Documentation required by compliance auditors

See Section 4.5 for a description of the audit and archive collection procedures.

#### **4.6.2 Retention period for archive**

Archive records are kept for a period of at least twenty years, six months. The same applications identified in section 4.6.1, above, required to process the archive data (e.g., CA software)) are also maintained for a period determined by the FPKIPA for the FBCA..

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site and approved by the FBCA OA and FPKIPA. The FBCA archive site is:

This information, clearly “about critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a)(i), §3544(A)(1)(a)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3545(f), as well as GSA Orders 1800.3C (draft) and PBS 3490.1, is omitted in the publicly universally available version of this document. This information is available upon request to authorized organizations with a need to know.

Prior to the end of the archive retention period, the FBCA will provide the archived data and the applications necessary to read the archives to the FPKIPA.

#### **4.6.3 Protection of archive**

Long-term protection of the archive is provided by use of 4mm digital tape.

Archive data is clearly labeled as follows:

- Classification Label: SBU

- Name of the Program: FBCA
- Type of item (e.g., Entrust CA Log Report)
- Start Date through End Date
- Copy control number.

Long-term archive data for the FBCA is stored on site at the location listed in section 4.6.2.

Short-term media (i.e., one month's storage) that contains archive data for the FBCA is stored in a location separate from the FBCA equipment, at the following location:

This information, clearly "about critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a)(i), §3544(A)(1)(a)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3545(f), as well as GSA Orders 1800.3C (draft) and PBS 3490.1, is omitted in the publicly universally available version of this document. This information is available upon request to authorized organizations with a need to know.

This facility is temperature controlled and behind locked doors.

The FBCA Auditor maintains a list of individuals who can access and delete the on-line archive files. Deletion of on-line archive files is accomplished under multi-person control procedures.

Once the on-line archive is written to tape, it cannot be modified. The equipment used to create the tape archive is secured under multi-person control procedures. The contents of the archive will not be released except as determined by the FPKIPA or as required by law.

#### **4.6.4 Archive backup procedures**

Archive records are backed-up as part of the nightly normal system backup procedure to single session, 4mm digital tapes.

Incremental backups are performed nightly. Full system backups are performed to weekly and monthly to digital tape removable storage media.

Weekly and monthly backups are stored at the short-term archive facility described in Section 4.6.3. Quarterly backups are stored at the long-term archive facility described in Section 4.6.2.

#### **4.6.5 Requirements for time-stamping of records**

Records will be clearly labeled with date/time period information of the data contained in the record as described in section 4.6.3.

#### **4.6.6 Archive collection system**

The archive information will be collected by the FBCA OA Auditor, who will be responsible for maintaining the integrity of the archived data.

#### **4.6.7 Procedures to obtain and verify archive information**

Creation of archive data via digital tape is described in section 4.6.3. The FBCA OA Auditor verifies the archive by reading the digital tape directories and viewing the files listed by size and date to compare that information with the source archive information. The archive data is placed in clearly labeled, double wrapped packaging for transport to short-term and long-term archive locations. Transport of archive data is via hand carry for short-term archive is via hand carry by the FBCA Auditor. Transport of archive data is via hand carry by the FBCA Auditor or approved courier services. Storage and protection of archive data is described in section 5.

The FBCA OA auditing official will maintain logging information (and receipts) as archived data is transported to short-term and long-term archive facilities.

### **4.7 KEY CHANGEOVER**

The FBCA key changeover procedures are as follows:

- The FBCA CA will generate a self-issued certificate signed by the old private key whose subjectPublicKeyInfo field contains the new public key.
- The FBCA CA will generate a self-issued certificate signed by the new private key whose subjectPublicKeyInfo field contains the old public key.
- The FBCA CA will generate a self-issued certificate signed by the new private key whose subjectPublicKeyInfo field contains the new public key.
- The FBCA CAs and all Agency PCAs will process new cross-certificates as described in this CPS.
- All certificates generated as part of the key changeover process will be posted to the FBCA repository.

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

The FBCA will support Agency PCA key changeovers by issuing and posting new certificates as required.

#### **4.8 COMPROMISE AND DISASTER RECOVERY**

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

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

1. Notification of the GSA Designated Official For Facilities (DOFF) and Facility Emergency Response Team Leader (FERTL). These individuals along with the FBCA OA will assess the outage and determine whether all or part of the Recovery team needs to be assembled.
2. Activation of the recovery team
3. Based on the severity of the event, activate the recovery procedures for that severity type
4. Interface with the FBCA OA Management team
5. If the severity/scenario (to exceed 6 hours) of the event is critical, activation of the alternate site (hot site).
6. The FBCA POCs (“hot list”) will be notified of this change, so that any changes required by the Agency PCAs can be performed
7. Manage the recovery process of the primary FBCA facility.

