Criteria and Methodology For Cross-certification with the U.S. Federal Bridge Certification Authority (FBCA)

Version 3.0

January 25, 2012

Document Control Grid

Document Owner	FPKIPA/Certificate Policy Working Group (CPWG)
Contact	Fpki.webmaster@gsa.gov
Document Title	Criteria and Methodology for Cross-certification with the U.S. Federal Bridge Certification Authority (FBCA)

Revision History Table

Date	Version	Description	Author
4/10/07	2.0	First Released Version	CPWG
4/14/08	2.01	C4CA audit requirements edit	Judith Fincher
4/30/08	2.1	C4CA Crits and Methods-edit	Dr. Peter Alterman
10/22/08	2.2	C4CA Crits and Methods edit to update dates, references, terminology	Brant Petrick, Judith Fincher, Matt King
10/05/09	2.3	Modify Step 2 Documentation Submission to include Applicant's self-evaluation and Step 3 CPWG Policy Mapping process	CPWG New Way to Map Work Group
12/01/09	2.4	Additional modifications for self-evaluation	CPWG New Way to Map Work Group
1/25/12	3.0	2011 update. Various updates including but not limited to (1) hyperlink updates, (2) recognition of PIV-I, and (3) process revisions, (4) removal of the decommissioned C4CA, (5) revision to diagrams to reflect current FPKI environment, (6) enhance document terminology, consistency, and presentation, (7) option for Legacy Federal PKIs to cross-certify directly with the FCPCA.	CPWG

TABLE OF CONTENTS

Figures

1 INTRODUCTION

1.1 OBJECTIVE

This document identifies the criteria for determining Applicant suitability, and defines the methodology for implementing and maintaining cross-certification with the U.S. Federal Government's Federal Bridge Certification Authority (FBCA) by external entity Public Key Infrastructures (PKIs) and PKI Bridges.

1.2 BACKGROUND

In December 2000, the Federal Chief Information Officer's Council approved the "*X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)*" [FBCA CP]. The policy defines the FBCA as an interoperability mechanism for ensuring trust across disparate PKI domains. Successful cross-certification with the FBCA asserts that the Applicant operates in accordance with the standards, guidelines and practices of the Federal PKI Policy Authority (FPKIPA) and of the Identity, Credential, and Access Management Subcommittee (ICAMSC).

Subsequently, the FPKI Trust Infrastructure (formerly known as FPKI Architecture) was expanded to include the following Certification Authorities (CAs): the Federal PKI Common Policy Framework CA (FCPCA), and three e-Governance CAs (EGCA). In 2009, the ICAMSC published [FICAM Roadmap and Implementation Guidance] to help agencies manage their ICAM Program. The term FPKI Trust Infrastructure refers to the CAs maintained by the FPKI Management Authority (FPKIMA).

The FCPCA is the trust anchor and root for the U.S. Federal Government's PKI Shared Service Provider program. This program certifies trusted third-party PKIs that operate CAs under the [FCPCA CP] for the purpose of providing PKI services to federal agencies. The FCPCA is cross-certified with the FBCA at medium, medium hardware, and high levels of assurance. The FCPCA can also be used as the Trust Anchor for legacy Federal PKIs cross-certified with either the FBCA or FCPCA. Legacy federal PKIs cross-certified directly to the FCPCA were mapped to the FBCA, therefore this document is still applicable. Information about becoming a PKI Shared Service Provider can be found at the FPKI Shared Service Provider Working Group web site.

The EGCA support the E-Authentication Program by issuing SSL/TLS server certificates to federated credential service providers. The EGCA are not cross-certified with any other CA in the FPKI Trust Infrastructure. Additional information about the EGCA can be found at the FPKI web site.

In December, 2010, the SHA-1 Federal Root CA (SHA1 FRCA) was established to facilitate interoperability with the FPKI Trust Infrastructure for those unable to transition to SHA-256 by January 1, 2011. In addition, the FPKIPA determined legacy Federal PKIs may perform policy mapping and cross-certification with either the FCPCA or FBCA. **Error! Reference source not found.** Figure 1 shows a simplified layout of the Federal PKI Trust Infrastructure.

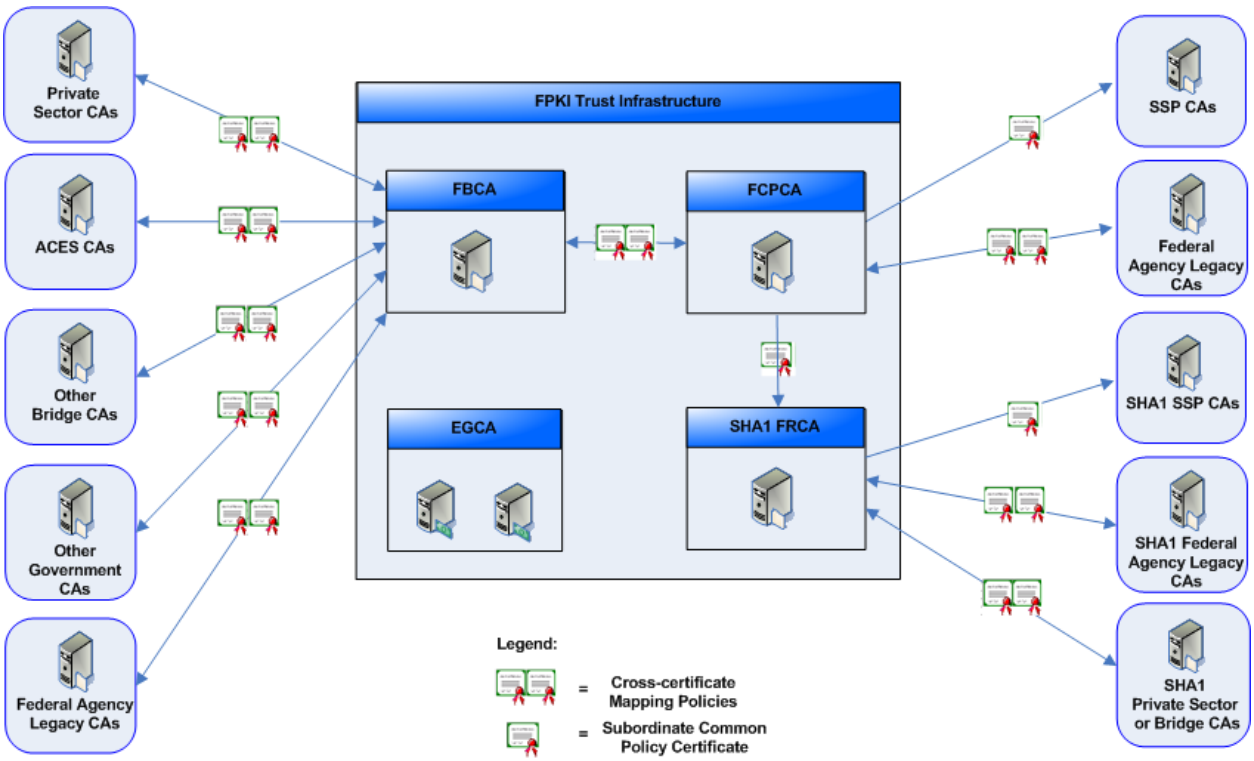

Figure 1: Federal PKI Trust Infrastructure

1.3 FEDERAL PKI POLICY AUTHORITY (FPKIPA)

The FPKIPA, operating under the authority of the Federal CIO Council, sets policy governing operation of the FBCA and FCPCA. It also approves Applicants for cross-certification with the FBCA. The "*Federal PKI Policy Authority Charter For Operations*" [FPKIPA Charter] identifies the operations of the FPKIPA.

Figure 2 shows the organization of the FPKIPA and its Working Groups.

