

# **CPWG Mapping Comparison Matrix**

**Federal Bridge Certification Authority (FBCA) CP**

**General Requirements**

**Mapping Matrix for Cross Certification**

Booz | Allen | Hamilton  
900 Elkridge Landing Road  
Linthicum, MD 21090

**TABLE OF CONTENTS**

**1.0 INTRODUCTION.....3**

**2.0 EXECUTIVE SUMMARY.....4**

**3.0 BRIEF ASSESSMENT .....6**

**4.0 DETAILED ASSESSMENT .....9**

**5.0 REFERENCES.....34**

**6.0 CONTACT DETAILS .....34**

## 1.0 INTRODUCTION

The purposes of this certificate policy comparison, in relation to the comparison study conducted with the XXXX Certificate Policy [2] and the FBCA Certificate Policy [3], are:

- 1) To identify at a high-level the most severe areas of inconsistency and/or similarity between the contents of these two Certificate Policy (CP) documents to cross certify,
- 2) To identify at a high-level the areas of consistency and/or similarity between the contents of these two Certificate Policy (CP) documents to cross certify, and
- 3) To recommend appropriate changes, if required, to the XXXX CP [2] that would make it more consistent with the FBCA CP [3];
- 4) This mapping comparison is all the necessary requirements needed for all assurance levels to complete a cross certification. This comparison documents works in tandem with one of the four delta mapping matrices located at <http://www.cio.gov/fpkipa> . When submitted an application for cross-certification, the applicant must use this General Requirements Matrix and one of the four assurance Matrices to identify the level of assurance for the cross certificate.

This document is organized to achieve these purposes in the following sections:

- 1) **EXECUTIVE SUMMARY**, provides a high-level overview of the PKIs represented by the Certificate Policies being compared in this analysis as well as an overview of the findings of this mapping comparison,
- 2) **BRIEF ASSESSMENT**, provides a brief indication of the degree of similarity of each XXXX CP section as compared to the FBCA CP by indicating the evaluation term used in each main subsection of the CP; and
- 3) **DETAILED ASSESSMENT**, presents a detailed breakdown of the requirements in the FBCA CP, Section by Section, and categorizes the degree of similarity of the XXXX CP requirements to the FBCA CP. Comments to explain the rationale for the degree of similarity are also provided. The topical and organizational framework used as a basis for this comparison is Request for Comments (RFC) 2527, the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [1].

## 2.0 EXECUTIVE SUMMARY

The Federal Bridge Certification Authority (FBCA) is the unifying element to link autonomous Certification Authorities (CA's) into a logically connected Public Key Infrastructure (PKI). The FBCA functions as a hierarchical hub allowing relying parties to create certificate trust paths from their PKI domains back to the PKI domain of the Certification Authority that issued the presented certificate, so that the level of assurance honored by disparate PKI's can be reconciled.

The General Services Administration (GSA), under the auspices of the Federal Public Key Infrastructure Policy Authority (FPKIPA) and the Federal PKI Steering Committee (FPKISC) operates the FBCA. In order to promote interoperability and the appropriate use of certificate policies, the FBCA has issued a minimum set of operational requirements that support trust path creation and verification of digital certificates. The FBCA will issue cross-certificates to other autonomous Principal CA's, and then only when authorized by the FPKIPA. Initially, autonomous CA's that operate in trust domains that meet the assurance and security requirements established by the FPKIPA will be eligible to cross-certify with the FBCA.

The FBCA is designed to provide a mechanism for entities employing entity-specific PKI's to interoperate efficiently. The FBCA allows entities to create and process trust paths between specific PKI's, to enable digital certificates issued by one CA to be honored with an appropriate level of trust [or assurance] by a different CA.

The FBCA acts as a hierarchical "hub." A Principal CA receives permission to interoperate with the FBCA under terms and conditions described in the FBCA Application for cross certification. This system allows every CA that cross certifies with the FBCA the possibility of interoperating with all participating agencies using FBCA-issued cross certificate pairs, in an environment of trust and reliability. This is facilitated through the use of a certificate policy mapping, which is how certificates issued by different CA's meet one another's standards for identity proofing, integrity of data and system operations, non-repudiation, and encryption of data. Policy mappings between an autonomous Principal CA and the FBCA are proposed by the entity and approved by the FPKIPA, and then placed in the certificate issued by the FBCA to the autonomous Principal CA's.

When the Applicant is determining whether to rely on a certificate issued by another party, it is not required to use the certificate policy mapping expressed in the FBCA certificates. The Applicant, at its sole discretion, may choose to use a separate policy mapping for certain transactions or for all transactions.

The XXXX operates a PKI to provide security for its electronic information. The XXXX PKI consists of products and services that provide and manage X.509v3 certificates for digital signatures and encryption. An XXXX digital certificate identifies the individual named in the certificate requestor/holder, and binds that person to a unique X.509v3 compliant key pair.

Programs that carry out or support XXXX missions may require the type of security services provided by a PKI such as authentication, confidentiality, encryption, non-repudiation, and access control. These services are met with an array of network security components such as web servers, guards, firewalls, routers, and trusted database servers. The operation of these components is supported and complemented

by use of public-key cryptography. As a system solution, the components share the burden of the total system security. The use of public key certificates does not add any security services to a poorly designed or implemented system. The reliability of the public-key cryptography portion of the security solution is a direct result of the secure and trustworthy operation of an established PKI, including equipment, facilities, personnel, and procedures.

The XXXX Certificate Policy (CP) follows and complies with the Internet Engineering Task Force (IETF) Request for Comment (RFC) 2527, X.509 PKI CP and Certification Practices Framework. The XXXX CP defines the primary obligations and operational responsibilities of all XXXX PKI program participants, and defines the creation, management and use of X.509 Version 3 digital certificates. The XXXX CP defines the applicability of assurance levels for the protection of information based on its value or sensitivity, the risk and the consequences of loss, disclosure or modification.