Submit post recovery logs to FPKIPA

In order to provide 6-hour window for FBCA service re-activation, the FBCA OA has implemented a synchronized hot site. The hot site will include an identical configuration of the primary site. The FBCA directory entertains a supplier shadowing agreement whereas shadowing occurs when the supplying DSA initiates the exchange with the alternate FBCA directory. Shadows occur according to the X.500 DISP whenever the primary DSA is updated (CRLs/CARLs, cross-certificates). The hot site FBCA CA is quickly restored via backup tapes.

During system restoration the FBCA will need to ensure CARLs/CRLs are current with their respective Agency PCAs. Additionally, cross-certificates need to be validated and new public keys/cross-certificates issued in the event anomalies exist.

The following reports are generated:

1. Activity log – this log is maintained throughout the disaster recovery process.

2. Test plan results
3. Equipment list – Update configuration management
4. Restoration Expense report

The FBCA hot site will be in operation within 90-days following full initial operation of the primary FBCA site. In the event recovery of the primary site is required during this time period, the recovery process will be performed and completed as quickly as possible. Notification of all parties will be performed as described above.

#### **4.8.2 FBCA signature keys are revoked**

Within 6 hours, the FBCA OA will securely advise (via callback and challenge-response) the FPKIPA and all of the FBCA POC “hot list” in the event of a disaster where the FBCA installation is physically damaged and all copies of the FBCA signature keys are destroyed.

The FBCA AO will securely (via callback and challenge-response) notify via telephone the FBCA POC “hot list,” if the FBCA cannot issue a CARL/CRL within 6 hours.

The FPKIPA will determine whether to revoke the FBCA certificate issued to the Agency PCAs.

The FBCA OA will reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in section 4.8.1.

#### **4.8.3 FBCA signature keys are compromised**

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

1. The FPKIPA and all of its member agencies (the POCs holist is retrieved from the secure storage container) will be securely notified (so that agencies may issue CARLs revoking any cross-certificates issued to the FBCA) via telephone (via callback and challenge-response) to the designated POCs;
2. The PCAs that have issued certificates to the FBCA will publish a CARL revoking the cross-certificate issued to the FBCA as set forth above;
3. The FBCA CA will generate a new FBCA CA key pair in accordance with procedures set forth in section 4.2
4. New FBCA certificates will be issued to Agency PCAs also in accordance with section 4.2.

The FBCA OA will also investigate and report to the FPKIPA 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**

The FBCA servers will operate with back-up power and telecommunications and appropriate infrastructure system redundancies, and, therefore, no outages longer than 24-hours are anticipated. However, if an outage is anticipated to become, or becomes, an extended outage, the disaster recovery plan will come into effect. An extended outage is defined as one in which the ability of FBCA to revoke certificates cannot be re-established within 24 hours. The details of this plan are defined in the FBCA Disaster Recovery Plan.

In the case of a disaster whereby the FBCA primary installation is physically damaged and all copies of the FBCA signature key are destroyed as a result, the FPKIPA and all of its member agencies will be securely notified (via callback and challenge-response), and the procedures described in section 4.8.1 will be followed. The FBCA installation will then be completely rebuilt, by reestablishing the FBCA equipment, generating new private and public keys, being re-certified, and re-issuing all cross certificates.

#### **4.9 CA TERMINATION**

In the event of termination of the FBCA operation, certificates signed by the FBCA will be revoked and the FPKIPA will advise agencies that have entered into MOAs with the FPKIPA that FBCA operation has terminated so they may revoke certificates they have issued to the FBCA. Prior to FBCA termination, the FBCA will provide archived data to a FPKIPA approved archival facility.

Agencies 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.

### **5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS**

#### **5.1 PHYSICAL CONTROLS FOR THE FBCA OR AGENCY CA**

The FBCA imposes physical security requirements that provide similar levels of protection as those specified below. All the physical control requirements apply to the FBCA.

This information, clearly “about critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a)(i), §3544(A)(1)(a)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3545(f), as well as GSA Orders 1800.3C (draft) and PBS 3490.1, is omitted in the publicly universally available version of this document. This information is available upon request to authorized organizations with a need to know.

### **5.1.1 Site location and construction**

This information, clearly “about critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a)(i), §3544(A)(1)(a)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3545(f), as well as GSA Orders 1800.3C (draft) and PBS 3490.1, is omitted in the publicly universally available version of this document. This information is available upon request to authorized organizations with a need to know.

### **5.1.2 Physical access**

This information, clearly “about critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a)(i), §3544(A)(1)(a)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3545(f), as well as GSA Orders 1800.3C (draft) and PBS 3490.1, is omitted in the publicly universally available version of this document. This information is available upon request to authorized organizations with a need to know.

### **5.1.3 Electrical Power**

This information, clearly “about critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a)(i), §3544(A)(1)(a)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3545(f), as well as GSA Orders 1800.3C (draft) and PBS 3490.1, is omitted in the publicly universally available version of this document. This information is available upon request to authorized organizations with a need to know.

#### **5.1.4 Water exposures**

The FBCA CA room implements water protection safeguards equivalent to those implemented for the GSA FTS computer room.