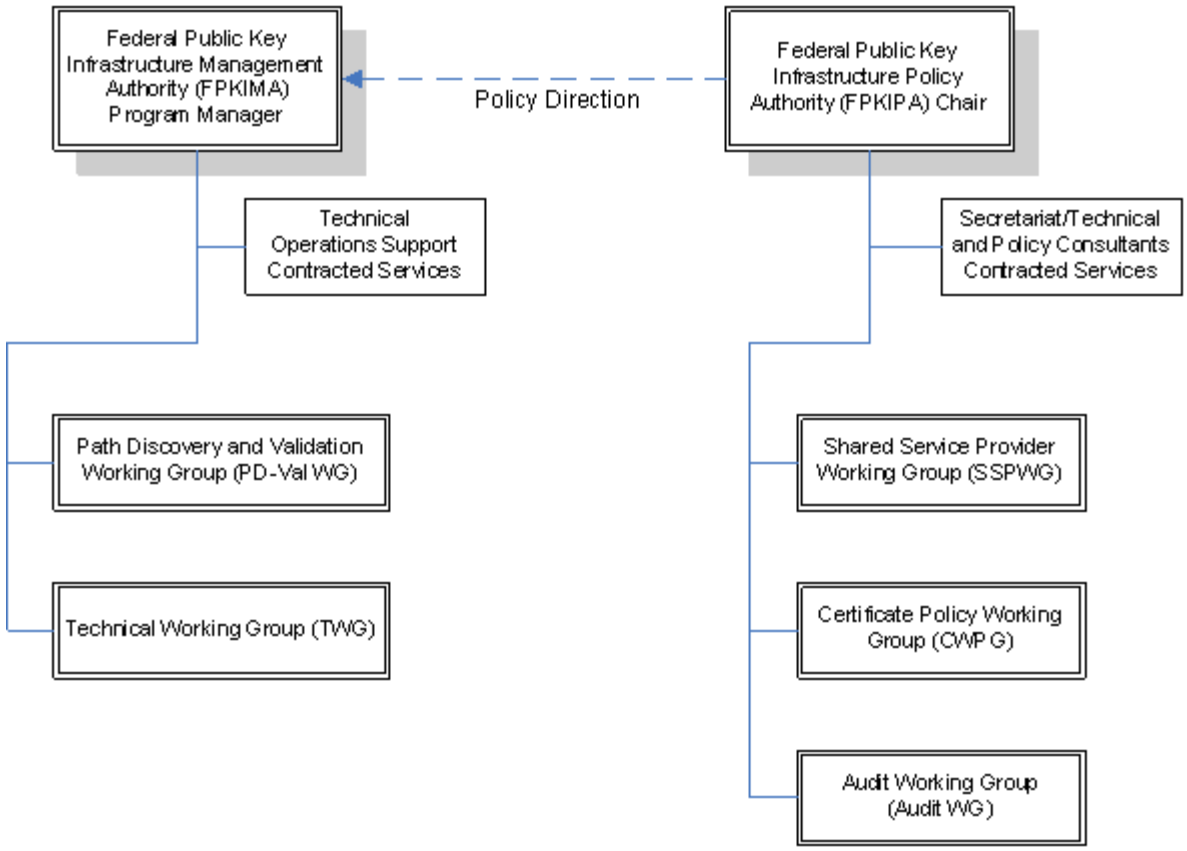

Figure 2: FPKIPA and Working Groups

1.4 INTENDED AUDIENCE AND SCOPE

This document, issued under the authority of the FPKIPA, is intended for the use of information technology officials, PKI managers, and personnel involved in cross-certification activities within the government, and between the FBCA and external CAs. Cross-certification activities between the FCPCA and Shared Service Provider CAs, and activities regarding the EGCA are out of scope of this document. Additional information about these and other government credentialing activities can be found at www.idmanagement.gov.

These cross-certification guidelines should be read in conjunction with the [FBCA CP].

Readers can find further detail on the U.S. federal government FBCA at the FPKI web site. Requests for information can also be directed to fpki.webmaster@gsa.gov.

1.5 GENERAL PRINCIPLES

The full benefits of public key cryptography can be achieved through the widespread cross-certification of PKIs. However, given the need to allocate resources carefully within the government, some parameters must be established in order to prioritize cross-certification activities.

Note: *It must be emphasized that cross-certification with the U.S. federal government FBCA is not a right, nor should any discussions be considered a commitment to issue cross-certificates.*

Cross-certificates issued by the FBCA are issued and revoked at the sole discretion of the FPKIPA. When the FBCA issues a cross-certificate to a non-federal entity, it does so for the convenience of the U.S. Federal Government. Any review by the FPKIPA of any information from an Applicant is for the use of the FPKIPA in determining whether or not interoperability is possible and desirable, and will be treated as proprietary in accordance with any applicable Non-Disclosure Agreements.

Applicants must determine whether the FBCA meets the policy and legal requirements for issuing a cross-certificate to the FBCA by mapping one or more Applicant assurance levels to the FBCA assurance levels. The FPKI Certificate Policy Working Group (CPWG) will conduct a similar review of the Applicant's CP at the requested assurance levels. CPWG review and FPKIPA acceptance of an Applicant CP is not a substitute for due care and mapping of certificate policies by the Applicant.

Subject to this document, the U.S. Federal Government will consider applications for cross-certification from any entity operating a CA if such cross-certification is in support of U.S. Federal Government initiatives, specifically to facilitate electronic business applications and operating programs that require confidence in the asserted identity's validity, or that use PKI technology to transmit identity information for authentication.

PKIs operated by U.S. federal government agency Applicants must be certified and accredited in accordance with the requirements of Office of Management and Budget (OMB) Circular A-130 Appendix III, [FPKI Security Controls of NIST SP 800-53], [FPKI Security Controls of NIST SP 800-53A], and other relevant Federal IT security policies. PKIs run by non-U.S. federal government agency Applicants are expected to satisfy equivalent IT security standards[1].

All Applicants for cross-certification must obtain unique policy Object Identifiers (OIDs) in the standard International Organization of Standardization (ISO) object identifier registry from the appropriate commercial or national registration authority. U.S. federal government agencies may obtain policy OIDs from the NIST Computer Security Objects Registry.

1.6 DEFINITIONS

The following terms are used in this guideline. Some definitions have been provided for terms contained in the "Internet Security Glossary" [RFC 2828].

Affiliate PKI: An approved Applicant or Applicant Bridge PKI that has successfully completed all steps required to become cross-certified and has been issued a cross-certificate by the FBCA (or one of the other FPKI Trust Infrastructure CAs).

Applicant: An entity requesting cross-certification with the FBCA.

Bridge CA: A CA that itself does not issue certificates to end entities (except those required for its own operations) but establishes unilateral or bilateral cross-certification with other CAs.

[1] The FPKIPA will draft a document that discusses IT security standard equivalencies for private sector PKIs.

Certification Authority (CA): An entity that issues certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate [RFC 2828].

Certificate Policy (CP): A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements [RFC 2828]. A PKI may adopt more than one CP.

Certificate Policy Working Group (CPWG): A subordinate committee of the FPKIPA that is responsible for reviewing Applicant CPs; for performing the policy mapping of the submitted policies to the [FBCA CP] on behalf of the FPKIPA; and, for advising the FPKIPA at which level of assurance the Applicant CP(s) would map to the [FBCA CP]. The CPWG also recommends changes to the [FBCA CP] to the FPKIPA for approval.

Certificate Revocation List (CRL): A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire [RFC 2828].

Certification Practice Statement (CPS): A declaration by a CA of the details of the system and practices it employs in its certificate management operations A CPS is usually more detailed and procedurally oriented than a CP [RFC 2828].

Cross-Certificate: A certificate issued by one CA to another CA for the purpose of establishing a trust relationship between the two CAs.

Cross-certification: The act or process by which two CAs each certify a public key of the other, issuing a public-key certificate to that other CA [RFC 2828].

Digital Signature: A value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity [RFC 2828].

Directory: A database server or other system that provides information, such as a digital certificate or CRL, about an entity whose name is known [RFC 2828].

Federal Bridge Certification Authority (FBCA): the U.S. Federal Government's mechanism for enabling trust domain interoperability at a level of assurance satisfying E-Authentication levels 1 through 4 using public key certificates.

Public Key Certificate: A digital certificate that binds a system entity's identity to a public key value, and possibly to additional data items; a digitally-signed data structure that attests to the ownership of a public key [RFC 2828].

Public Key Infrastructure (PKI): A system of CAs that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography [RFC 2828]. As used in this document, PKI also includes the entire set of policies, processes, and CAs used for the purpose of administering certificates and keys. The term also designates the person or organizational unit within an entity responsible for the following:

(a) Operation of a Certification Authority trusted by one or more users to issue and manage public key certificates and certificate revocation mechanisms; or
(b) Management of:

(i) Any arrangement under which an entity contracts for the provision of services relating to the issuance and management of public key certificates and certificate revocation lists on its behalf; and

(ii) Policies and procedures within the entity for managing public key certificates issued on its behalf.

Note: *A PKI remains at all times responsible and accountable for managing the public key certificates it issues or arranges to be issued on behalf of its organization.*

Repository: A system for storing and distributing digital certificates and related information (including CRLs, CPSs, and certificate policies) to certificate users [RFC 2828].

Subscriber: An entity whose public key is contained in a certificate bound to the entity.

2 CROSS-CERTIFICATION PROCESS

Cross-certifying entity PKIs with the FBCA is a nine-step process. This process is designed to achieve a mutually-reliable trust relationship at an agreed-upon level or levels of assurance of identity. This section identifies the required steps and provides specific activities undertaken by the FPKIPA, subordinate committees of the FPKIPA, the FPKIMA, and the entity PKI to complete each step. For Applicants seeking cross-certification at Personal Identity Verification – Interoperable (PIV-I), additional documentation and actions are required for steps 1-6. Specifics on what is required are described at each step. The nine steps are:

- Step 1: Application Submission
- Step 2: Applicant FPKI Certification Evaluation Requirements and Documentation Submission
- Step 3: FPKI CPWG Policy Mapping
- Step 4: Compliance Audit Review
- Step 5: Analysis of Operational Parameters
- Step 6: Technical Review And Testing
- Step 7: Application Approval
- Step 8: Negotiation Of Memorandum Of Agreement (MOA)
- Step 9: Cross-certification

Once a completed application has been submitted (Step 1), the FPKIPA votes to accept or reject the application. If the application is accepted, the FPKIPA requests that the Applicant complete the *Applicant FPKI Certification Evaluation Requirements* [FBCA Mapping Matrix] document (self-evaluation) and submit required documentation (Step 2). If the application is rejected, the Applicant is notified in writing of the decision and provided the reasons why the application has been rejected. The FPKIPA may offer the Applicant the opportunity to resubmit an amended application depending upon the reasons for initial rejection.