This CP mapping comparison identifies all major and minor differences between the FBCA CP and the XXXX certificate policies, based on a set of predetermined evaluation parameters, defined in the [BRIEF ASSESSMENT](#). The results of this comparison identify the sections that require modification to facilitate policy compatibility and interoperability of the underlying technology and operations.

### 3.0 BRIEF ASSESSMENT

This section of the report contains a table representing the high level mapping comparisons between the FBCA CP [3] and the XXXX CP [2]. The table presents a concise indication of the degree of conformity between the XXXX CP [2] and the FBCA CP [3].

The “Brief Assessment” table provides for a quick review of the finding to facilitate the quick identification of the CP sections that the XXXX CP was evaluated against and the “Overall Match” status as compared to the FBCA CP requirement. The XXXX section column is populated with the section number that covers the mapping requirement.

The Brief Assessment table contains four main columns described as follows:

- 1) **FBCA CP Section** – identifies the section numbers for each of the CPs
- 2) **XXXX Section Topics** – identifies the CP framework section titles corresponding to the section numbers. If there is not a corresponding section in one of the CPs, it is indicated with “N/A” for Not Applicable.
- 3) **Section Topic** - Title Category
- 4) **Evaluation Summary** – displays the corresponding evaluation result, which indicates the *lowest* degree of conformity contained within each section.

The following seven evaluation terms and their definitions, listed in order of degree of conformity, were used to assess the XXXX CP alignment to the FBCA CP elements:

- 1) **Exceeds** - The XXXX CP policy provides a higher level of assurance/security than the FBCA CP requirement
- 2) **Equivalent** - The XXXX CP policy provides exactly the same assurance/security as the FBCA CP requirement.
- 3) **Comparable** - The XXXX CP contains dissimilar policy contents, but provides a comparable level of assurance to meet the security to the FBCA CP requirement.
- 4) **Partial** - The XXXX CP contains policy that is comparable, but it does not address the entire FBCA CP requirement.
- 5) **Not Comparable** - The XXXX CP contains dissimilar policy contents, which provides a lower level of assurance/security than the FBCA CP requirement.
- 6) **Missing** - The XXXX CP does not contain policy contents that can be compared to the FBCA CP requirement in any way.
- 7) **N/A** – Not Applicable to XXXX CP or required for FBCA cross certification.

Table #	FBCA Section	XXXX Section	Section Topic	Evaluation Summary
<b>1.0</b>		<b>INTRODUCTION</b>		
1	1.4.2		Contact Person	
2	1.4.3		Person determining Certification Practice Statement suitability for the policy	
<b>2.0</b>		<b>GENERAL PROVISIONS</b>		
3	2.4.1		Severability of Provisions, Survival, Merger, and Notice	
4	2.7		Compliance Audit	
5	2.7.1		Frequency of Entity Compliance Audit	
6,7	2.7.2		Identity/Qualifications of Compliance Auditor	
8	2.7.3		Compliance Auditor's Relationship to Audited Party	
9	2.7.5		Actions Taken as a Result of Deficiency	
<b>3.0</b>		<b>IDENTIFICATION AND AUTHENTICATION</b>		
10,11	3.1.1		Types of Names	
12	3.1.2		Need for Names to be Meaningful	
13,14	3.1.3		Rules for Interpreting Various Name Forms	
15,16	3.1.4		Uniqueness of Names	
17 - 21	3.1.7		Method to Prove Possession of Private Key	
22,23	3.1.8		Authentication of Organizational Identity	
24,25	3.1.9		Authentication of Individual Identity	
26,27	3.1.10		Authentication of Component Identities	
28	3.2.1		Certificate Re-Key	
29	3.2.2		Certificate Renewal	
30 - 32	3.2.3		Certificate Update	
33	3.3		Obtaining a New Certificate After Revocation	
34,35	3.4		Revocation Request	
<b>4.0</b>		<b>OPERATIONAL REQUIREMENTS</b>		
36,37	4.1.1		Delivery of Public Key for Certificate Issuance	
38,39	4.2		Certificate Issuance	
40-45	4.2.1		Delivery of Subscriber's Private Key to Subscriber	
46	4.4.1		Circumstances for revocation of a certificate issued by the FBCA or Entity CA	
47	4.4.1.1		Who can request revocation...	
48 - 52	4.4.1.2		Procedure for Revocation Request	
53	4.4.3		Certification Authority Revocation Lists / CRL's	
54	4.4.3.1		CARL/CRL Issuance Frequency	
55,56	4.5		Security Audit Procedure	
57,58	4.5.1		Types of Events Recorded	
59	4.5		Security Audit Procedure	
60,61	4.5.2		Frequency of processing data	
62,63	4.5.3		Retention Period for Security Audit Data	
64-66	4.5.4		Protection of Security Audit Data	
67,68	4.5.5		Security Audit Data Backup Procedures	
69,70	4.5.6		Security Audit Collection System (Internal vs. External)	
71	4.5.8		Vulnerability Assessments	
72	4.6.1		Types of Events Archived	
73	4.6.2		Retention Period for Archive	
74-77	4.6.3		Protection of Archive	
78	4.8.1		Computing Resources, Software, and/or Data are Corrupted	
78	4.8.2		CA Signature Keys are Revoked	
79	4.8.3		CA Signature Keys are Compromised	
80	4.9		CA Termination	
<b>5.0</b>		<b>PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS</b>		
81,82	5.1		Physical Controls for the CA or Entity CA	
83,84	5.1.1		Site Location and Construction	

