

CPWG Mapping Comparison Matrix

Federal Bridge Certification Authority (FBCA) and the XXXX

**For cross certification at a
High Level of Assurance**

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

TABLE OF CONTENTS

1.0 INTRODUCTION..... 3

2.0 EXECUTIVE SUMMARY..... 3

3.0 BRIEF ASSESSMENT 5

4.0 DETAILED ASSESSMENT..... 6

5.0 REFERENCES..... 14

6.0 CONTACT DETAILS 14

1.0 INTRODUCTION

The purposes of this certificate policy comparison, in relation to the comparison study conducted with **XXXX** [2] and the FBCA CP [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 at a High Level of Assurance,
- 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 at a High Level of Assurance, and
- 3) To recommend appropriate changes, if required, to **XXXX** [2] that would make it more consistent with the FBCA CP [3];

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

- 1) **EXECUTIVE SUMMARY**, which 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**, which provides a brief indication of the degree of similarity of each **XXXX** as compared to the FBCA CP by indicating the evaluation term used in each main subsection of the CP; and
- 3) **DETAILED ASSESSMENT**, which presents a detailed breakdown of the requirements in the FBCA CP, Section by Section, and categorizes the degree of similarity of the **XXXX** 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 systematic overall Public Key Infrastructure (PKI). The FBCA functions as a non-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 certificate, so that the levels 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 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, so that digital certificates issued by one CA can be honored with an appropriate level of trust [or assurance] by a different CA.

The FBCA acts as a non-hierarchical "hub." A Principal CA receives permission to interoperate with the FBCA under terms and conditions described in the application for cross certification. This system will allow every CA that cross certifies with the FBCA the possibility of interoperating with all participating agencies using FBCA-issued cross 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 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 agency or party, it is not required to use the mapping expressed in the FBCA certificates. The Applicant, at its sole discretion, may choose to use a separate mapping for certain transactions or for all transactions.

The **XXXX** operates a PKI to provide security for its electronic information. The **XXXX** consists of products and services that provide and manage X.509v3 certificates for public-key cryptography. A **XXXX** digital certificate identifies the individual named in the certificate requestor/holder, and binds that person to a unique public/private 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 in 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** defines the primary obligations and operational responsibilities of all **XXXX** program participants, and defines the creation, management and use of X.509 Version 3 digital certificates. The **XXXX** 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 High Level CP mapping comparison identifies any differences between the FBCA CP and **XXXX** based on a set of predetermined evaluation terms, 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 the mapping table results, representing a high level view of the mapping comparison between the FBCA CP [3] and the **XXXX** [2]. This table presents a concise indication of the degree of conformity between the **XXXX** [2] and the FBCA CP [3] at the High Level of Assurance. This brief assessment in conjunction with the *General Requirements CP Mapping Matrix* report dated **DD MM YYY**, verify that the **XXXX**, verify that the **XXXX** is compliant with the FBCA CP for a cross certification with the FBCA at a High Level of Assurance.

The “Brief Assessment” table provides a quick evaluation list to facilitate the quick identification that the **XXXX** was evaluated against and the “Overall Match” status as compared to the FBCA CP requirement. The **XXXX** Section column is left blank if it is the same as the FBCA Section for the data being analyzed, if a different Section number reference has been inserted, it is the corresponding Section in the **XXXX** that carries the data that is being compared.

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

- 1) **FBCA** – identifies the FBCA CP reference section number of the CP
- 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 **XXXXXX** 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.

HIGH LEVEL OF ASSURANCE MAPPING RESULTS

FBCA Section	XXXX Section	Section Topic	Evaluation Summary
	1.0	INTRODUCTION	
1.2		Identification	
1.3.4		Applicability	
	2.0	GENERAL PROVISIONS	
2.7.1		Frequency of Entity Compliance Audit	
	3.0	IDENTIFICATION AND AUTHENTICATION	
3.1.1		Types of Names	
3.1.2		Need for Names to be Meaningful	
3.1.7		Method to prove possession of private key	
3.1.9		Authentication of Individual Identity	
3.2.1		Certificate Re-Key	
	4.0	OPERATIONAL REQUIREMENTS	
4.1.1		Delivery of public key for certificate issuance	
4.3		Certificate Acceptance	
4.4.3.1		CRL issuance requirements	
4.5		Security Audit Procedure	
4.5.2		Frequency of processing data	
4.6.1		Types of events archived	
4.6.2		Retention period for archive	
	5.0	PHYSICAL, PROCEDURAL AND PERSONELL SECURITY CONTROLS	
5.1.2		Physical access	
5.1.3		Electrical Power	
5.1.8		Off-site backup	
5.2.2		Separation of Roles	
5.2.4		Identification and authentication for each role	
	6.0	TECHNICAL SECURITY CONTROLS	
6.1.1		FBCA and CA key pair generation	
6.1.8		Hardware/Software Subscriber key generation	
6.1.9		Key usage purposes (as per X.509 v3 key usage field)	
6.2.1		Standards for cryptographic module	
6.2.4.2		Backup of subscriber private signature key	
6.3		Good Practices Regarding Key-Pair Management	
6.4.1		Activation data generation and installation	