Once the self-evaluation and additional documentation has been submitted, the CPWG, FPKIMA, and ICAM Lab then complete steps 3, 4, 5, and 6. The CPWG, FPKIMA, or ICAM Lab bring any significant concerns raised in completing Steps 3-6 to the attention and possible vote of the FPKIPA. These steps can be worked in parallel, but must all be completed prior to

the FPKIPA vote to approve or deny the application (Step 7). If the FPKIPA decides to terminate the cross-certification process, the Applicant is notified in writing of the decision and provided the reasons why the application has been rejected. The Applicant is also notified of any recourse or other steps that can be taken to address the reason for termination. If the application is accepted, the Applicant and the FPKIPA negotiate an MOA (Step 8), and cross-certify (Step 9) with the FBCA. Figure 3 illustrates the cross-certification process.

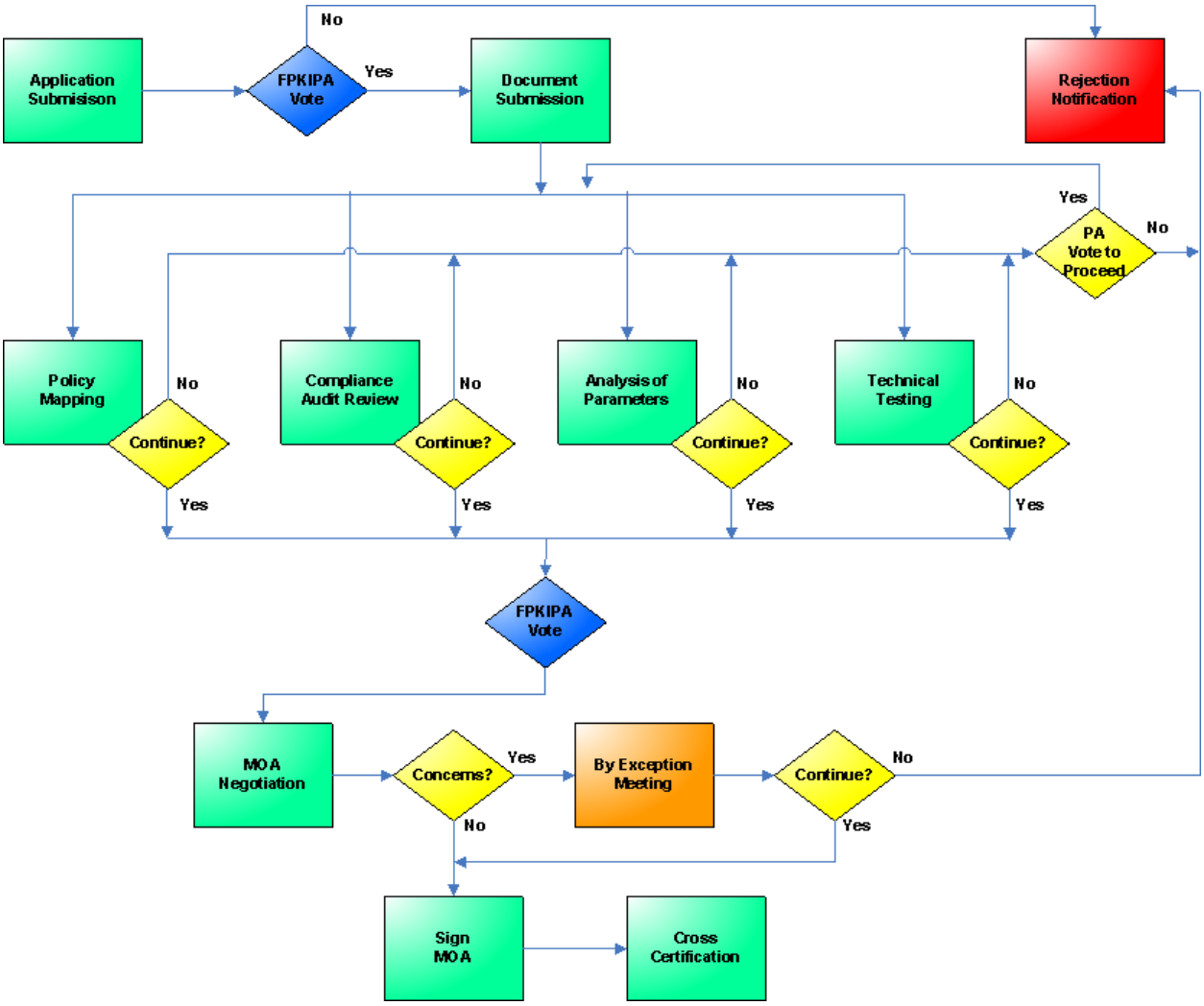

Figure 3: Cross-certification Process

2.1 STEP 1: APPLICATION SUBMISSION

The objective of this step is to determine if it is in the interest of the U.S. Federal Government to cross-certify with an Applicant.

To initiate the process of cross-certification with the FBCA, an Applicant must submit a formal application to cross-certify. The [Application Template] is available at the FPKIPA web site. The application must contain the following:

- Name and contact information (email address, phone number and address) for a principal point of contact (POC) and for a secondary POC.
- Information on the Applicant's PKI and Repositories (CA product, PKI architecture, and directory product for repository).
- The proposed FBCA level(s) of assurance at which cross-certification is sought.
- For Applicants other than U.S. federal entities or state governments, a statement of why cross-certification is sought, along with the name and contact information (organization, email address, phone number, and address) of a federal advocate where available.
- For non-government Applicants, evidence of the corporate status of the entity responsible for the PKI and financial capacity to manage the risks associated with the operation of the PKI. The nature and sufficiency of the corporate status and financial capacity will be determined at the discretion of the FPKIPA on a case-by-case basis.
- The signature of an appropriate senior official (an officer or executive) of the organization responsible for the Applicant who is authorized to commit the organization to completing the cross-certification process. Such a commitment would include bearing any expenses incurred by the organization during the cross-certification process, and the authorization of any submission of information or statement required from the Applicant.

Generally, an application is considered if it is from one of the following:

- A U.S. federal government entity.
- A commercial or non-commercial organization where there are reasonable expectations from a U.S. federal government entity that it would benefit from being able to do PKI-based transactions interactions with the Applicant PKI community of interest.
- A U.S. state, local, or tribal government.
- A country or a sub-federal entity of a country, where it would be in the interest of the U.S. Federal Government's international relations to cross-certify.

Activities

1. Applicant submits a formal written application to cross-certify with the FBCA to the FPKIPA Chair or Secretariat. Such application will use the format provided in [Application Template] to ensure completeness, and be signed by an appropriate senior official of the Applicant organization.
2. For non-government Applicants, the FPKIPA Attorney advises the FPKIPA on the legitimacy and authority of the Applicant organization and representation. The legal review may entail online research and verification of the authorization of the individual submitting the application[2].
3. The FPKIPA Secretariat schedules a review of the application at the next available FPKIPA Meeting.

[2] For non-U.S. Applicant PKIs, the Department of State advises the FPKIPA on the legitimacy and authority of the Applicant organization and representation, as well as on the need for and providing assistance with any international treaty.

4. Where provided, the federal agency advocate is invited to the FPKIPA meeting where the application will be reviewed.
5. The FPKIPA reviews the application.
6. Following review, the FPKIPA votes whether to accept or reject the application. A record of the discussion, and vote, and a copy of the application are kept in the Minutes of the FPKIPA meeting.
7. The FPKIPA Chair communicates the decision to proceed or not to proceed to the Applicant POC and to the FPKIPA members.

    a. If the decision is to proceed,

        – The Applicant is instructed to provide required self-evaluation and additional documentation to the FPKIPA point of contact as identified in Section 2.2, Step 2: Self-evaluation and Documentation Submission,
        – The FPKIPA Chair authorizes the CPWG Co-chairs to initiate mapping of the Applicant's CP(s), self-evaluation document ([FBCA Mapping Matrix]), review of compliance audit information, and analysis of Applicant CP operational parameters
        – The FPKIPA Chair authorizes the FPKIMA to initiate technical review and testing, and authorizes the ICAM Lab to initiate PIV-I Card testing if the application includes a request for PIV-I.
        – At the behest of Applicant, the FPKIPA may execute a Non-Disclosure Agreement (NDA) to ensure that all information presented during the application process will be treated in compliance with the terms of the agreement.

    b. If the decision is not to proceed,

        – The FPKIPA Chair notifies the Applicant POC in writing and provides the reasons why the request has been rejected.
        – The FPKIPA Chair, at his/her discretion, may provide the opportunity for resubmission of the application.

2.2 STEP 2: SELF-EVALUATION AND DOCUMENTATION SUBMISSION

The Applicant must submit the [FBCA Mapping Matrix] and additional documentation to support policy, audit compliance, operational analysis, and technical reviews by the FPKIPA. All documentation must be submitted in electronic format, either by email to fpki.webmaster@gsa.gov or by mail to the FPKIPA Chair, as listed at the FPKIPA web site. Signed documents should be submitted in a scanned Adobe Acrobat PDF format. Other documents may be submitted in either Adobe Acrobat PDF or Microsoft Office compatible formats. A checklist of documents to be submitted is also provided as Appendix .