Table #	FBCA Section	XXXX Section	Section Topic	Evaluation Summary
85-93	5.1.2		Physical Access	
94,95	5.1.6		Media Storage	
96-99	5.1.8		Off-site Backup	
100,101	5.3.1		Background, Qualifications, Experience, and Security Clearance Requirements	
102	5.3.2		Background Check Procedures	
103	5.3.3		Training Requirements	
104	5.3.4		Retraining Frequency and Requirements	
105	5.3.6		Sanctions for Unauthorized Actions	
106	5.3.7		Contracting Personnel Requirements	
107,108	5.3.8		Documentation Supplied to Personnel	
<b>6.0</b>			<b>TECHNICAL SECURITY CONTROLS</b>	
109	6.1.2		Private Key Delivery to Subscriber	
110 - 112	6.1.5		Key Sizes	
113	6.1.6		Public Key Parameters Generation	
114	6.1.7		Parameter Quality Checking	
115	6.2.3		Key Escrow of CA Private Signature Key	
116,117	6.2.4.1		Backup of CA Private Signature Key	
118	6.2.5		Private Key Archival	
119	6.2.6		Private Key Entry into Cryptographic Module	
120,121	6.2.7		Method of Activating Private Keys	
122-124	6.2.8		Methods of Deactivating Private Keys	
125	6.2.9		Method of Destroying Subscriber Private Signature Keys	
126,127	6.4.1		Activation Data Generation and Installation	
128 - 130	6.4.2		Activation Data Protection	
131,132	6.5.1		Specific Computer Security Technical Requirements	
133 - 139	6.6.1		System Development Controls	
140 - 143	6.6.2		Security Management Controls	
144 - 147	6.7		Network Security Controls	
<b>7.0</b>			<b>CERTIFICATE AND CRL PROFILES</b>	
148	7.1.1		Version Numbers	
149,150	7.1.2		Certificate Extensions	
151,152	7.1.3		Algorithm Object Identifiers	
153	7.1.4		Name Forms	
154	7.1.6		Certificate Policy Object Identifier	
155	7.2.1		Version Numbers	
156	7.2.2		CARL/CRL Entry Extensions	

## 4.0 DETAILED ASSESSMENT

This section of the report presents the mapping comparison results for the FBCA CP and the XXXX CP. The mapping comparison is characterized using the evaluation terms listed in the BRIEF ASSESSMENT.

The detailed mapping results show the FBCA CP sections and requirements that are to be mapped, the XXXX CP section and appropriate applicable policy text, the evaluation result for each requirement element addressed by the XXXX CP, as well as the evaluation comments. By default, the evaluation results listed in the “Overall Match” field indicates the rating for each table requirement.