#### **5.1.5 Fire prevention and protection**

The FBCA CA room implements fire prevention and protection safeguards equivalent to those implemented for the GSA FTS computer room.

#### **5.1.6 Media storage**

The FBCA CA room also includes a small safe, fireproof locked cabinets, and a desk where media is stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive, or backup information is stored at a different location separate from the FBCA (i.e. in a separate GSA Office located in an offsite building for short term storage, specified in section 4.6.3) and after three months it is transported to long-term site specified in section 4.6.2.

#### **5.1.7 Waste disposal**

No stipulation.

#### **5.1.8 Off-site backup**

For the FBCA full system backups, sufficient to recover from total system failure, are conducted on a periodic schedule, described in section 4.5. The short-term backup site specified in section 4.6.3 and contains up to three months worth of backup information. The long-term backup site is specified in section 4.6.2.

### ***5.2 PROCEDURAL CONTROLS FOR THE FBCA AND AGENCY 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 are responsible for the integrity of the CA. The functions performed in these roles form the basis of trust for all uses of the FBCA. 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 encompasses CA products from several vendors. Different commercial products support somewhat different roles, and use different mechanisms for registering or enrolling subscribers and issuing certificates:

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, including:

- 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 is operating in accordance with this CPS;

#### **5.2.1.4 Operator**

The operator role is responsible for the routine operation of the FBCA 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, is enforced either by the FBCA equipment, or procedurally, or by both means.

The separation of roles for the FBCA, which is operated at the high assurance level, is as follows:

- Individual FBCA OA personnel are 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. 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.

The Operator role may be assumed by the Administrator, Officer, and/or Auditor.

Separation of roles is accomplished through the use of DataKey hardware tokens and procedures that ensure separation of roles and multi-person control of the FBCA CA where required and specified in section 5.1.2.

This information, clearly “about critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a)(i), §3544(A)(1)(a)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3545(f), as well as GSA Orders 1800.3C (draft) and PBS 3490.1, is omitted in the publicly universally available version of this document. This information is available upon request to authorized organizations with a need to know.

Once the Entrust CA is activated, access to the CA private signing key for issuance and revocation of cross-certificates requires a minimum of 2 officers, who are authenticated via individual DataKey smartcards.

Audit log data is generated automatically by Entrust CA for all access and CA activities.

### 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, with the exception of operator. The separation provides a set of checks and balances over the FBCA operation.

Under no circumstances does the incumbent of a FBCA role perform its own auditor function.

#### **5.2.4 Identification and authentication for each role**

Individuals 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**

The FPKIPA and the FBCA OA are responsible and accountable for the operation of the FBCA

All persons filling trusted roles are selected on the basis of loyalty, trustworthiness, and integrity, and are U.S. citizens. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the FBCA are set forth in Appendix X of this CPS.

All unescorted FBCA personnel hold TOP SECRET security clearances.

#### **5.3.2 Background check procedures**

FBCA personnel background checks are performed in accordance with TOP SECRET security clearance requirements.

#### **5.3.3 Training Requirements**

All personnel performing duties with respect to the operation of the FBCA receive comprehensive training. One-on-one training is conducted in the following areas by certified product engineers:

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

Training in the overall security procedures of the FBCA is conducted for all personnel at the initial full operation capability of the FBCA. Training and review of security procedures is conducted at the time a change in procedures occurs and/or annually. Personnel are required to sign acknowledgements that they have received this training.

#### **5.3.4 Retraining frequency and requirements**

Individuals responsible for trusted roles are made aware of changes in the FBCA operation as described personnel training procedures documentation Any significant change to the operations are documented and personnel are informed and made aware of changes in accordance with the personnel training procedures. Examples of such changes are FBCA software or hardware upgrades, 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 FPKIPA takes appropriate administrative and disciplinary actions against personnel who have performed unauthorized actions involving the FBCA or its repository. .

#### **5.3.7 Contracting personnel requirements**

Contractor personnel employed to perform functions pertaining to the FBCA meet applicable requirements set forth in the FBCA CP and this CPS as determined by the FBCA OA.

#### **5.3.8 Documentation supplied to personnel**

The FBCA makes available to all of its personnel the FBCA CP, CPS, and any relevant statutes, policies or contracts. Documentation identifying all personnel receiving and completing training is maintained by the FBCA OA.

## **6. TECHNICAL SECURITY CONTROLS**

### ***6.1 KEY PAIR GENERATION AND INSTALLATION***

#### **6.1.1 FBCA and CA key pair generation**

The key pair for the FBCA CAs are generated on the Chrysalis LunaCA3 cryptographic module. The key pair generation is RSA for digital signature in compliance with PKCS-1 (FIPS 140-1, level 3). The private key will never be exposed outside the module in unencrypted form. Backup copies of the LunaCA3 private keys will be created.

#### **6.1.2 Private Key Delivery to Subscriber**

The Agency PCA generates its own key pair and therefore does not need private key delivery.