The Applicant must demonstrate that the PKI is operated to a level of assurance comparable to the requirements in the [FBCA CP]. To support this process, mapping matrices have been developed that show requirements all PKIs must meet and those that are specific to each level of assurance [FBCA Mapping Matrix]. The Applicant will use [FBCA Mapping Matrix] to perform a self-evaluation. Evidence of compliant operation must also be provided through an

independent compliance audit performed by a qualified evaluator/auditor. Therefore, Applicants must submit the following:

- CP in the IETF RFC 3647, "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*" [RFC 3647] format, unless prior approval to submit in other format has been granted.
- Identification of which of the Applicant's CPs are to be considered for cross-certification at which assurance levels. NOTE: cross-certification at FBCA High assurance level is only authorized for U.S. federal government entity PKIs.
- Principal CA Certification Practice Statement (CPS).
- [FBCA Mapping Matrix]
- Other documentation needed to show evidence of comparability between the Applicant PKI and the requirements in the [FBCA CP].
- A signed third-party Auditor Letter of Compliance summarizing the results of an audit of its PKI operations that attests to the Applicant's claim that its PKI is operated in accordance with its CPS, and that the CPS implements the requirements of the CP. A template for the contents of this Auditor Letter of Compliance is provided in [FBCA Audit Letter].
- Additional Applicant POC information to support the remaining steps of the application process.

The Applicant must demonstrate that their PKI is technically compatible with the FBCA. This technical information includes the architecture of the PKI to include the X.500/LDAP directory structure for interoperating with the FPKI directory, if appropriate, and all URIs and repositories included to support the configuration of certificates issued by the Applicant. Applicants must submit the following documentation to support the technical review:

- Applicant PKI Architecture including a designated Principal CA and a list of subordinate CAs or cross-certified CAs within the PKI.
- List of CAs that have any other trust relationship with the Applicant PKI Principal CA, such as cross-certifications with other PKIs external to the Applicant PKI and the FPKI.
- Hierarchical DN relationships, if any, with other existing Affiliate PKIs (PKIs already cross-certified with the FPKI).
- Directory structure the Applicant PKI will use to interoperate with the FPKI Trust Infrastructure directory.
- Any additional repositories to support URLs in Applicant PKI certificates.
- Any additional certificate status mechanisms in the Applicant PKI.
- Configuration of certificates issued by the Applicant PKI. Capability of Applicant PKI to produce certificates conforming to the "*Federal PKI Certificate and CRL Extensions Profile*" [FPKI Profile].
- For PIV-I policy level Applicants conformance with "*X.509 Certificate and Certificate Revocation List Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards*" [PIV-I Profile] is also required.
- Statement of whether algorithms used by the Principal CA or by any other CA in the Applicant PKI architecture are executed in conformance with the "Digital Signature Standard" [FIPS 186]. If not, specify the standard with which it complies.

Activities

1. Applicant submits required self-evaluation and supporting documents to the FPKIPA Secretariat.
2. FPKIPA Secretariat forwards policy, self-evaluation and compliance audit documents to the CPWG. These documents are used by the CPWG to conduct Steps 3, 4, and 5, which may be conducted in parallel.
3. FPKIPA Secretariat forwards technical documents to the FPKIMA. These documents are used by the FPKIMA to conduct Step 6, which may be conducted in parallel with Steps 3, 4, and 5.

2.3 STEP 3: POLICY MAPPING

Policy mapping is the process of comparing and contrasting the Applicant CP to the [FBCA CP] and evaluating the extent to which the Applicant demonstrates policies, practices, and procedures consistent with those of the [FBCA CP] The specific [FBCA CP] requirements to be mapped at all assurance levels are contained in the [FBCA Mapping Matrix]. This policy mapping exercise allows the CPWG to determine if the Applicant CP is comparable to the appropriate CP at the requested level(s) of assurance. In some cases, [FBCA CP] requirements may not be contained in the Applicant CP, but are contained in other documents maintained by the Applicant. In this situation, the Applicant must reference the associated document in their CP to ensure that it will be included in any compliance audits, and must submit the associated documents containing the requirements to the CPWG to be included in the policy mapping. The CPWG will leverage the Applicant's self-evaluation as the primary source for policy mapping. When conducting the policy mapping exercise, the CPWG will:

- Analyze the Applicant's self-evaluation form and create the process area summary thread tables.
- Analyze the holistic process area summaries for comparability.
- Utilize the self-evaluation detailed tables for additional information if the process summary shows questionable comparability.
- If the CPWG recommends changes to the Applicant's CP, the Applicant may submit a revised CP. When the CPWG and Applicant agree the mapping is comparable, the CPWG will review the final Applicant CP to:
    1. Ensure the CP matches the Applicant's self assertions; and
    2. Ensure there are no contradictions or inconsistencies in the Applicant's CP.

Additional information can be found in [FBCA Mapping Matrix].

The results of the policy mapping exercise are recorded in the thread analysis summary tables by the CPWG. If there is a requirement for additional information to support or detail the comment, additional documentation may be used as long as the information is referenced correctly. At the conclusion of the mapping exercise, the CPWG prepares a [Certificate Policy Mapping Report] identifying any remaining discrepancies and identifying any additional documentation used in the mapping process, and forwards it to the FPKIPA Chair.

This Criteria and Methodology document only describes the CP mapping process that is performed by the CPWG to determine the appropriate mapping from the FBCA assurance levels to the Applicant PKI assurance levels for the cross-certificate issued to the Applicant PKI. It is the responsibility of the Applicant to perform a mapping exercise from the Applicant PKI to the FBCA to determine the appropriate mapping for the cross-certificate issued by the Applicant PKI.

Activities

> **Note:** *This is a participatory process. The Applicant will be required to provide a knowledgeable and authorized representative to the CPWG for the Certificate Policy mapping process. This representative shall not be the compliance auditor.*

1. The Applicant's self-evaluation will be reviewed by the CPWG to determine comparability.
2. The CPWG will create the process area summary thread tables with levels of assurance identified by the Applicant in the application, using the [FBCA Mapping Matrix] document.
3. The CPWG provides the Applicant POC with the completed process area summary thread tables identifying any discrepancies.
4. The Applicant addresses identified discrepancies by updating their CP or including additional documents and returns the updated documentation along with [FBCA Mapping Matrix]. If additional documentation is offered, the documentation must be referenced in the appropriate sections of the CP. Note that the Applicant will submit a delta matrix, not a brand new matrix.
5. Steps 1-3 may be repeated as necessary until the CPWG either determines that the Applicant has addressed all discrepancies or that the Applicant is not able or willing to address remaining discrepancies. See [FBCA Mapping Matrix] for time frame information.
6. Upon completion of the mapping process, the CPWG prepares a [Certificate Policy Mapping Report] identifying any remaining discrepancies, identifying additional documentation used in the mapping process, and containing a recommendation for acceptance or rejection.
7. If the CPWG recommends rejection or the [Certificate Policy Mapping Report] identifies significant discrepancies, the CPWG requests a FPKIPA discussion and vote. If no significant discrepancies are reported, the FPKIPA is notified of the completion of the policy mapping step.
8. If a vote has been requested, the FPKIPA reviews the Certificate Policy Mapping Request and votes whether to accept or reject the mapping recommendation of the CPWG. A record of the discussion and vote are kept in the Minutes of the FPKIPA meeting.
    a. If the decision is to accept, the FPKIPA Chair provides the [Certificate Policy Mapping Report] to the FPKIMA for archival.
    b. If the decision is to reject,
        – The FPKIPA Chair notifies the Applicant POC in writing of the decision, providing the reasons why the request for cross-certification has been rejected and the Applicant's recourse.

– No further cross-certification steps will be completed unless the Applicant satisfactorily resolves the identified issues.

2.4 STEP 4: COMPLIANCE AUDIT REVIEW

The trustworthiness of an Applicant PKI must be evaluated for the purposes of cross-certification. This evaluation must be performed by an independent third party who has demonstrated knowledge of PKI systems using explicitly-defined and appropriate auditing methodologies. Examples of the auditor are a commercial auditing firm, an Agency Inspector General, or an autonomous auditing entity of an academic institution or financial institution operated under Securities and Exchange Commission (SEC) review. Specific FPKI qualification requirements for the evaluator/auditor are found in the [FBCA CP] Section 8.2, *Identify and Qualifications of Assessor*, and Section 8.3, *Assessor's Relationship to Assessed Entity*.

The FPKIPA may request the bona fides of any third-party compliance auditor indicating that the auditor meets the specified requirements.

The Applicant must present evidence that its policy enforcement processes are performed as stated in their CP or CPS. This evidence must include a statement that audit reports showing compliance are on file for all CA components of the Applicant PKI. Evidence may include additional audit letters for various components of the Applicant PKI such as subordinate CAs and Registration Authorities (RAs) if these components are not covered in the PKI's Auditor Letter of Compliance.

As PKI and CA audit standards evolve and become more accepted, adherence to an international standard with verification through an independent audit performed by qualified auditors may become a pre-requisite for cross-certification with the FBCA. Given the absence of such standards at this time, audits will be accepted when performed by independent third parties who have demonstrated knowledge of PKI systems.

Specific requirements for what the Auditor Letter of Compliance must address are provided in [FBCA Audit Letter].