Table No.	CP Section	Mapping Phrase
1	FBCA <b>1.4.2</b>	Questions regarding this CP shall be directed to the Chair of the Federal PKI Policy Authority, ...
	XXXX:	
	Overall Match:	Comments:
2	FBCA <b>1.4.3</b>	Entities are responsible for determining whether their CA CPSs conform to their CA CPs, and in particular, properly adhere to any policy mappings approved by the Federal PKI Policy Authority between the FBCA CP and the Entity Principal CA CP.
	XXXX:	
	Overall Match:	Comments:
3	FBCA <b>2.4.1</b>	Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated.
	XXXX:	
	Overall Match:	Comments:
4	FBCA <b>2.7</b>	Entity CAs must have a compliance audit mechanism in place to ensure that the requirements of their CP/CPS are being implemented and enforced.
	XXXX:	
	Overall Match:	Comments:
5	FBCA <b>2.7.1</b>	The FBCA and Entity Principal CAs have the right to require periodic and aperiodic compliance audits or inspections of subordinate CA or RA operations to validate that the subordinate entities are operating in accordance with the security practices and procedures described in their respective CPS.
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
6	FBCA 2.7.2	The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with requirements which the Federal PKI Policy Authority imposes on the issuance and management of FBCA certificates, and which Entities impose on the issuance and management of their certificates.
	XXXX:	
	Overall Match:	Comments:
7	FBCA 2.7.2	The compliance auditor must perform such compliance audits as a primary responsibility.
	XXXX:	
	Overall Match:	Comments:
8	FBCA 2.7.3	For both the FBCA and Entity CAs, the compliance auditor either shall be a private firm which is independent from the entity being audited, or it shall be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation.
	XXXX:	
	Overall Match:	Comments:
9	FBCA 2.7.5	When the compliance auditor finds a discrepancy between how the FBCA or Entity CA is designed or is being operated or maintained, and the requirements of this CP, the Entity CP, the MOA, or the applicable CPS, the following actions shall be performed: <ul style="list-style-type: none"> <li>- The compliance auditor shall note the discrepancy;</li> <li>- The compliance auditor shall notify the Entity of the discrepancy. The Entity shall notify the Federal PKI Policy Authority promptly;</li> <li>- The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this CP and the MOA, and then proceed to make such notifications and take such actions without delay.</li> </ul>
	XXXX:	
	Overall Match:	Comments:
10	FBCA 3.1.1	Where DNs are required, subscribers shall have them assigned through their organizations, in accordance with a naming authority.
	XXXX:	
	Overall Match:	Comments:
11	FBCA 3.1.1	X.500 Distinguished Name, and optional Alternative Subject Name if marked non-critical
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
12	FBCA <b>3.1.2</b>	Names used in the certificates must identify the person or object to which they are assigned in a meaningful way.
	XXXX:	
	Overall Match:	Comments:
13	FBCA <b>3.1.3</b>	Rules for interpreting name forms shall be contained in the applicable certificate profile and are established by the Federal PKI Policy Authority.
	XXXX:	
	Overall Match:	Comments:
14	FBCA <b>3.1.3</b>	The authority responsible for Entity CA name space control shall be identified in the respective CP.
	XXXX:	
	Overall Match:	Comments:
15	FBCA <b>3.1.4</b>	The FBCA, Entity CAs and RAs shall enforce name uniqueness within the X.509 name space which they have been authorized.
	XXXX:	
	Overall Match:	Comments:
16	FBCA <b>3.1.4</b>	When name forms other than a DN (e.g., an electronic mail address or DNS name) are used, they too must be allocated such that name uniqueness across the FPKI is ensured.
	XXXX:	
	Overall Match:	Comments:
17	FBCA <b>3.1.7</b>	In all cases where the party named in a certificate generates its own keys, that party shall be required to prove possession of the private key which corresponds to the public key in the certificate request.
	XXXX:	
	Overall Match:	Comments:
18	FBCA <b>3.1.7 (H/W)</b>	If the party is not in possession of the token when the key is generated, then the token (e.g., a smartcard or a PKCS #12 encoded message) shall be delivered to the subject via an accountable method (see Section 6.1.2).
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
19	FBCA 3.1.7 (H/W) (RBMH)	For all assurance levels, when keyed hardware tokens are delivered to certificate subjects, the delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subjects.
	XXXX:	
	Overall Match:	Comments:
20	FBCA 3.1.7 (H/W)	The FBCA (or Entity) must maintain a record of validation for receipt of the token by the subject.
	XXXX:	
	Overall Match:	Comments:
21	FBCA 3.1.7	When any mechanism that includes a shared secret (e.g., a password or PIN) is used, the mechanism shall ensure that the applicant and the FBCA (or Entity CA) are the only recipients of this shared secret.
	XXXX:	
	Overall Match:	Comments:
22	FBCA 3.1.8	Requests for FBCA or Entity CA certificates in the name of an organization shall include the organization name, address, and documentation of the existence of the organization.
	XXXX:	
	Overall Match:	Comments:
23	FBCA 3.1.8	The FBCA Operational Authority or Entity RA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
24	FBCA <b>3.1.9</b>	<p>Process information shall depend upon the certificate level of assurance and shall be addressed in the FBCA or Entity CPS. The process documentation and authentication requirements shall include the following depending upon the level of assurance (as set forth below):</p> <ul style="list-style-type: none"> <li>- The identity of the person performing the identification;</li> <li>- A signed declaration by that person that he or she verified the identity of the Subscriber as required by the applicable certificate policy which may be met by establishing how the applicant is known to the verifier as required by this certificate policy;</li> <li>- A unique identifying number from the ID of the verifier and, if in-person identity proofing is done, from the ID of the applicant;</li> <li>- The date and time of the verification; and</li> <li>- A declaration of identity signed by the applicant using a handwritten signature. If in person identity proofing is done, this shall be performed in the presence of the person performing the identity authentication.</li> </ul>
	XXXX:	
	Overall Match:	Comments:
25	FBCA <b>3.1.9 (RBMH)</b>	<p>If an Applicant is unable to perform face-to-face registration alone (e.g., a network device), the applicant shall be represented by a trusted person already issued a digital certificate by the Entity. The trusted person will present information sufficient for registration at the level of the certificate being requested, for both himself/herself and the applicant who the trusted person is representing.</p>
	XXXX:	
	Overall Match:	Comments:
26	FBCA <b>3.1.10</b>	<p>Some computing and communications components (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases, the component must have a human sponsor. The PKI sponsor is responsible for providing the following registration information:</p> <ul style="list-style-type: none"> <li>- Equipment identification (e.g., serial number) or service name (e.g., DNS name)</li> <li>- Equipment public keys</li> <li>- Equipment authorizations and attributes (if any are to be included in the certificate)</li> <li>- Contact information to enable the CA or RA to communicate with the sponsor when required</li> </ul>
	XXXX:	
	Overall Match:	Comments:
27	FBCA <b>3.1.10</b>	<p>The registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested.</p>
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
28	FBCA 3.2.1	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
	XXXX:	
	Overall Match:	Comments:
29	FBCA 3.2.2	A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged.
	XXXX:	
	Overall Match:	Comments:
30	FBCA 3.2.3	The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.
	XXXX:	
	Overall Match:	Comments:
31	FBCA 3.2.3	Further, if an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or other designated agent (as set forth above) in order for an updated certificate having the new name to be issued.
	XXXX:	
	Overall Match:	Comments:
32	FBCA 3.2.3	Finally, when a CA updates its private signature key and thus generates a new public key, the CA shall notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed. For self-signed ("root") certificates, such certificates shall be conveyed to users in a secure fashion to preclude malicious substitution attacks.
	XXXX:	
	Overall Match:	Comments:
33	FBCA 3.3	After a certificate has been revoked other than during a renewal or update action, the subscriber is required to go through the initial registration process described in Section 3.1 to obtain a new certificate. This applies to Entity CAs.
	XXXX:	
	Overall Match:	Comments:
34	FBCA 3.4	Revocation requests must be authenticated.
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
35	FBCA 3.4	Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.
	XXXX:	
	Overall Match:	Comments:
36	FBCA 4.1.1	In those cases where public/private key pairs are generated by the FBCA or Entity CA on behalf of the Subscriber, the FBCA or Entity CA (respectively) shall implement secure mechanisms to ensure that the token on which the public/private key pair is held is securely sent to the proper Subscriber.
	XXXX:	
	Overall Match:	Comments:
37	FBCA 4.1.1 (H/W)	The FBCA or Entity CA (respectively) shall also implement procedures to ensure that the token is not activated by an unauthorized entity.
	XXXX:	
	Overall Match:	Comments:
38	FBCA 4.2	While the Subscriber may do most of the data entry, it is still the responsibility of the RA to verify that the information is correct and accurate.
	XXXX:	
	Overall Match:	Comments:
39	FBCA 4.2	If databases are used to confirm Subscriber information, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance of the certificate being sought.
	XXXX:	
	Overall Match:	Comments:
40	FBCA 4.2.1	If the key is generated elsewhere, then the module must be delivered to the Subscriber. Accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it.
	XXXX:	
	Overall Match:	Comments:
41	FBCA 4.2.1 (H/W)	The Subscriber shall acknowledge receipt of the module.
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
42	FBCA 4.2.1	Under no circumstances shall anyone other than the Subscriber have substantive knowledge of or control over private signing keys after generation of the key.
	XXXX:	
	Overall Match:	Comments:
43	FBCA 4.2.1	Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private key to the Subscriber.
	XXXX:	
	Overall Match:	Comments:
44	FBCA 4.2.1 (H/W)	Hardware tokens containing FBCA or Entity CA private signature keys may be backed-up in accordance with security audit requirements defined Section 4.5.1.
	XXXX:	
	Overall Match:	Comments:
45	FBCA 4.2.1	For cases where there are several entities acting in one capacity, and where non-repudiation for transactions is not desired, a certificate may be issued that corresponds to a private key that is shared by multiple Subscribers. In these cases:
	XXXX:	<ul style="list-style-type: none"> <li>- An Information Systems Security Office or equivalent shall be responsible for ensuring control of the private key, including maintaining a list of Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time.</li> <li>- The list of those holding the shared private key must be provided to, and retained by, the applicable CA or its designated representative; and</li> <li>- The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations).</li> </ul>
	Overall Match:	Comments:
46	FBCA 4.4.1	Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.
	XXXX:	
	Overall Match:	Comments:
47	FBCA 4.4.1.1	The process for requesting revocation of a Subscriber certificate issued by an Entity CA shall be set forth in the Entity CP or CPS.
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
48	FBCA 4.4.1.2	A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed).
	XXXX:	
	Overall Match:	Comments:
49	FBCA 4.4.1.2	In particular, if the revocation is being requested for reason of key compromise or suspected fraudulent use, then the Subscriber's or the RA's revocation request must so indicate. If a RA performs this on behalf of a Subscriber, a formal, signed message format known to the CA shall be employed.
	XXXX:	
	Overall Match:	Comments:
50	FBCA 4.4.1.2	All requests shall be authenticated; for signed requests from the certificate subject, or from an RA, verification of the signature is sufficient.
	XXXX:	
	Overall Match:	Comments:
51	FBCA 4.4.1.2	If the revocation request appears to be valid, the Federal PKI Policy Authority shall direct the FBCA Operational Authority to revoke the certificate by placing its serial number and other identifying information on a CARL/CRL and then post the CARL/CRL in the FBCA repository, in addition to any other revocation mechanisms used.
	XXXX:	
	Overall Match:	Comments:
52	FBCA 4.4.1.2 (H/W)	If a Subscriber leaves an organization and the hardware tokens cannot be obtained from the Subscriber, then all Subscriber's certificates associated with the unretrieved tokens shall be immediately revoked. The token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction.
	XXXX:	
	Overall Match:	Comments:
53	FBCA 4.4.3	All Entity CAs shall issue Certification Authority Revocation Lists (CARLs) and Certificate Revocation Lists (CRL).
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
54	FBCA 4.4.3.1	CARLs and CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information.
	XXXX:	
	Overall Match:	Comments:
55	FBCA 4.5	Audit log files shall be generated for all events relating to the security of the FBCA or Entity CAs.
	XXXX:	
	Overall Match:	Comments:
56	FBCA 4.5	Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used.
	XXXX:	
	Overall Match:	Comments:
57	FBCA 4.5.1	All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with <i>Retention period for archive</i> , Section 4.6.2.
	XXXX:	
	Overall Match:	Comments:
58	FBCA 4.5.1	All security auditing capabilities of the FBCA or Entity CA operating system and PKI CA applications required by this CP shall be enabled.
	XXXX:	
	Overall Match:	Comments:
59	FBCA 4.5	At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event): <ul style="list-style-type: none"> <li>- The type of event</li> <li>- The date and time the event occurred</li> <li>- A success or failure indicator when executing the FBCA or Entity CA's signing process</li> <li>- A success or failure indicator when performing certificate revocation</li> <li>- The identity of the entity and/or operator (of the FBCA or Entity CA) that caused the event.</li> <li>- A message from any source requesting an action by the FBCA or Entity CA is an auditable event. The message must include message date and time, source, destination and contents.</li> </ul>
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
60	FBCA 4.5.2	Audit logs shall be reviewed in accordance to the table below. The FBCA OA shall explain all significant events in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs.
	XXXX:	
	Overall Match:	Comments:
61	FBCA 4.5.2	Actions taken as a result of these reviews shall be documented.
	XXXX:	
	Overall Match:	Comments:
62	FBCA 4.5.3	Audit logs shall be retained onsite for at least two months...
	XXXX:	
	Overall Match:	Comments:
63	FBCA 4.5.3	The individual who removes audit logs from the FBCA or Entity CA system shall be an official different from the individuals who, in combination, command the FBCA or an Entity CA signature key.
	XXXX:	
	Overall Match:	Comments:
64	FBCA 4.5.4	FBCA (or Entity CA) system configuration and procedures must be implemented together to ensure that: - only authorized people have read access to the logs; - only authorized people may archive audit logs; and, - audit logs are not modified.
	XXXX:	
	Overall Match:	Comments:
65	FBCA 4.5.4	The entity performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion requires modification access).
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
66	FBCA 4.5.4	Audit logs shall be moved to a safe, secure storage location separate from the FBCA equipment. Practice Note: If a system over-writes audit logs after a given time, the audit log is not considered deleted or destroyed if the audit log has been backed up and archived.
	XXXX:	
	Overall Match:	Comments:
67	FBCA 4.5.5	Audit logs and audit summaries shall be backed up at least monthly.
	XXXX:	
	Overall Match:	Comments:
68	FBCA 4.5.5	A copy of the audit log shall be sent off-site in accordance with the CPS on a monthly basis.
	XXXX:	
	Overall Match:	Comments:
69	FBCA 4.5.6	Audit processes shall be invoked at system startup, and cease only at system shutdown.
	XXXX:	
	Overall Match:	Comments:
70	FBCA 4.5.6	Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the FBCA Operational Authority Administrator (or comparable Entity authority) shall determine whether to suspend FBCA operation (or Entity CA operation respectively) until the problem is remedied.
	XXXX:	
	Overall Match:	Comments:
71	FBCA 4.5.8	The Operational Authority will perform routine self assessments of security controls.
	XXXX:	
	Overall Match:	Comments:
72	FBCA 4.6.1	FBCA or Entity CA archive records shall be sufficiently detailed to establish the proper operation of the FBCA or Entity CA, or the validity of any certificate (including those revoked or expired) issued by the FBCA or Entity CA.