### **6.1.3 Public Key Delivery to Certificate Issuer**

Public keys are delivered to the certificate issuer electronically in a certificate request (i.e., using PKCS #10) messages to the FBCA OA via secure non-electronic means (e.g., floppy disk delivered by registered mail or courier) as described in section 4.2. . Identity checking and proof of possession of the private key will be accomplished as described in section 4.1.

### **6.1.4 FBCA cross-certificates and public key availability and delivery to Agency PCAs**

The FBCA will post all cross-certificates it issues in the FBCA repository. The FBCA will also post all cross-certificates issued by the Agency PCAs to the FBCA. The FBCA and Agency PCA public keys will be transported in a secure, out-of-band mechanism, using PKCS#10 messages via e-mail or floppy disk delivered by registered mail or courier.

### **6.1.5 Key sizes**

Public key sizes are 1024 bits for RSA, SHA-1, in accordance with FIPS 186.

### **6.1.6 Public key parameters generation**

There are no public key parameters for RSA.

### **6.1.7 Parameter quality checking**

There are no public key parameters for RSA.

### **6.1.8 Hardware/Software key generation**

The FBCA CA key pairs are generated in a FIPS 140-1 Level 3 validated, LunaCA3 hardware cryptographic module.

Key pairs for trusted roles and provision of multi-person controls are generated in a FIPS 140-1 Level 2 validated DataKey SmartCard cryptographic module.

### **6.1.9 Key usage purposes (as per X.509 v3 key usage field)**

Keys are certified for use in a combination of digital signature and non-repudiation. Two key usage bits: *cRLSign* and *CertSign*, are set in FBCA certificates.

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

## **6.2 PRIVATE KEY PROTECTION**

### **6.2.1 Standards for cryptographic module**

The CA private keys are protected using FIPS 140-1 Level 3 validated cryptographic module: Chrysalis LunaCA3 hardware token.

Key pairs for FBCA separation of roles are generated in a FIPS 140-1 Level 2 validated cryptographic module. DataKey SmartCards

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

See section 5.2.2 for a description of the procedures used for accessing and operating the Entrust CA.

### **6.2.2 FBCA private key multi-person control**

All CA private keys shall be under 2 out of N control, where  $N \geq 2$ . See Section 6.2.7 for details on how this is achieved.

### **6.2.3 Key Escrow of FBCA private signature key**

The FBCA CA signature keys used to support non-repudiation services are not escrowed by a third-party.

### **6.2.4 Private Key Backup**

One secure backup of the FBCA CA private keys has been made following procedures described in the Chrysalis operations manuals. The private keys backup has been stored at the FBCA interim storage site. No FBCA private keys will be archived.

### **6.2.5 Private Key Archival**

(See section 6.2.3)

### **6.2.6 Private key entry into cryptographic module**

FBCA CA private keys are generated by and remain in a cryptographic module. The Chrysalis product uses proprietary secure means for transferring keys from one cryptographic module to another to back up the CA keys.

### **6.2.7 Method of activating private keys**

This information, clearly “about critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the

security of Federal facilities and persons in those facilities” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a)(i), §3544(A)(1)(a)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3545(f), as well as GSA Orders 1800.3C (draft) and PBS 3490.1, is omitted in the publicly universally available version of this document. This information is available upon request to authorized organizations with a need to know.

Procedures for activating and using the private keys are provided in section 5.2.2. See section 5.1.2 for a description of physical protection procedures for the hardware tokens.

### **6.2.8 Methods of deactivating private keys**

The LunaCA3 cryptographic module will be deactivated and stored in a secure container when not in use.

This information, clearly “about critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a)(i), §3544(A)(1)(a)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3545(f), as well as GSA Orders 1800.3C (draft) and PBS 3490.1, is omitted in the publicly universally available version of this document. This information is available upon request to authorized organizations with a need to know.

### **6.2.9 Method of destroying private signature keys**

The triple-DES encrypted key blobs on the hard drive are destroyed and the administrator tokens reinitialized, under the same multi-person control procedures used to initially generate the key pairs described above. Note that if the tokens are not reinitialized, they could be used to restore the key with any backup copy of the key blobs.

## **6.3 GOOD PRACTICES REGARDING KEY-PAIR MANAGEMENT**

### **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 CA private signing keys will be used to sign certificates for one-half of the certificate lifetime (e.g. for 2 years if the certificate lifetime is 4 years). The certificate lifetime will be valid not more than 6 years. Entrust CA issues certificates with a validity period of 5 years. Rekeying will be performed after 2.5 years.

## **6.4 ACTIVATION DATA**

### **6.4.1 Activation data generation and installation**

On the Chrysalis device, the Datakey tokens take the place of PINs for enabling use of the CA private signing keys. These tokens satisfy the policy enforced by Chrysalis. Once the use of the CA private signing keys are enabled, actual use of the private signing keys is under multi-person control through the use of DataKey Smart Card tokens. Activation data for accessing the smart cards complies with FIPS 112. .