Activities

1. The CPWG reviews the Applicant's Auditor Letter of Compliance and determines whether it does the following:
   – Identifies the individuals performing the audit.
   – Identifies the experience these individuals have in auditing PKI systems.
   – Describes the relationship between the auditor and the Applicant.
   – States when the audit was performed.
   – States whether a particular methodology was used, and if so, what methodology.
   – Specifies which documents were reviewed as a part of the audit, including document dates and version numbers.
   – States that the Applicant's Principal CA CPS conforms to the requirements of the Applicant CP.
   – States that the Applicant's Principal CA is being operated in conformance with its CPS.

- For PKIs with multiple CAs, states that audit reports showing compliance were on file for additional CA components of the Applicant PKI, or are an included part of the report.

2. If the Applicant's Auditor Letter of Compliance is not sufficient, the CPWG provides feedback to the Applicant POC.
3. The Applicant may choose to submit an updated Auditor Letter of Compliance and/or additional information to address CPWG feedback.
4. Activities 1-3 are repeated as necessary until the CPWG either determines that the Applicant PKI has met the compliance audit requirements or that the Applicant is not able or willing to address remaining issues.
5. The CPWG provides the final version of the Auditor Letter of Compliance received from the Applicant along with recommendation as to its sufficiency in a [Compliance Review Report] to the FPKIPA Chair.
6. If the CPWG recommends that the Auditor Letter of Compliance is not sufficient or identifies other significant discrepancies, the CPWG requests a FPKIPA discussion and vote. If no significant discrepancies are reported, the FPKIPA is notified of the completion of the compliance audit review step.
7. If a vote has been requested, the FPKIPA reviews the [Compliance Review Report] and votes whether to accept or reject the recommendation in the [Compliance Review Report] concerning the adequacy of the Applicant's Auditor Letter of Compliance. A record of the discussion and vote are kept in the Minutes of the FPKIPA meeting. If the decision is to reject,
   - The FPKIPA Chair notifies the Applicant POC in writing of the decision, providing the reasons why the Applicant's Auditor Letter of Compliance has been rejected and the Applicant's recourse.
   - No further cross-certification steps will be completed unless the Applicant satisfactorily resolves the identified issues.
8. The FPKIPA Chair provides the Auditor Letter of Compliance and the [Compliance Review Report] to the FPKIMA for archival.

2.5 STEP 5: ANALYSIS OF OPERATIONAL PARAMETERS

Applicants must demonstrate that their operational parameters are consistent with the parameters of the [FBCA CP], and will not have an adverse affect on the FPKIPA or on U.S. federal government relying parties that may rely on certificates based on cross-certificate trust paths. A specific requirement-by-requirement mapping process was performed in the Policy Mapping step in Section 2.3. This analysis is a more general review of the Applicant CP and any other documentation provided regarding the requirements for operation of the Applicant PKI to ensure that text provided in these documents is consistent with the mapped sections of the CP and with the operational parameters of the FBCA. Although particular attention will be paid to CP Sections 1 and 9, heading sections and areas without specific [FBCA CP] requirements will also be reviewed.

If the CPWG identifies concerns with language contained in the CP or other documentation, the CPWG will provide feedback to the Applicant and request updated documentation addressing the identified concerns. Upon completion of the analysis, the CPWG documents its findings in the [PKI Operational Parameters Analysis Report] and forwards it to the FPKIPA Chair.

Activities

1. The CPWG performs an analysis of the Applicant CP and any other associated documentation provided by the Applicant to ensure that text provided in these documents is consistent with the mapped sections of the CP and with the operational parameters of the FBCA.
2. The CPWG informs the Applicant of any identified concerns and requests updates to the documentation to address those concerns.
3. Activities 1-2 may be repeated as necessary until the CPWG either determines that the Applicant has addressed all concerns or that the Applicant is not able or willing to address remaining concerns.
4. Upon completion of the operational parameters analysis, the CPWG prepares an [PKI Operational Parameters Analysis Report].
5. If the CPWG identifies significant discrepancies in the [PKI Operational Parameters Analysis Report], the CPWG requests a FPKIPA discussion and vote. If no significant discrepancies are reported, the FPKIPA is notified of the completion of the analysis of operational parameters step.
6. If a vote has been requested, the FPKIPA reviews the [PKI Operational Parameters Analysis Report] and votes whether to accept or reject the CPWG recommendation concerning the operational parameters of the Applicant PKI. A record of the discussion and vote are kept in the Minutes of the FPKIPA meeting.
    a. If the decision is to accept, the FPKIPA Chair provides the [PKI Operational Parameters Analysis Report] to the FPKIMA for archival.
    b. If the decision is to reject,
        – The FPKIPA Chair notifies the Applicant POC in writing of the decision, providing the reasons why the request for cross-certification has been rejected and the Applicant's recourse.
        – No further cross-certification steps will be completed unless the Applicant satisfactorily resolves the identified issues.

2.6 STEP 6: TECHNICAL REVIEW AND TESTING

Applicants must demonstrate that their PKI is technically compatible with the FBCA. Technical compatibility is determined through a review of the technical information submitted by the Applicant and through interoperability testing. Applicants for PIV-I policy levels are also required to go through PIV-I Card Testing.

The FPKIMA reviews the Applicant PKI architecture, any existing trust relationships that the Applicant PKI has entered into, the directory configuration that the Applicant PKI will use to

interoperate with the FPKI directory, and the conformance of the Applicant PKI certificates to the [FPKI Profile] and [FIPS 186].

Technical interoperability testing is used to ensure technical interoperability between the FBCA and the Applicant PKI. The objective of this step is to determine whether there can be a successful generation and exchange of conformant cross-certificates and directory interoperability, to identify and resolve any incompatibilities between the technologies of the FBCA and Applicant PKI products, and to minimize the risk of introducing incompatibilities with Affiliate PKIs.

The FPKI Community Interoperability Test Environment (CITE) [FPKI CITE] has been established to provide the community with a test environment to (1) identify and resolve issues, and (2) to ensure proper functionality, prior to deploying to the production environment. It is configured with a duplicate of the Production FPKI Trust Infrastructure. Technical personnel representing the Applicant will be required to work with the FPKIMA to complete the technical interoperability testing. Ongoing participation in CITE is optional for individual Entity PKIs.

Interoperability testing is best conducted when both the FPKIMA and the Applicant use test-bed systems. The Applicant is strongly encouraged to use a test-bed facility, set and configured in a manner that accurately represents the properties and specifications of the Applicant PKI production system for the purposes of cross-certification. This facility must be configured in accordance with [FPKI CITE]. Any costs incurred by the Applicant resulting from technical interoperability testing will be the responsibility of the Applicant. The Applicant is also strongly encouraged to maintain the test-bed facility after completion of the application process, so as to provide an environment for testing directory, patches, and new applications prior to deployment in the production environment. Technical interoperability testing at a minimum will demonstrate:

- Network connectivity can be achieved using all required protocols.
- If applicable, the directories of the FPKI and the Applicant PKI are interoperable.
- The cross-certificate is correctly constructed by the FBCA, and exchanged and recognized by the Applicant PKI CA.
- The cross-certificate is correctly constructed by the Applicant PKI CA, exchanged with the FBCA, and recognized by the FBCA.
- Upon Applicant request, a test transaction, using a test subscriber of the Applicant PKI, can be successfully validated.
- The FBCA and the Applicant PKI can share revocation information.
- If PIV-I is requested, the Applicant will provide a PIV-I Card to the ICAM Lab for logical testing and will support the ICAM Lab in performing Physical Access Control System (PACS) testing. PACS testing requires the person whose biometrics are on the Card to be present during testing.

The results of the interoperability testing, including a description of any deficiencies identified during the test, are documented in a [Technical Analysis Report], and forwarded to the FPKIPA Chair. Deficiencies may include technical interoperability deficiencies and potential performance issues that were not specifically identified by the test criteria. The report will also include the anticipated consequences of the deficiencies and a recommendation by the FPKIMA. The FPKIMA may provide the [Technical Analysis Report] to the FPKIPA for discussion as needed.

The results of the PIV-I Card Testing are documented in a [PIV-I Card Test Report] and provided to the FPKIPA Chair.

Activities

1. The FPKIMA and the Applicant determine if any constraints need to be placed in any cross-certificates issued between the FBCA and the Applicant PKI.
2. The FPKIMA schedules an initial meeting with the Applicant to discuss the technical interoperability process. The following occurs at this initial meeting.
   a. The FPKIMA provides information on the technical configuration of the Trust Infrastructure portion of CITE, and provides the Applicant with a copy of [FPKI CITE],
   b. The Applicant provides the FPKIMA with information on the technical configuration of the Applicant PKI to permit it and the CITE to interoperate at a technical level.
3. Having shared their respective technical data, the Applicant and the FPKIMA undertake a test cross-certification between their respective test-bed environments. The FPKIMA reviews the certificates provided against [FPKI Profile] and [PIV-I Profile] for conformance.
4. Upon completion of the interoperability testing, the FPKIMA prepares a [Technical Analysis Report] identifying any concerns from the documentation review, a description of any deficiencies identified during the test, the anticipated consequences of the deficiencies, and a recommendation for acceptance or rejection.
5. If the FPKIMA identifies significant deficiencies in the [Technical Analysis Report], the FPKIMA requests a FPKIPA discussion and vote. If no significant discrepancies are reported, the FPKIPA is notified of the completion of the technical review step.
6. If a vote has been requested, the FPKIPA reviews the [Technical Analysis Report] and votes whether to accept or reject the FPKIMA [Technical Analysis Report] recommendation. A record of the discussion and vote are kept in the Minutes of the FPKIPA meeting. If the decision is to accept, the FPKIPA Chair provides the [Technical Analysis Report] to the FPKIMA for archival. If the decision is to reject,
   – The FPKIPA Chair notifies the Applicant POC in writing of the decision, providing the reasons why the request for cross-certification has been rejected and the Applicant's recourse.
   – No further cross-certification steps will be completed unless the Applicant satisfactorily resolves the identified issues.
7. If the Applicant is seeking cross-certification as a PIV-I Issuer, the Applicant provides a test Card to the ICAM Lab to perform PIV-I Card testing described in [PIV-I Test Plan]. This activity is only required for Applicants wishing to cross-certify as a PIV-I issuer.