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
73	FBCA <b>4.6.2</b>	Executive branch Entities must follow either the General Records Schedule established by the National Archives and Records Administration or an Entity-specific schedule as applicable. All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities.
	XXXX:	
	Overall Match:	Comments:
74	FBCA <b>4.6.3</b>	No unauthorized user shall be permitted to write to, modify, or delete the archive.
	XXXX:	
	Overall Match:	Comments:
75	FBCA <b>4.6.3</b>	The contents of the archive shall not be released except as determined by the Federal PKI Policy Authority for the FBCA (or Entity for the Entity CA) or as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents.
	XXXX:	
	Overall Match:	Comments:
76	FBCA <b>4.6.3</b>	Archive media shall be stored in a safe, secure storage facility separate from the FBCA or Entity CA itself.
	XXXX:	
	Overall Match:	Comments:
77	FBCA <b>4.8.1</b>	If FBCA or Entity CA equipment is damaged or rendered inoperative, but the FBCA or Entity CA signature keys are not destroyed, FBCA or Entity CA operation shall be reestablished as quickly as possible, giving priority to the ability to generate certificate status information.
	XXXX:	
	Overall Match:	Comments:
78	FBCA <b>4.8.2</b>	The FBCA or Entity Principal CA shall reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS.
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
79	FBCA 4.8.3	If the FBCA or Entity CA signature keys are compromised or lost (such that compromise is possible even though not certain): <ul style="list-style-type: none"> <li>- The Federal PKI Policy Authority and all of its member entities shall be securely notified at the earliest feasible time (so that entities may issue CARLs revoking any cross-certificates issued to the FBCA);</li> <li>- A new FBCA or Entity CA key pair shall be generated by the FBCA or Entity CA in accordance with procedures set forth in the FBCA or Entity CPS; and</li> <li>- New FBCA or Entity CA certificates shall be issued to Entities also in accordance with the FBCA or Entity CPS.</li> </ul>
	XXXX:	
	Overall Match:	Comments:
80	FBCA 4.9	In the event that an Entity CA terminates operation, the Entity shall provide notice to the FBCA prior to termination.
	XXXX:	
	Overall Match:	Comments:
81	FBCA 5.1	RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated.
	XXXX:	
	Overall Match:	Comments:
82	FBCA 5.1	The RA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.
	XXXX:	
	Overall Match:	Comments:
83	FBCA 5.1.1	The location and construction of the facility housing the FBCA and Entity CA equipment shall be consistent with facilities used to house high value, sensitive information.
	XXXX:	
	Overall Match:	Comments:
84	FBCA 5.1.1	The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors shall provide robust protection against unauthorized access to the FBCA and Entity CA equipment and records.
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
85	FBCA 5.1.2	The FBCA and Entity CA equipment shall always be protected from unauthorized access, and especially while the cryptographic module is installed and activated.
	XXXX:	
	Overall Match:	Comments:
86	FBCA 5.1.2	Physical access controls shall be implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the equipment environment.
	XXXX:	
	Overall Match:	Comments:
87	FBCA 5.1.2	Removable cryptographic modules shall be inactivated prior to storage.
	XXXX:	
	Overall Match:	Comments:
88	FBCA 5.1.2	When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, FBCA and Entity CA equipment shall be placed in secure containers.
	XXXX:	
	Overall Match:	Comments:
89	FBCA 5.1.2	Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.
	XXXX:	
	Overall Match:	Comments:
90	FBCA 5.1.2 (BMH)	A security check of the facility housing the FBCA or Entity CA equipment (operating at the Basic Assurance level or higher) shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following: <ul style="list-style-type: none"> <li>- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open”, and secured when “closed”; and for the FBCA, that all equipment other than the repository is shut down);</li> <li>- Any security containers are properly secured;</li> <li>- Physical security systems (e.g., door locks, vent covers) are functioning properly; and</li> <li>- The area is secured against unauthorized access.</li> </ul>
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
91	FBCA <b>5.1.2</b>	A person or group of persons shall be made explicitly responsible for making such checks.
	XXXX:	
	Overall Match:	Comments:
92	FBCA <b>5.1.2</b>	When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained.
	XXXX:	
	Overall Match:	Comments:
93	FBCA <b>5.1.2</b>	If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.
	XXXX:	
	Overall Match:	Comments:
94	FBCA <b>5.1.6</b>	FBCA and Entity CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic).
	XXXX:	
	Overall Match:	Comments:
95	FBCA <b>5.1.6</b>	Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the FBCA and Entity CAs.
	XXXX:	
	Overall Match:	Comments:
96	FBCA <b>5.1.8</b>	For the FBCA and Entity CAs (operating at the Basic Assurance level or higher), full system backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in the respective CPS.
	XXXX:	
	Overall Match:	Comments:
97	FBCA <b>5.1.8</b>	Backups are to be performed and stored off-site not less than once per week.
	XXXX:	
	Overall Match:	Comments:
98	FBCA <b>5.1.8</b>	At least one full backup copy shall be stored at an offsite location (separate from the FBCA and Entity CA equipment).
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
99	FBCA <b>5.1.8</b>	The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational FBCA and Entity CA.
	XXXX:	
	Overall Match:	Comments:
100	FBCA <b>5.3.1</b>	Each Entity shall identify at least one individual or group responsible and accountable for the operation of each CA in that Entity.
	XXXX:	
	Overall Match:	Comments:
101	FBCA <b>5.3.1</b>	All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and must be U.S. citizens.
	XXXX:	
	Overall Match:	Comments:
102	FBCA <b>5.3.2</b>	Entity background check procedures shall be described in the CPS and shall demonstrate that Entity requirements set forth in Section 5.3.1 are met.
	XXXX:	
	Overall Match:	Comments:
103	FBCA <b>5.3.3</b>	All personnel performing duties with respect to the operation of the FBCA or Entity CA shall receive comprehensive training. Training shall be conducted in the following areas: <ul style="list-style-type: none"> <li>- CA/RA security principles and mechanisms</li> <li>- All PKI software versions in use on the CA system</li> <li>- All PKI duties they are expected to perform</li> <li>- Disaster recovery and business continuity procedures.</li> </ul>
	XXXX:	
	Overall Match:	Comments:
104	FBCA <b>5.3.4</b>	Individuals responsible for PKI roles shall be aware of changes in the FBCA and Entity CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented.
	XXXX:	
	Overall Match:	Comments:
105	FBCA <b>5.3.6</b>	The Federal PKI Policy Authority or Entity CA Policy Authority shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the FBCA or its repository not authorized in this CP, the FBCA CPS, or other procedures published by the FBCA Operational Authority.
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
106	FBCA <b>5.3.7</b>	Contractor personnel employed to perform functions pertaining to the FBCA or an Entity CA shall meet applicable requirements set forth in the FBCA CP or Entity CP as determined by the FBCA Operational Authority or the corresponding Entity.
	XXXX:	
	Overall Match:	Comments:
107	FBCA <b>5.3.8</b>	The FBCA and Entity CA shall make available to its CA and RA personnel the certificate policies it supports, relevant parts of the CPS, and any relevant statutes, policies or contracts.
	XXXX:	
	Overall Match:	Comments:
108	FBCA <b>5.3.8</b>	Documentation shall be maintained identifying all personnel who received training and the level of training completed.
	XXXX:	
	Overall Match:	Comments:
109	FBCA <b>6.1.2</b> <b>(ENCRYPTION)</b>	For encryption keys, delivery of the private key to the Subscriber (or, if the Subscriber generates the encryption key pair, delivery by the Subscriber to the Entity) shall be in accordance with the requirements of this CP and the applicable Entity CP/CPS.
	XXXX:	
	Overall Match:	Comments:
110	FBCA <b>6.1.5</b>	All FIPS-approved signature algorithms shall be considered acceptable.
	XXXX:	
	Overall Match:	Comments:
111	FBCA <b>6.1.5</b>	Certificates issued by Entity CAs shall use at least 1024 bit RSA or DSA, with SHA-1 (or better), in accordance with FIPS 186.