### **6.4.2 Activation data protection**

Activation data shall be 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.

Note that on the Chrysalis unit, the activation data is on physical tokens. These tokens are locked in secure containers. The M of N keys are stored in separate containers locked using devices for which no one person has access to both combinations and keys.

Activation data will never be shared.

Entrust CA is configured to temporarily lock out access following three unsuccessful login attempts.

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

### **6.4.3 Other Aspects of Activation Data**

Passwords are changed periodically to decrease the likelihood of discovery. The cryptographic module activation data will be changed not less than once every three months

## **6.5 COMPUTER SECURITY CONTROLS**

### **6.5.1 Specific computer security technical requirements**

The FBCA CA servers are operated on dedicated workstations with no network services and/or connections to external networks.

The FBCA repository is operated on a dedicated workstation and will only run the network services required to operate the repository and to support on-line certificate validations by agency CA subscribers (i.e., LDAP, DNS).

The FBCA CA servers use configurations that have been clearly demonstrated and passed the Compliance Audit process as described in section 2.7.

The FBCA CA equipment is configured with appropriate security features turned on as recommended by the host operating system vendor in accordance with any associated security validation rating. The Entrust CA has the following security features and functions:

- Requires authenticated logins via FIPS PUB 140-1, Level 3 and Level 2 cryptographic modules
- Provides Discretionary Access Control via permissions and policies defined in the Entrust CA software
- Provides a security audit capability via automatic logging of all CA activity
- Restricts access control to FBCA services and PKI roles as described in sections 5.1.2 and 5.2.2
- Enforces separation of duties for PKI roles as described in sections 5.1.2 and 5.2.2
- Requires identification and authentication of PKI roles and associated identities as described in sections 5.1.2 and 5.2.2
- Prohibits object re-use or require separation for FBCA random access memory. It is assumed that verification of meeting this requirement is provided by the NT operating system. NT enforces the required prohibition/separation. NT was evaluated under IT SEC E3/FC2, since the FC2 functional package is equivalent to the Orange Book's C2, it includes the required memory protection controls. More information on the NT evaluation is available at:  
<http://www.microsoft.com/presspass/press/1999/Apr99/UKSecurPR.asp>.
- Requires use of cryptography for session communication and database security. The use of cryptography for session communication is not required because the certificate request messages (PKCS#10) are exchanged using an out-of-band mechanism and are imported manually directly at the CA. The Entrust CA database is protected via triple-DES cryptography.
- Archives FBCA history and audit data through data collection and archive procedures described in sections 4.5 and 4.6
- Requires self-test security related FBCA services. Entrust CA security audit logs are signed objects and the software verifies those objects at startup and each time the logs are accessed. If the verification changes, the software provides a dialogue box “alarm” through the user interface and logs the event.

- Requires a trusted path for identification of PKI roles and associated identities logins via FIPS PUB 140-1, Level 3 and Level 2 cryptographic modules. Requires a recovery mechanisms for keys and the FBCA system through backup and protection procedures described in 4.5.5
- Enforces domain integrity boundaries for security critical processes through self-test procedures described above

### **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 are as follows:

- The Entrust CA software is commercial- off-the-shelf software that has been developed under a very formal development process that is well documented..
- Hardware procured to operate the FBCA has been purchased in a fashion whereby the provider does not know that it is intended for the FBCA operations. The Entrust CA software has been ordered and installed by Entrust certified engineers under the direction and control of authorized FBCA operation personnel. Hardware and software updates will be purchased or developed in the same manner as the original equipment and will be installed by trusted and trained personnel.
- All software and hardware installed in or run on the FBCA CA server will be purchased using commercial buys. Hardware and non-CA software is purchased randomly, through standard procurement procedures provided by the FBCA OA. An accountable method of packaging and delivery will be used to provide a continuous chain of accountability from the vendor to the facility (e.g., UPS, Federal Express, USPS Express Mail). The FBCA establishes a relationship with the CA software vendors prior to acquisition that gives assurance that the software has not been tampered with. Installation is performed under multi-person control with only authorized FBCA operation personnel.
- Proper care is taken to prevent malicious software from being loaded onto the FBCA equipment. From the time the software is received, it remains under continuous control. All shrink wrapped packaging is opened and installed inside the secure FBCA facility under multi-person control. Norton AntiVirus will be used to scan all applications and files for malicious code, initially, periodically, and any time a new file is introduced to the system. Vulnerability assessments are conducted at startup, periodically, and any time a system configuration change occurs (i.e., adding a new

CA to the FBCA). Two or more of the following risk assessment tools are used: Internet System Security (ISS), CyberCop, Saint, and NMAP.

### **6.6.2 Security management controls**

The initial configuration of the FBCA software (i.e., CA software, repository software) as well as any modifications and upgrades will be documented and controlled in accordance with FBCA Configuration Management Procedures (separate FBCA OA document). System and application level logging will be enabled and reviewed weekly to maintain the ongoing integrity of the software and configuration. The source for the software is described in section 6.6.1 above.