   PIV-I Applicants must demonstrate that PIV-I Cards they issue at a minimum conform to all the requirements of the [PIV-I Test Plan]. Testing is done by the ICAM Lab. PIV-I Card testing requires a cross-certification with the test FBCA in CITE and a PIV-I Card. There are three (3) categories of PIV-I Card testing (details can be found in the [PIV-I Test Plan]):

   - PIV-I Card validation;

- PIV-I Data Model Validation; and
- PIV-I Application Interoperability Validation.

Activity 7 sub-Activities:

a. The Applicant and FPKIMA exchange cross-certificates in CITE, which include mapping the test OIDs for PIV-I. This activity can be accomplished through the Technical Interoperability Testing activity above.
b. The ICAM Lab schedules an initial meeting with the Applicant to provide the Applicant with requirements for PIV-I Card testing. If the entity intends to include any optional elements such as symmetric keys, key history or retired key management objects, the entity negotiates with the ICAM Lab to include the appropriate tests.
c. The Applicant can use the [PIV-I Test Plan] and test tool to do a self-test in preparation for this step.
d. The Applicant generates a test PIV-I Card and provides it to the ICAM Lab. If the entity intends to include any optional elements such as digital signature and key management certificates, these must be included in the test PIV-I Card.
e. The ICAM Lab conducts the first two sections of the [PIV-I Test Plan].
f. The ICAM Lab schedules and conducts the Interoperability Validation testing with the Applicant. The Applicant must participate in this portion of the testing, as the individual whose biometrics are on the PIV-I Card must be present for some of these tests.
g. Upon completion of the PIV-I Card testing, the ICAM Lab prepares a [PIV-I Card Test Report].
h. If the ICAM Lab identifies significant deficiencies in the [PIV-I Card Test Report], the CPWG may request a FPKIPA discussion and vote. If no significant discrepancies are reported, the FPKIPA is notified of the completion of the analysis of operational parameters step.
i. If a vote has been requested, the FPKIPA reviews the [PIV-I Card Test Report] and votes whether to accept or reject the ICAM Lab recommendation. A record of the discussion and vote are kept in the Minutes of the FPKIPA meeting. If the decision is to accept, the FPKIPA Chair provides the [PIV-I Card Test Report] to the FPKIMA for archival. If the decision is to reject,
    i. The FPKIPA Chair notifies the Applicant POC in writing of the decision, providing the reasons why the request for cross-certification has been rejected and the Applicant's recourse.
    ii. No further cross-certification steps will be completed unless the Applicant satisfactorily resolves the identified issues.

2.7 STEP 7: APPLICATION APPROVAL

The objective of this step is for the FPKIPA to review the results of the previous steps and determine whether to approve the issuance of a cross-certificate to the Applicant PKI. This step is performed after the completion of Steps 3-6, regardless of the order of completion of those steps.

The overall evaluation of the Applicant PKI's comparability and trustworthiness involves an assessment of the information collected during the previous steps, as provided in the following documents.

- [Certificate Policy Mapping Report]
- Auditor Letter of Compliance and [Compliance Review Report]
- [PKI Operational Parameters Analysis Report]
- [Technical Analysis Report]
- For PIV-I Applicants only, a [PIV-I Card Test Report]

The FPKIPA reviews this information and any other concerns or other issues discussed during FPKIPA meetings regarding the application, including the results of any requested interim votes. Once the FPKIPA has completed review and discussions, the FPKIPA votes whether to cross-certify with the Applicant.

Activities

1. The FPKIPA reviews the results from Steps 3-6 as identified in the [Certificate Policy Mapping Report], Auditor Letter of Compliance and [Compliance Review Report], [PKI Operational Parameters Analysis Report], and [Technical Analysis Report] and discusses any remaining issues.
2. If required, the FPKIPA discusses remaining issues with representatives of the Applicant, such as conditions identified in previous requested votes.
3. Following discussion, the FPKIPA votes whether to cross-certify with the Applicant. The documentation provided by the FPKIMA and CPWG and a record of the discussion and vote are kept in the Minutes of the FPKIPA meeting.
   a. If the decision is to accept, the FPKIPA Chair notifies the Applicant by formal letter, providing instructions for completing the cross-certification MOA.
   b. If the decision is to reject,
      – The FPKIPA Chair notifies the Applicant POC in writing of the decision, providing the reasons why the request for cross-certification has been rejected and the Applicant's recourse.
      – No further cross-certification steps will be completed unless the Applicant satisfactorily resolves the identified issues.

2.8 STEP 8: NEGOTIATION OF MEMORANDUM OF AGREEMENT (MOA)

The relationship between the U.S. Federal Government and an organization operating a PKI will be governed by the cross-certification MOA to be signed by a cognizant authority from the Applicant and by the FPKIPA Chair on the recommendation of the FPKIPA. Negotiation will be conducted as stipulated in the [FPKIPA Charter] and "By-Laws and Operational Procedures and Practices of the Federal PKI-Policy Authority" [FPKI Bylaws].

An assessment to determine whether an agreement is in a suitable form cannot be undertaken in the abstract. To facilitate the construction of the MOA, the FPKIPA has provided the "*Template for use by the U.S. Federal PKI Policy Authority for Cross-certifying with U.S. federal agencies*

and other U.S. Federal Entities, with U.S. state and local governments and U.S. private sector Entities, and with Governments of other Nations" [FPKI MOA] that may be used as a starting point for negotiations at the option of the Applicant. If during the application process, the documents used during the mapping process change, or new FPKIPA or Applicant conditions are introduced, those changes must be incorporated into the MOA.

The draft MOA provided by the Applicant is reviewed by the FPKIPA Attorney for suitability and to ensure that required elements, such as the following, are included.

- The obligations accepted by the Applicant are sufficient to maintain membership in the FPKI.
- The obligations imposed on the FPKI and its members are acceptable.
- Any obligations imposed on relying parties of FPKI member PKIs are acceptable.
- Any conditions identified during the application review process have been included.
- Applicant documentation, including the CP and any other documents used to complete the mapping process, are incorporated by reference and the Applicant is obligated to submit notice of any changes to these documents to the FPKIPA.

The FPKIPA Attorney reviews the MOA language and works to achieve agreement with the Applicant. If no issues remain unresolved, the MOA is signed by the FPKIPA Chair and a senior official from the Applicant. Any unresolved issues will be reviewed and decided by the FPKIPA.

Activities

1. The Applicant POC submits a draft MOA to the FPKIPA, who forwards it to the FPKIPA Attorney.
2. The FPKIPA Attorney and Applicant POC negotiate the MOA. The FPKIPA Attorney ensures that all referenced documentation described in the [Certificate Policy Mapping Report] is included in the MOA.
3. If the FPKIPA Attorney identifies issues with the MOA, the following steps are completed.
   - The FPKIPA Attorney convenes a meeting of the FPKIPA member legal subject matter experts to discuss and resolve identified issues.
   - If necessary, the FPKIPA Attorney works with the Applicant POC to resolve issues and update the MOA.
   - The FPKIPA Attorney provides results of the subject matter expert review and the updated MOA to the FPKIPA.
   - The FPKIPA reviews the updated MOA and votes whether to accept or reject the MOA. A record of the discussion and vote are kept in the Minutes of the FPKIPA meeting.
4. If no issues are identified by the FPKIPA or if the FPKIPA votes to accept the updated MOA, the following steps are completed.
   - The FPKIPA Chair signs two (2) originals of the MOA and provides them to the Applicant POC.

- The senior official from the Applicant signs the two (2) originals of the MOA and returns one original to the FPKIPA Chair.

  Note: *These two tasks can be completed in either order – i.e., the Applicant senior official can sign first.*

  Note: *If the Applicant desires more than one original signed MOA, the Applicant POC must inform the FPKIPA and provide additional signed originals.*

- One original is provided to the FPKIMA for archival; any remaining originals are returned to or retained by the Applicant POC.

5. If the FPKIPA votes to reject the updated MOA, the following steps are completed.
   - The FPKIPA Chair notifies the Applicant POC in writing of the decision, providing the reasons why the updated MOA has been rejected and the Applicant's recourse.
   - No further cross-certification steps will be completed unless the Applicant satisfactorily resolves the identified issues.

2.9 STEP 9: CROSS-CERTIFICATION

Once the MOA has been signed by the Applicant and the FPKIPA Chair, the remaining step for cross-certification is to issue the cross-certificates themselves. The FPKIPA provides a [Worksheet] to the Applicant requesting technical and POC information for the cross-certification. Using this information, the FPKIPA Chair issues a Letter of Authorization to the FPKIMA to initiate cross-certification with the Applicant PKI. This Letter of Authorization contains:

- Key personnel including primary and alternate technical and managerial contacts for the Applicant and the FPKI.
- Level(s) of assurance of cross-certificates to be issued.
- Policy OID(s) for inclusion in the cross–certificate.
- Directory information tree for subject names in certificates issued by the Applicant PKI.
- Distinguished Name (DN) of the CA.