	XXXX:	
	Overall Match:	Comments:
112	FBCA <b>6.1.5</b>	Use by the FBCA or an Entity of SSL or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys.
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
113	FBCA <b>6.1.6</b>	Public key parameters prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186.
	XXXX:	
	Overall Match:	Comments:
114	FBCA <b>6.1.7</b>	Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186 or a more stringent test if specified by the Federal PKI Policy Authority.
	XXXX:	
	Overall Match:	Comments:
115	FBCA <b>6.2.3</b>	Under no circumstances shall the FBCA or an Entity CA signature keys used to support non-repudiation services be escrowed by a third party.
	XXXX:	
	Overall Match:	Comments:
116	FBCA <b>6.2.4.1</b>	If backed up, the FBCA and Entity CA private signature keys shall be backed up under the same multi-person control as the original signature key.
	XXXX:	
	Overall Match:	Comments:
117	FBCA <b>6.2.4.1</b>	A single copy of the signature key may be stored at the FBCA or CA location, respectively.
	XXXX:	
	Overall Match:	Comments:
118	FBCA <b>6.2.5</b>	Private signature keys shall not be escrowed or archived.
	XXXX:	
	Overall Match:	Comments:
119	FBCA <b>6.2.6</b>	FBCA and Entity CA private keys shall be generated by and remain in a cryptographic module.
	XXXX:	
	Overall Match:	Comments:
120	FBCA <b>6.2.7</b>	The subscriber must be authenticated to the cryptographic module before the activation of any private key(s).
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
121	FBCA <b>6.2.7</b>	Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).
	XXXX:	
	Overall Match:	Comments:
122	FBCA <b>6.2.8</b>	If cryptographic modules are used to store subscriber private keys, then the cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access.
	XXXX:	
	Overall Match:	Comments:
123	FBCA <b>6.2.8</b>	After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS.
	XXXX:	
	Overall Match:	Comments:
124	FBCA <b>6.2.8</b>	Hardware cryptographic modules shall be removed and stored in a secure container when not in use.
	XXXX:	
	Overall Match:	Comments:
125	FBCA <b>6.2.9</b>	Subscriber private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked.
	XXXX:	
	Overall Match:	Comments:
126	FBCA <b>6.4.1</b>	Where passwords are used as activation data, the password data shall be generated in conformance with FIPS-112.
	XXXX:	
	Overall Match:	Comments:
127	FBCA <b>6.4.1</b>	If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
128	FBCA <b>6.4.2</b>	Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms.
	XXXX:	
	Overall Match:	Comments:
129	FBCA <b>6.4.2</b>	Activation data should either be biometric in nature or memorized, not written down. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module.
	XXXX:	
	Overall Match:	Comments:
130	FBCA <b>6.4.2</b>	The protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CP or CPS.
	XXXX:	
	Overall Match:	Comments:
131	FBCA <b>6.5.1</b>	The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. <ul style="list-style-type: none"> <li>- Require authenticated logins</li> <li>- Provide Discretionary Access Control</li> <li>- Provide a security audit capability</li> <li>- Restrict access control to FBCA services and PKI roles</li> <li>- Enforce separation of duties for PKI roles</li> <li>- Require identification and authentication of PKI roles and associated identities</li> <li>- Prohibit object re-use or require separation for FBCA random access memory</li> <li>- Require use of cryptography for session communication and database security</li> <li>- Archive FBCA history and audit data</li> <li>- Require self-test security related FBCA services</li> <li>- Require a trusted path for identification of PKI roles and associated identities</li> <li>- Require a recovery mechanisms for keys and the FBCA system</li> <li>- Enforce domain integrity boundaries for security critical processes</li> </ul>
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
132	FBCA <b>6.5.1</b>	When CA equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as that which received the evaluation rating.
	XXXX:	
	Overall Match:	Comments:
133	FBCA <b>6.6.1</b>	Use software that has been designed and developed under a formal, documented development methodology.
	XXXX:	
	Overall Match:	Comments:
134	FBCA <b>6.6.1</b>	Hardware and software procured to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
	XXXX:	
	Overall Match:	Comments:
135	FBCA <b>6.6.1</b>	Hardware and software developed specifically for the CA shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
	XXXX:	
	Overall Match:	Comments:
136	FBCA <b>6.6.1</b>	All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the CA physical location.
	XXXX:	
	Overall Match:	Comments:
137	FBCA <b>6.6.1</b>	The CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications; hardware devices, network connections, or component software installed which are not part of the CA operation.
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
138	FBCA <b>6.6.1</b>	Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Only applications required to perform the operation of the CA shall be obtained from sources authorized by local policy. RA hardware and software shall be scanned for malicious code on first use and periodically thereafter.
	XXXX:	
	Overall Match:	Comments:
139	FBCA <b>6.6.1</b>	Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.
	XXXX:	
	Overall Match:	Comments:
140	FBCA <b>6.6.2</b>	The configuration of the FBCA or Entity CA system as well as any modifications and upgrades shall be documented and controlled.
	XXXX:	
	Overall Match:	Comments:
141	FBCA <b>6.6.2</b>	There shall be a mechanism for detecting unauthorized modification to the FBCA or Entity CA software or configuration.
	XXXX:	
	Overall Match:	Comments:
142	FBCA <b>6.6.2</b>	A formal configuration management methodology shall be used for installation and ongoing maintenance of the FBCA or Entity CA system.
	XXXX:	
	Overall Match:	Comments:
143	FBCA <b>6.6.2</b>	The FBCA or Entity CA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.
	XXXX:	
	Overall Match:	Comments:
144	FBCA <b>6.7</b>	Entity CAs shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks.
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
145	FBCA <b>6.7</b>	Unused network ports and services shall be turned off.
	XXXX:	
	Overall Match:	Comments:
146	FBCA <b>6.7</b>	Any network software present shall be necessary to the functioning of the Entity CA.
	XXXX:	
	Overall Match:	Comments:
147	FBCA <b>6.7</b>	Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.
	XXXX:	
	Overall Match:	Comments:
148	FBCA <b>7.1.1</b>	The FBCA and Entity CAs shall issue X.509 v3 certificates (populate version field with integer "2").
	XXXX:	
	Overall Match:	Comments:
149	FBCA <b>7.1.2</b>	Certificates issued by the FBCA shall comply with Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile [FPKI-Prof].
	XXXX:	
	Overall Match:	Comments:
150	FBCA <b>7.1.2</b>	Whenever private extensions are used, they shall be identified in a CPS.
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
151	FBCA 7.1.3	Certificates issued under this CP shall use the following OIDs for signatures: id-dsa-with-sha1 (1.2.840.10040.4.3) or sha-1WithRSAEncryption (1.2.840.113549.1.1.5).
	XXXX:	
	Overall Match:	Comments:
152	FBCA 7.1.3	Certificates under this CP will use the following OIDs for identifying the algorithm for which the subject key was generated: id-dsa (1.2.840.10040.4.1), RsaEncryption (1.2.840.133549.1.1.1), Dhpublicnumber (1.2.840.10046.2.1) or id-keyExchangeAlgorithm (2.16.840.1.101.2.1.1.22).
	XXXX:	
	Overall Match:	Comments:
153	FBCA 7.1.4	Where required as set forth above, the subject and issuer fields of the base certificate shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by [RFC2459].
	XXXX:	
	Overall Match:	Comments:
154	FBCA 7.1.6	Certificates issued under this CP shall assert the OID appropriate to the level of assurance with which it was issued.
	XXXX:	
	Overall Match:	Comments:
155	FBCA 7.2.1	Entity CAs shall also issue X509 version two (2) CARLs/CRLs.
	XXXX:	
	Overall Match:	Comments:
156	FBCA 7.2.2	Detailed CARL/CRL profiles addressing the use of each extension shall conform to [FPKI-PROF].
	XXXX:	
	Overall Match:	Comments:
157	FBCA Cross Certification Prerequisites	<ol style="list-style-type: none"> <li>1. Certification Practices Statement has been submitted to the FPKIPA.</li> <li>2. Independent audit has been satisfactory completed.</li> <li>3. Executive audit summary has been submitted to the FPKIPA.</li> <li>4. Memorandum of Agreement has been signed and submitted to the FPKIPA.</li> </ol>
	XXXX:	
	Overall Match:	Comments:

Note: See Table 69 for reference to Auditable events:

## ROLES as Described in Section 5.2.1 (See Table 125)

1. *Administrator* – authorized to install, configure, and maintain the CA; establish and maintain CA system accounts; configure certificate profiles or templates and audit parameters; and generate and backup component keys. Administrators do not issue certificates to subscribers.
2. *Officer* – authorized to issue certificates; that is, register new subscribers, verify the identity of subscribers and the accuracy of information included in certificates, request, approve, and execute the issuance of certificates, and request, approve, and execute the revocation of certificates.
3. *Auditor* – authorized to review, maintain, and archive audit logs, and perform or oversee internal compliance audits to ensure that the FBCA or Entity CA is operating in accordance with its CPS
4. *Operator* – authorized to perform routine CA equipment operations, such as system backup and recovery or changing recording media.

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

## 5.0 REFERENCES

- [1] Request for Comments (RFC): 2527; Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, March 1999, <http://www.ietf.org/rfc/rfcXXXX527.txt>
- [2] CMS XXXX Department of Central Management Services, XXXX Certificate Policy for Digital Signature And Encryption Applications v1.2.4, January 3, 2003
- [3] X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), 10 September 2002.

## 6.0 CONTACT DETAILS

Comments about this document may be sent to the following people:

Tim Polk, NIST	301.975.3348	<a href="mailto:tim.polk@nist.gov">tim.polk@nist.gov</a>
Brian Dilley, Booz Allen Hamilton	410.684.6202	<a href="mailto:dilley_brian@bah.com">dilley_brian@bah.com</a>