## **6.7 NETWORK SECURITY CONTROLS**

Each FBCA CA is connected only with its own directory within the FBCA CA Room. They will not be connected to any network external to the FBCA, nor to FBCA repository.

The FBCA repository will be connected to the Internet to provide continuous service. The directory server is protected behind a firewall and is housed in rack. Information is transported from the Internal Directories to the FBCA repository using floppy disks.

The FBCA repository supports TCP/IP, DSP, and, as directed by the FPKIPA, LDAP V2 or better protocols for operation and interoperability of the repository with Agency PCA directories, including support for X.500 directory chaining, referrals, and cross-referencing mechanisms.

The FBCA firewall permits passage of only DSP and, as directed by FPKIPA, LDAPv2 or better.

Network monitoring software is implemented to monitor performance of the FBCA on-line directory as a countermeasure for Denial of Service Attacks.

## **6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS**

Requirements for cryptographic modules are as stated above in Section 6.2

## **7. CERTIFICATE AND CARL/CRL PROFILES**

The FPKIPA has defined the Certificate and CARL/CRL profiles used by the FBCA. The profiles are described in the FBCA Interoperability Guidelines, however, for ease of reference, this CPS also includes their description in the following sections.

### 7.1 CERTIFICATE PROFILE

The FBCA will issue certificates in accordance with the following certificate profile:

Field	Criticality Flag	Field contents	Comments
Certificate			
tbsCertificate			Fields to be signed.
<b>version</b>		2	Integer Value of "2" for Version 3 certificate.
<b>serialNumber</b>			
CertificateSerialNumber		INTEGER	Positive integer, unique for the set of certificates issued by this CA
<b>signature</b>			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field.
algorithm		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
parameters		NULL	Always NULL for rsa with SHA-1
<b>issuer</b>			
Name			C=US, O=U.S. Government, OU=FBCA, OU=<product name>
RDNSquence			C= ; O= ; and OU= are required
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	

Field	Criticality Flag	Field contents	Comments
AttributeValue		See comment.	use printableString (first choice), or bmpString (second choice) [Note: utf8string must be used in all certificates after December 31st, 2003.]
<b>validity</b>			
notBefore			
Time			
utcTime			
UTCTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime			[This encoding should not required until 2050.]
GeneralizedTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
notAfter			
Time			
utcTime			
UTCTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime			[This encoding should not required until about 2044.]
GeneralizedTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
<b>subject</b>			
Name			X.500 Distinguished name of the owner of the certificate.

Field	Criticality Flag	Field contents	Comments
RDNSequence			C= ; O= ; OU= ; CN= ; and DC= are required.
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	The string types used to encode the subject name must match the issuer name encoding in certificates issued by this subject.
<b>subjectPublicKeyInfo</b>			
algorithm			
AlgorithmIdentifier			Public key algorithm used.
The next two entries apply only to RSA Public keys			
algorithm		1.2.840.113549.1.1.1	RSA Encryption
parameters		NULL	Always assert NULL in the parameters for RSA public keys
The next two entries apply only to DSA Public Keys			
algorithm		1.2.840.10040.4.1	DSA
parameters		dss-parms	Always include the parameters for DSA public keys; syntax is defined in RFC 2459.
The next entry applies to both DSA and RSA Public Keys			
subjectPublicKey		BIT STRING	

Field	Criticality Flag	Field contents	Comments
<b>extensions</b>			
<b>authorityKeyIdentifier</b>	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
<b>subjectKeyIdentifier</b>	FALSE		
keyIdentifier		OCTET STRING	Must match the authorityKeyIdentifier in certificates issued by the subject whose signature can be validated using the subjectPublicKey. Use the key identifier provided by the subject.
<b>keyUsage</b>	TRUE		
digitalSignature		1	This value MAY be asserted.
nonRepudiation		1	This value MAY be asserted.
keyEncipherment		0	This value MUST NOT be asserted.
dataEncipherment		0	This value MUST NOT be asserted.
keyAgreement		0	This value MUST NOT be asserted.
keyCertSign		1	REQUIRED. This value MUST be asserted.
cRLSign		1	This value MAY be asserted.
encipherOnly		0	This value MUST NOT be asserted.