This information is used to populate the cross-certificate requests and perform the cross-certification process. Following a satisfactory review of the technical data, the production cross-certificates are issued and posted to the appropriate repositories.

Activities

1. The FPKIPA provides a [Worksheet] to the Applicant requesting technical and POC information for cross-certification.
2. The Applicant returns the completed [Worksheet] to the FPKIPA.
3. The FPKIPA prepares and issues a Letter of Authorization to the FPKIMA to initiate cross-certification with the Applicant PKI.
4. The FPKIMA and the Applicant take the necessary procedural and technical steps to issue the production cross-certificate(s).

5. The FPKIMA verifies the extensions in the cross-certificate issued and the cross-certificate received against the [Worksheet] to verify everything is correct. The FPKIMA also verifies the Subject Key ID is the same as the Subject Key ID provided in the Letter of Authorization.
6. The FPKIMA and Applicant (now an Affiliate) post the cross-certificate(s) to the FPKI and Affiliate PKI Repositories, respectively.
7. The FPKIMA notifies the FPKIPA of the completion of the cross-certification process in the respective production environments.

3 ADDITIONAL REQUIREMENTS FOR CROSS-CERTIFICATION OF BRIDGES

When two PKI Bridges choose to interoperate, special considerations apply, since what are being cross-certified are two domains of trust, not just two or more PKIs. The following section addresses the additional requirements necessary in each step of the cross-certification process to enable trusted interoperability between the FBCA and an Applicant Bridge PKI. These steps are performed in addition to the steps listed in Section 2 and address requirements that are either not applicable to Applicant Bridge PKIs, or are necessary to justify the inherent added risks of Bridge-to-Bridge interoperation. For consistency, all steps are included in this section. Those steps with no additional considerations are so marked.

The FBCA will only enter into two-way cross-certification agreements with external Bridges. If at any point during the application process the Applicant Bridge determines that they are not willing to cross-certify with the FBCA, no further cross-certification steps will be completed.

3.1 STEP 1: APPLICATION SUBMISSION

By its nature, a Bridge CA supports a much larger community than a Principal CA of a non-Bridge PKI. As a result, the initiation step must include collection of additional information such as the intended community served by the Applicant Bridge and the methodology that the Applicant Bridge uses to cross-certify applicants.

In evaluating the application of an Applicant Bridge, the FPKIPA must answer the following questions.

- What is the cognizant authority for the Applicant Bridge?
- Who is legally responsible and what are the conflict resolution processes and procedures for the Bridge?
- Under what authority does the Applicant Bridge speak and act on behalf of its membership? Does this authority extend to Bridge-to-Bridge relationships?
- What is the nature of the relationship between member PKIs and the Applicant Bridge (e.g., if a member PKI also operates the Applicant Bridge, or leads the Applicant Bridge Policy Authority, the FPKIPA might be concerned about such a relationship)?
- What is the community served or intended to be served by the Applicant Bridge?

To support this discussion, Applicant Bridges must provide some additional information along with their application package.

Additional Activities:

1. Applicant Bridge submits a formal written application that also includes the following.
   - Sufficient information to allow the FPKIPA to specify the cognizant authority and determine that this authority can speak and act on behalf of the membership of the Applicant Bridge, such as a charter or other governance document.
   - A statement regarding the intended community served by the Applicant Bridge.
2. As part of its application review, the FPKIPA Attorney evaluates the charter of the Applicant Bridge Policy Authority to ensure that it has the authority to speak and act on behalf of its membership.

3.2 STEP 2: DOCUMENTATION SUBMISSION

In performing policy mapping, determining sufficiency of audit compliance, and review of operational parameters, the FPKIPA must determine the following.

- What are the criteria for a PKI to be cross-certified and interoperable with the Applicant Bridge?
- Are sufficient processes in place to ensure that PKIs meet the requirements of the Applicant Bridge CP prior to cross-certifying with the Applicant Bridge?
- How are PKIs evaluated for cross-certification with the Applicant Bridge?
- What technical interoperability testing is performed by the Applicant Bridge to determine suitability of member PKIs.
  1. For Bridges seeking PIV-I policy levels, what equivalent PACS and Card testing is done?
- How does the Applicant Bridge Policy Authority ensure that member PKIs continue to operate in compliance with their agreements with the Applicant Bridge?
- Will the Applicant Bridge place requirements on the FBCA prior to issuing a cross-certificate to it?
- Does the Applicant Bridge CP require compliance audits that meet the standards of the [FBCA CP]; and, has the Applicant Bridge CA satisfied those requirements itself?
- Are the Applicant Bridge operational parameters in consonance with those of the FBCA?

The FPKIPA will only enable a bilateral cross-certification with an Applicant Bridge. As a result, a required part of the application process is ensuring that the FBCA can be cross-certified by the Applicant Bridge without imposing undue requirements on the FBCA. In other words, the [FBCA CP] and this criteria and methodology document must be acceptable to the Applicant Bridge for issuing a cross-certificate to the FBCA.

Additional Activities:

1. The Applicant Bridge submits the following additional documents.
   - Documentation showing the criteria and methodology used by the Applicant Bridge for it to assess its own Applicant Bridge PKIs for membership. This documentation must include its requirements for member PKI demonstration of compliance through compliance audits.

- Documentation showing the methodology for ensuring that member PKIs continue to operate in compliance with their agreements with the Applicant Bridge.
- Documentation showing the procedures for technical interoperability testing done for the Applicant Bridge PKIs members.
- For Applicant Bridges seeking PIV-I policy levels, Documentation showing the procedures for technical interoperability testing done for PIV-I credentials.
- MOA Template or other information indicating the structure of the agreement between the Applicant Bridge and its member PKIs.
- Signed third-party Auditor Letter of Compliance that also includes an indication that the Applicant Bridge has sufficient information on file showing that the Applicant Bridge and its member PKIs are operating in conformance with their CPs and CPSs.
- Applicant Bridge PKI Architecture, including a list of current member PKIs (including Bridges), and directory structure indicating how the Applicant Bridge PKI will interoperate with the FPKI directory; and how Applicant Bridge member CA certificate and CRL information will be made available to FPKI members.

2. The FPKIPA submits the following documents to the Applicant Bridge.
   - The [FBCA CP].
   - The [FBCA CPS].
   - This criteria and methodology document [Crits and Methods].
   - The [FPKIPA Charter]
   - The [FPKI MOA]
   - A compliance audit letter attesting that the FBCA is operating in compliance with the [FBCA CP] and [FBCA CPS] and that audit letters are on file for each FBCA Affiliate PKI that are current and indicate conformance.
   - Description of the FBCA architecture including how the FPKI directory provides CA and CRL information to its member PKIs.
   - Documentation showing the procedures for technical interoperability testing done by the FPKIMA.
   - For Applicant Bridges seeking PIV-I policy levels, the PIV-I testing procedures.

3.3 STEP 3: POLICY MAPPING

When mapping an Applicant Bridge CP, the CPWG will focus on two aspects of the CP:

- Whether the Applicant Bridge CP shows comparable requirements to [FBCA CP] requirements for the Applicant Bridge CA itself; and
- Whether the Applicant Bridge CP shows comparable requirements to [FBCA CP] requirements for member PKIs.

Additional Activity

[Additive to Step 3 Activities 1-3] The CPWG performs the mapping activities focusing on both whether the Applicant Bridge CP is comparable to the [FBCA CP] requirements for the Applicant Bridge CA; and whether the Applicant Bridge CP imposes comparable requirements on its member PKIs.

3.4 STEP 4: COMPLIANCE AUDIT REVIEW

It is important for Bridge governing organizations to know that external Bridge member PKIs are also acting in compliance with their CPs and CPSs. Because audit compliance reports are sensitive, allowing an external Bridge to examine audit reports of Bridge member PKIs is not desirable. Therefore, a statement in the external Bridge's own audit letter that audit letters for each member PKI were on file, current, showing conformance to their CPSs and CPs, is sufficient.

Additional Activity

The CPWG reviews the Applicant Bridge CA Compliance Auditor Letter to ensure that it states that audit letters for each of the Applicant Bridge's member PKIs are on file and that they are current and indicate conformance to their CPSs and CPs.

3.5 STEP 5: ANALYSIS OF OPERATIONAL PARAMETERS

Because Applicant Bridges have their own processes for accepting member PKIs, the analysis of operational parameters is critical for Bridge-to-Bridge cross-certification, and must include, at a minimum, a review of the criteria and methodology the Applicant Bridge uses to process their Applicant Bridge PKIs and a review of the information that the Applicant Bridge requires to be included in the MOA or other governance documentation that it signs with its member PKIs.

Unlike policy mapping, where demonstration of policies, practices, and procedures consistent with each [FBCA CP] requirement is necessary, the review of the criteria and methodology used by the Applicant Bridge need not have a one to one mapping to the criteria and methodology in this document. However, the Applicant Bridge must identify procedures and practices for reviewing its member PKIs that provide a sufficient degree of assurance that its member PKIs demonstrate operation in accordance with the Applicant Bridge CP prior to becoming member PKIs, and that they continue to operate in accordance with their agreements with the Applicant Bridge.