4.0 DETAILED ASSESSMENT

This section of the report presents the mapping comparison results for the FBCA CP and the **XXXX** for High Level of Assurance requirements. This mapping comparison report works in conjunction with

the FPKIPA General Requirements CP Mapping Matrix report [4], **dated DD MM YYYY**. Following are the specific High Level CP requirements for mapping to the FBCA CP. The mapping comparison is characterized using the evaluation terms listed in the BRIEF ASSESSMENT.

The detailed mapping results provide the FBCA and requirements to be mapped, the **XXXX** and appropriate applicable policy text, the evaluation result for each requirement element addressed by the **XXXX**, as well as the evaluation comments. By default, the evaluation results listed in the “Overall Match” field indicates all results when multiple policy elements from the **XXXX** are mapped to a particular FBCA CP requirement.

Table No.	CP Section	Mapping Phrase
1	FBCA: 1.2	The OIDs are registered under the id-infosec arc as follows: Id-fpki-certpcy-highAssurance (:= fbca-policies 4) := { 2 16 840 1 101 3 2 1 4 }
	XXXX:	
	Overall Match:	Comments:
2	FBCA: 1.3.4	The sensitivity of the information processed or protected using certificates issued by FBCA or an Agency CA will vary significantly. High - This level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.
	XXXX:	
	Overall Match:	Comments:
3	FBCA: 2.7.1	The FBCA, Agency Principal CAs and RAs and their subordinate CAs and RAs shall be subject to a periodic compliance audit which is no less frequent than once per year for High and Medium Assurance.
	XXXX:	
	Overall Match:	Comments:
4	FBCA: 3.1.1	...Below describes the naming requirements that apply to each level of assurance. High – X.500 Distinguished Name, and optional alternative subject Name if marked non-critical
	XXXX:	
	Overall Match:	Comments:
5	FBCA: 3.1.2	All certificates issued by the FBCA at the Medium or High Assurance levels shall have name constraints asserted that limit the name space of the Principal CAs to that appropriate for their domains.
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
6	FBCA: 3.1.7	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:
7	FBCA: 3.1.9	...summarizes the identification requirements for each level of assurance. High - Identity established by in-person appearance before the Registration Authority or Trusted Agent; information provided shall be checked to ensure legitimacy Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License)
	XXXX:	
	Overall Match:	Comments:
8	FBCA: 3.2.1	Subscribers of Agency CAs shall identify themselves for the purpose of re-keying as required in table below. 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
	XXXX:	
	Overall Match:	Comments:
9	FBCA: 4.1.1	For all levels of assurance, this binding may be accomplished using cryptography. If cryptography is used, it must be at least as strong as that employed in certificate issuance.
	XXXX:	
	Overall Match:	Comments:
10	FBCA: 4.3	For Medium and High Assurance levels, a Subscriber shall be required to sign a document containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate.
	XXXX:	
	Overall Match:	Comments:
11	FBCA: 4.4.3.1	...CRL issuance requirements (Routine), and CRL issuance requirements (Loss or Compromise of Private Key). High – At Least Once Each Day (Routine)/Within 6 Hours of Notification (Loss or Compromise of Private Key).
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
12	FBCA: 4.5	Auditing capabilities are as set forth in the table below. [SEE END OF DOCUMENT]
	XXXX:	
	Overall Match:	Comments:
13	FBCA: 4.5.2	Frequency of processing data High: At least once per month Statistically significant set of security audit data generated by Entity CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity
	XXXX:	
	Overall Match:	Comments:
14	FBCA: 4.6.1	The following minimum data shall be recorded for archive: <ul style="list-style-type: none"> - Agency CA accreditation - CPS - 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 Agency CA re-key - All CARLs and CRLs issued and published - All audit logs - Other data or applications to verify archive contents - Documentation required by compliance auditors
	XXXX:	
	Overall Match:	Comments:
15	FBCA: 4.6.2	The minimum retention period for archive records is 20 years and 6 months.
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
16	FBCA: 5.1.2	<p>A security check of the facility housing the FBCA or Agency CA equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:</p> <ul style="list-style-type: none"> - The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open”, and secured when “closed”; and for the FBCA, that all equipment other than the repository is shut down); - Any security containers are properly secured; - Physical security systems (e.g., door locks, vent covers) are functioning properly; and - The area is secured against unauthorized access.
	XXXX:	
	Overall Match:	Comments:
17	FBCA: 5.1.2	<p>In addition to those requirements, the following requirements shall apply to CAs that issue Medium or High assurance certificates:</p> <ul style="list-style-type: none"> - Be manually or electronically monitored for unauthorized intrusion at all times - Ensure an access log is maintained and inspected periodically - Require two-person physical access control to both the cryptographic module and computer system
	XXXX:	
	Overall Match:	Comments:
18	FBCA: 5.1.3	<p>The FBCA and Agency CAs (operating at the Basic Assurance level or higher) shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown.</p>
	XXXX:	
	Overall Match:	Comments:
19	FBCA: 5.1.8	<p>Full system backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in the respective CPS.</p>
	XXXX:	
	Overall Match:	Comments:
20	FBCA: 5.2.2	<p>Separation of Roles</p> <p>High - Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume only one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA system shall identify and authenticate its users and shall ensure that no user identity can:</p> <ul style="list-style-type: none"> - Assume both the Administrator and Officer roles - Assume both the Administrator and Auditor roles - Assume both the Auditor and Officer roles. - No individual shall have more than one identity
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
21	FBCA: 5.2.4	An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.
	XXXX:	
	Overall Match:	Comments:
22	FBCA: 6.1.1	Cryptographic keying material for certificates issued by the FBCA or Entity CAs shall be generated in FIPS 140 validated cryptographic modules. For the FBCA, the modules shall meet or exceed Security Level 3. For Entity CAs, the modules shall meet or exceed Security Level 1 (for Rudimentary), Security Level 2 (for Basic or Medium), or Security Level 3 (for High).
	XXXX:	
	Overall Match:	Comments:
23	FBCA: 6.1.8	Any pseudo-random numbers used for key generation material shall be generated by a FIPS approved method. High – Hardware Only
	XXXX:	
	Overall Match:	Comments:
24	FBCA: 6.1.9	Agencies are encouraged at all levels of assurance to issue Subscribers two key pairs, one for data encryption and one for digital signature and authentication.
	XXXX:	
	Overall Match:	Comments:
25	FBCA: 6.2.1	... minimum requirements for XXXX cryptographic modules High – Latest version of FIPS 140 series - Required FBCA - Level 3 (Hardware) Certification Authority - Level 3 (Hardware) Subscriber – Level 2 (Hardware) Registration Authority - Level 2 (Hardware)
	XXXX:	
	Overall Match:	Comments:
26	FBCA: 6.2.4.2	Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the FBCA high Assurance policy, or an agency policy which maps to the FBCA high Assurance policy may not be backed up or copied.
	XXXX:	
	Overall Match:	Comments:
27	FBCA: 6.3	A single dual use key pair is prohibited for High assurance implementations, where one key-pair shall be used for digital signature/authentication, and a separate key-pair shall be used for confidentiality.
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
28	FBCA: 6.4.1	The activation data used to unlock FBCA, Agency CA or subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. High: it shall either entail the use of biometric data or satisfy the policy enforced at/by the cryptographic module. Where passwords are used as activation data, the password data shall be generated in conformance with FIPS-112. 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:

Note: this information is derived from the Certificate Issuing and Management Components Protection Profile being developed by NIST:

#	Auditable Event	XXXX High	FBCA High
	SECURITY AUDIT		
1	Any changes to the Audit parameters, e.g., audit frequency, type of event audited		X
2	Any attempt to delete or modify the Audit logs		X
	IDENTIFICATION AND AUTHENTICATION		
3	Successful and unsuccessful attempts to assume a role		X
4	Change in the value of maximum authentication attempts		X
5	Maximum number of unsuccessful authentication attempts during user login		X
6	An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts		X
7	An Administrator changes the type of authenticator, e.g., from password to biometrics		X
	KEY GENERATION		
8	Whenever the FBCA or Agency CA generates a key. (Not mandatory for single session or one-time use symmetric keys)		X
	PRIVATE KEY LOAD AND STORAGE		
9	The loading of Component private keys		X
10	All access to certificate subject private keys retained within the FBCA or Agency CA for key recovery purposes		X
	TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE		
11	All changes to the trusted public keys, including additions and deletions		X
	PRIVATE KEY EXPORT		
12	The export of private keys (keys used for a single session or message are excluded)		X
	CERTIFICATE REGISTRATION		
13	All certificate requests		X
	CERTIFICATE REVOCATION		
14	All certificate revocation requests		X
	CERTIFICATE STATUS CHANGE APPROVAL		
15	The approval or rejection of a certificate status change request		X
	FBCA OR AGENCY CA CONFIGURATION		
16	Any security-relevant changes to the configuration of the FBCA or Agency CA		X
	ACCOUNT ADMINISTRATION		
17	Roles and users are added or deleted		X
18	The access control privileges of a user account or a role are modified		X
	CERTIFICATE PROFILE MANAGEMENT		

#	Auditable Event	XXXX High	FBCA High
19	All changes to the certificate profile		X
	REVOCAION PROFILE MANAGEMENT		
20	All changes to the revocation profile		X
	CERTIFICATE REVOCAION LIST PROFILE MANAGEMENT		
21	All changes to the certificate revocation list profile		X
	MISCELLANEOUS		
22	<i>Installation of the Operating System</i>		X
23	<i>Installation of the FBCA or Agency CA</i>		X
24	<i>Installing hardware cryptographic modules</i>		
25	<i>Removing hardware cryptographic modules</i>		
26	<i>Destruction of cryptographic modules</i>		X
27	<i>System Startup</i>		X
28	<i>Logon Attempts to FBCA or Agency CA Apps</i>		X
29	<i>Receipt of Hardware / Software</i>		
30	<i>Attempts to set passwords</i>		X
31	<i>Attempts to modify passwords</i>		X
32	<i>Backing up FBCA or Agency CA internal database</i>		X
33	<i>Restoring FBCA or Agency CA internal database</i>		X
34	<i>File manipulation (e.g., creation, renaming, moving)</i>		
35	<i>Posting of any material to a repository</i>		
36	<i>Access to FBCA or Agency CA internal database</i>		
37	<i>All certificate compromise notification requests</i>		X
38	<i>Loading tokens with certificates</i>		
39	<i>Shipment of Tokens</i>		
40	<i>Zeroizing tokens</i>		X
41	<i>Rekey of the FBCA or Agency CA</i>		X
	<i>Configuration changes to the CA server involving:</i>		
42	<i>Hardware</i>		X
43	<i>Software</i>		X
44	<i>Operating System</i>		X
45	<i>Patches</i>		X
46	<i>Security Profiles</i>		
	PHYSICAL ACCESS / SITE SECURITY		
47	<i>Personnel Access to room housing FBCA or Agency CA</i>		
48	<i>Access to the FBCA or Agency CA server</i>		
49	<i>Known or suspected violations of physical security</i>		X
	ANOMALIES		
50	<i>Software Error conditions</i>		X
51	<i>Software check integrity failures</i>		X
52	<i>Receipt of improper messages</i>		X
53	<i>Misrouted messages</i>		X
54	<i>Network attacks (suspected or confirmed)</i>		X
55	<i>Equipment failure</i>		X
56	<i>Electrical power outages</i>		X
57	<i>Uninterruptible Power Supply (UPS) failure</i>		X
58	<i>Obvious and significant network service or access failures</i>		X
59	<i>Violations of Certificate Policy</i>		X
60	<i>Violations of Certification Practice Statement</i>		X
61	<i>Resetting Operating System clock</i>		X

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/rfc2527.txt>
- [2] X.509 Certificate Policy for XXXX Public Key Infrastructure (PKI), Revision **XXXX**, **DD MM YYYY**.
- [3] X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), 10 September 2002.
- [4] CPWG General Requirements CP Mapping Matrix for the **XXXX**, dated **DD MM YYYY**.

6.0 CONTACT DETAILS

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

Tim Polk, NIST	301.975.3348	tim.polk@nist.gov
Brian Dilley, Booz Allen Hamilton	410.684.6202	dilley_brian@bah.com