Field	Criticality Flag	Field contents	Comments
decipherOnly		0	This value MUST NOT be asserted.
<b>certificatePolicies</b>	FALSE		MUST be able to assert a sequence of between one and four policies, inclusive.
PolicyInformation			
policyIdentifier			
CertPolicyId		OID	May be any of the following: {2.16.840.1.101.3.2.1.3.1, 2.16.840.1.101.3.2.1.3.2, 2.16.840.1.101.3.2.1.3.3, 2.16.840.1.101.3.2.1.3.4}
policyQualifiers			Policy qualifiers MUST NOT appear.
<b>policyMappings</b>	FALSE		This extension will appear in all certificates issued to Agency PCAs. This extension does not appear in certificates issued to other FBCA nodes.  This extension will be non-critical in all certificates issued by the FBCA; this extension may be critical in certificates issued to the FBCA to ensure policy mapping is processed by its relying parties.
issuerDomainPolicy			
CertPolicyId		OID	OID of policy from the FBCA domain that maps to the equivalent policy in

Field	Criticality Flag	Field contents	Comments
			to the equivalent policy in the subject CA's domain.  May be any of the following: {2.16.840.1.101.3.2.1.3.1, 2.16.840.1.101.3.2.1.3.2, 2.16.840.1.101.3.2.1.3.3, 2.16.840.1.101.3.2.1.3.4}
subjectDomainPolicy			
CertPolicyId		OID	OID of policy in the subject CA's domain that maps to the equivalent policy in the issuing CA's domain.
<b>basicConstraints</b>	TRUE		
cA		TRUE	Default is False.
pathLenConstraint		INTEGER	This field is omitted where path length constraints are not imposed by the FBCA.
<b>nameConstraints</b>	TRUE		MUST appear in every certificate issued by the FBCA to a PCA. MUST NOT appear in certificates issued to other FBCA nodes.
permittedSubtrees			MUST appear in every certificate issued by the FBCA to a PCA. This field will identify legal agency name spaces.
GeneralSubtree			Support for DN name form is required. Support for DNS names and rfc 822 names is

Field	Criticality Flag	Field contents	Comments
			recommended.
base			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	Must match string types used to encode names in certificates issued by the subject of this certificate.
uniformResourceIdentifier		IA5String	
minimum			
BaseDistance		0	Default value of zero.
maximum			Always omitted.
BaseDistance		INTEGER	Always omitted.
excludedSubtrees			Only used if a portion of the agency PKI name space is explicitly rejected by the FBCA.
GeneralSubtrees			
GeneralSubtree			
base			

Field	Criticality Flag	Field contents	Comments
GeneralName			
directoryName			
Name			
RDNSSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	utf8string must be used in all certificates after December 31st, 2003. Prior to that, if possible, use printableString (first choice), or bmpString (second choice)
uniformResourceIdentifier		IA5String	
minimum			
BaseDistance		0	Default value of zero.
maximum			Always omitted.
BaseDistance		INTEGER	Always omitted.
<b>policyConstraints</b>	TRUE		This extension only appears if the FBCA wishes to inhibit policy mapping.
requireExplicitPolicy			Always omitted.
SkipCerts		0	
inhibitPolicyMapping			<u>This may be used in the future</u>

Field	Criticality Flag	Field contents	Comments
SkipCerts		INTEGER	
<b>cRLDistributionPoints</b>	FALSE		
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			Identifies the X.500 entry that will contain the CRL which contains status information for this certificate.
Name			
RDNSSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	printableString (first choice), or bmpString (second choice).
uniformResourceIdentifier		IA5String	
nameRelativeToCRLIssuer			
RelativeDistinguishedName			
AttributeTypeAndValue			

Field	Criticality Flag	Field contents	Comments
AttributeType		OID	
AttributeValue		See comment.	utf8string must be used in all certificates after December 31st, 2003. Prior to that, if possible, use printableString (first choice), or bmpString (second choice)
reasons			
ReasonFlags			Always omitted – FBCA CRLs cover all reason codes.
cRLIssuer			Always omitted – FBCA does not issue indirect CRLs.

### 7.1.1 Version numbers

(see section 7.1)

### 7.1.2 Certificate Extensions

No critical extensions will be included in the certificates other than those listed in section 7.1.

### 7.1.3 Algorithm object identifiers

(see section 7.1)

### 7.1.4 Name forms

(see section 7.1)

### 7.1.5 Name constraints

(see section 7.1)

**7.1.6 Certificate policy object identifier**

(see section 7.1)

**7.1.7 Usage of Policy Constraints extension**

Policy constraints will appear in certificates only when the FBCA directs the OA to inhibit policy mapping. (see section 7.1)

**7.1.8 Policy qualifiers syntax and semantics**

Not used. (see section 7.1)

**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 the RFC 2459.

**7.2 CARL/CRL PROFILE**

The FBCA will issue CARLs and CRLs in accordance with the following profile:

Field	Criticality Flag	Field contents	Comments
CertificateList			
tbsCertList			Fields to be signed.
version		1	Integer Value of "1" for Version 2 CRL.
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field.
algorithm			
		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
parameters		NULL	Always NULL for SHA-1withRSA
issuer			

Field	Criticality Flag	Field contents	Comments
Name			
RDNSequence			C= ; O= ; and OU= are required
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	String types used to encode name MUST match subject field in certificate used to validate the signature on this CRL.
thisUpdate			
Time			
utcTime			
UTCTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime			
GeneralizedTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
nextUpdate			
Time			MUST appear in all CRLs.
utcTime			
UTCTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime			
GeneralizedTime		YYYYMMDDHHMMSSZ	Use for dates after 2049

Field	Criticality Flag	Field contents	Comments
revokedCertificates			
userCertificate			
CertificateSerialNumber		INTEGER	Integer of certificate being revoked
revocationDate			
Time			
utcTime			
UTCTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime			
GeneralizedTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
crlEntryExtensions			
reasonCode	FALSE		If no reason is specified, this extension is omitted. As the fBCA does not issue delta CRLs, the reason cannot be <code>removeFromCRL</code> .
CRLReason			Any CRLReason may be asserted, except <i>unspecified</i> and <i>removeFromCRL</i>
invalidityDate	FALSE		If the certificate is believed to have been compromised before the date of revocation, this extension should be included.
GeneralizedTime		YYYYMMDDHHMMSSZ	Contains the date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid.

Field	Criticality Flag	Field contents	Comments
crlExtensions			
<b>cRLNumber</b>	FALSE	INTEGER	MUST appear in all CRLs. Monotonically increasing sequential number.
<b>authorityKeyIdentifier</b>	FALSE		MUST appear in all CRLs.
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.  (Matches the subjectKeyIdentifier in certificates that can be used to validate this CRL..)

### 7.2.1 Version numbers

(see section 7.2)

### 7.2.2 CARL and CRL entry extensions

The CRL number and authority key identifier extensions will appear in all CRLs.

### 7.2.3

## 8. SPECIFICATION ADMINISTRATION

### 8.1 SPECIFICATION CHANGE PROCEDURES

Errors, updates, or suggested changes to this document will be communicated to the contact in section 1.4. Such communication will include a description of the change, justification for the change, contact information for the person requesting the change, and an impact assessment.

Changes to this document will be reviewed and approved by the FPKIPA, will be communicated to every Agency Principal CA, and will be posted at the website specified in section 2.6.4.

Errors, updates, or suggested changes to this CPS are notified to all Agency PCAs. All versions of this document will be reviewed and approved by the FPKIPA.

Revised versions of this document will be disseminated to interested parties (see section 8.2)

### **8.2 PUBLICATION AND NOTIFICATION POLICIES**

The FPKIPA will publish information (including this CPS) on the following web sites: <http://www.cio.gov/fpkipa>.

This CPS will also be disseminated via email to any that request it.

Proposed changes to the CPS will be sent to Agency PCAs.

The FPKIPA will provide an updated and approved document within 1 week to the PA web administrator, who has agreed to post this information.

### **8.3 CPS APPROVAL PROCEDURES**

The FPKIPA will make the determination that this CPS complies with FBCA CP. The FPKIPA will also determine if a change to this CPS is acceptable and that the changed CPS continues to comply with the FBCA CP.

### **8.4 WAIVERS**

There will be no waivers to the CPS – any changes will be effected through approval of a revised CPS.

## 9. BIBLIOGRAPHY

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

- ABADSG      Digital Signature Guidelines, 1996-08-01.  
<http://www.abanet.org/scitech/ec/isc/dsgfree.html>.
- 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-E      Federal PKI Version 1 Technical Specifications: Part E-X.509 Certificate and CRL Extensions Profile, 7 July 1997
- 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](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 OA	Federal Bridge Certification Authority Operational Authority

FED-STD	Federal Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKI	Federal Public Key Infrastructure
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile
FPKISC	Federal PKI Steering Committee
FPKIPA	Federal PKI Policy Authority
GPEA	Government Paperwork Elimination Act of 1998
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
MOA	Memorandum of Agreement (as used in the context of this CP, between an Agency and the FPKIPA allowing interoperability between the FBCA and Agency PCA)
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	Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.
Agency CA	A CA that acts on behalf of an Agency, and is under the operational control of an Agency.
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.

Attribute Authority	An entity, recognized by the FPKIPA or comparable Agency body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of

this CP in the “Certificate Policies” field of an X.509 v.3 certificate.

Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates that have been revoked.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies it’s Subscriber, (3) contains the Subscriber’s public key, (4) identifies it’s operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to subscribers.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support

provision of the security services required by particular applications.

Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Computer Security Objects	Computer Security Objects Registry operated by the National

Registry (CSOR)	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 Agency 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.
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 Agency 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 (FBCA OA)	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	The FPKIPA is a federal government body responsible for setting,

Infrastructure Policy Authority (FPKI PA)	implementing, and administering policy decisions regarding interagency PKI interoperability that uses the FBCA.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]
Inside threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract

binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]

Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Memorandum of Agreement (MOA)	Agreement between the FPKIPA and an Agency allowing interoperability between the Agency PCA 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 FPKIPA.
Principal CA	The Principal CA is a CA designated by an Agency to interoperate with the FBCA. An Agency may designate multiple Principal CAs to interoperate with the FBCA.
Privacy	Restricting access to subscriber or Relying Party information in accordance with Federal law and agency 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 Agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.

System High	The highest security level supported by an information system. [NS4009]
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Agency 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]