All documentation submitted by the Applicant Bridge to identify its criteria and methodology must be incorporated by reference in the MOA between the Applicant Bridge and the FPKIPA so that any changes to these associated documents will be communicated to the FPKIPA in accordance with the MOA.

Additional Activities

Note: *This is a participatory process. The Applicant Bridge will be required to provide a knowledgeable and authorized representative to the CPWG for the Criteria and Methodology mapping process. This representative shall not be the compliance auditor.*

1. The CPWG and FPKIPA Attorney review the MOA or other document template used by the Applicant Bridge and FBCA to stipulate agreements with member PKIs to ensure that they are sufficiently binding on member PKIs to meet the requirements of the appropriate Bridge CP. The Applicant Bridge does not need to submit all agreements it has signed with its member PKIs; providing an example agreement or a template for the agreement is sufficient.

2. The CPWG reviews the Applicant Bridge criteria and methodology and identifies any divergences.
   - For Applicant Bridges seeking PIV-I policy levels card interoperability testing is also evaluated.
3. The CPWG and Applicant Bridge POC discuss any identified divergences and determine how they may be reconciled.
4. Steps 1-3 are repeated as necessary until the CPWG and Applicant Bridge either determine that all divergences have been addressed or that the FPKIPA or Applicant Bridge governing body are unable or unwilling to address remaining divergences.
5. The CPWG includes the results of the MOA, technical interoperability testing and criteria and methodology review in the [Bridge Operational Parameters Analysis Report].

3.6 STEP 6: TECHNICAL REVIEW AND TESTING

The testing process for an Applicant Bridge is generally equivalent to the testing for an FBCA Applicant Bridge PKI. However, interoperability testing with Applicant Bridges requires ensuring interoperability between FBCA member PKIs and the Applicant Bridge member PKIs.

Additional Activity

The test cross-certification process must also demonstrate the ability of the FBCA to validate cross-certificates issued by the Applicant Bridge to its member PKIs and the CA certificates of member PKIs.

If the Applicant Bridge cross certifies with other CAs that issue PIV-I end-entity certificates, or has subordinate CAs that issue PIV-I end-entity certificates, the Applicant Bridge is responsible for ensuring successful interoperability testing using the [PIV-I Test Plan] before authorizing use of mapped PIV-I policy OIDs. In addition, the Applicant Bridge must agree to invite the FPKIPA to send representative to observe the first PIV-I Card Testing for a PIV-I issuer associated with that Bridge and to notify the FPKIPA whenever they approve a PIV-I issuer.

3.7 STEP 7: APPLICATION APPROVAL

No additional requirements.

3.8 STEP 8: NEGOTIATION OF MEMORANDUM OF AGREEMENT (MOA)

Because the Applicant Bridge may have their own agreement templates, developing the MOA between the FPKIPA and the Applicant Bridge Policy Authority may require additional discussions to include appropriate information from both Bridge templates in the MOA. At a minimum, the criteria and methodology documentation from the Applicant Bridge and the FPKIPA must be added as reference documents to the MOA in addition to any documents used for the policy mapping. The MOA should also address how the cross-certificates will limit and/or manage transitive trust with other cross-certified Bridges. Other wording of the MOA

may be updated to create additional reporting requirements between the two Bridges based on actions taken by either Bridge regarding member PKIs.

Additional Activity

[Replaces Step 8 Activity 1] The FPKIPA and Applicant Bridge Policy Authority develop a draft MOA that:

- Incorporates provisions of the agreement templates from both Bridges.
- Includes this document and the Applicant Bridge criteria and methodology documents by reference in addition to CP documentation.
- Addresses how cross-certificates will limit and/or manage transitive trust with other cross-certified Bridges.
- Outlines required reporting requirements based on actions taken by either Bridge regarding member PKIs.
- Permits the FPKIPA to participate in the Applicant Bridge governance.

3.9 STEP 9: CROSS-CERTIFICATION

For Bridge-to-Bridge cross-certification, it is required that both Bridges issue cross-certificates to each other. There are no additional activities for the issuance of the cross-certificates themselves.

4 MAINTENANCE OF AFFILIATE PKI RELATIONSHIP WITH THE FBCA

It is important to ensure that once in place and for its duration, the cross-certification arrangement continues to guarantee the agreed-upon level(s) of trust between the FBCA and the Affiliate PKI.

The maintenance phase provides mechanisms both for managing the relationship between cross-certified entities as required for the proper operation of the arrangement, and for terminating the arrangement if either party contravenes its terms and conditions, or at the desire of either party. The tasks described in this phase are not sequential and they apply as circumstances warrant.

1. Participation in the FPKIPA as a voting member (if a federal entity) or observer.
2. Submission and review of an annual compliance audit report.
3. Renewal of cross-certificate(s).
4. Update of cross-certificate(s).
5. Update of Affiliate PKI documentation referenced in the MOA.
6. Update of FBCA documentation.
7. Problem resolution.
8. Termination.

4.1 PARTICIPATION IN THE FPKI POLICY AUTHORITY

Active participation in the FPKIPA by Affiliates helps to ensure that decisions made by the FPKIPA benefit the entire FPKI member community. While voting membership in the FPKIPA is restricted to representatives from U.S. federal agencies, all Affiliates are expected to participate in observer status at all FPKIPA meetings and discussions. Participation in FPKIPA meetings will ensure that Affiliates have a voice in proposed changes to the FBCA. All Affiliates are encouraged to participate in FPKIPA working groups, especially those dealing with the development of PKI policies (CPWG) and with technical PKI issues (FPKI Technical Working Group).

Activities:

1. Affiliate identifies one or more POCs to the FPKIPA for inclusion on the FPKIPA mailing list to receive notice of meetings and items up for discussion.
2. Affiliate attends monthly FPKIPA meetings in person, via conference call, or via proxy (for voting members), as specified in [FPKIPA Charter].
3. Affiliate provides feedback on topics presented to the FPKIPA.

4.2 SUBMISSION AND REVIEW OF ANNUAL COMPLIANCE AUDIT REPORT

Independent compliance audits are required of the FBCA and all Affiliate PKIs. Each Affiliate must submit an Auditor Letter of Compliance summarizing the successful completion of the annual compliance audit prepared by the independent auditor. Specific requirements for what the Auditor Letter of Compliance must address are provided in [FBCA Audit Letter]. Affiliates are encouraged to follow the guidance provided in the Triennial Audit Document. The FPKIPA Secretariat will send a compliance audit notification to cross-certified Affiliates not more than 120 days, nor less than 90 days prior to the compliance audit due date. The following table indicates how often compliance audits are required.

Assurance Level	Frequency
FBCA Rudimentary	N/A
FBCA Basic	Once every 2 years
FBCA Medium and above	Once every year[3]

The Annual Compliance Audit Report submitted by Affiliate Bridges must indicate that the Affiliate Bridge has current compliance audit reports on file for its member PKIs.

[3] As an alternative to a full annual compliance audit against the entire CPS, the compliance audit of CAs and RAs may be carried out in accordance with the requirements as specified in the Triennial Audit Document.

Activities:

1. The FPKIPA Secretariat sends a reminder to the Affiliate POC 90-120 days prior to the Affiliate's Annual Auditor Letter of Compliance is due.
2. The Affiliate POC provides the Annual Auditor Letter of Compliance to the FPKIPA no more than two months after the end of the frequency period for the previous Auditor Letter of Compliance.
3. The CPWG reviews the Annual Auditor Letter of Compliance, develops a [Compliance Review Report] recommending whether the letter is satisfactory, and provides the [Compliance Review Report] to the FPKIPA
4. The FPKIPA reviews the Annual Auditor Letter of Compliance and the [Compliance Review Report].
5. The FPKIPA Chair communicates the decision of acceptability of the report to the Affiliate POC.
   - If the report is acceptable, the Chair notifies the Affiliate POC that the report is acceptable and forwards a copy of the report to the FPKIMA.
   - If the report is not acceptable, the Chair notifies the Affiliate POC in writing of the rejection and the reason for rejection, along with a deadline for the Affiliate POC to submit an updated report. Failure of the Affiliate to submit an acceptable audit report within the specified time may be grounds for termination of the MOA and revocation of the cross-certificate. Therefore, issues regarding the audit will be brought to the attention of the FPKIPA for discussion and possible vote.

4.3 RENEWAL OF CROSS-CERTIFICATE(S)

Cross-certificates must be re-issued as a result of normal expiration.

Activities:

1. 90 - 120 days prior to expiration of an existing cross-certificate, the FPKIMA notifies the FPKIPA and the Affiliate that the cross-certificate needs to be re-issued. The notice will contain a summary of all relevant issues and information from various documents, including:
   - The most recent MOA between the FPKIPA and the Affiliate.
   - The most recent [Compliance Review Report]s (the most recent Affiliate Report for review by the FPKIPA Chair, and the most recent FBCA Report for review by the Affiliate).
   - For PIV-I Issuers only, the most recent PIV-I Interoperability Report.
   - All Problem Resolution Reports related to the Affiliate since the cross-certificate was last renewed, if any.
   - All Change Management Reports since the cross-certificate was last renewed tracking the technical changes made to the FBCA that may affect interoperability, if any.
2. The CPWG will review the documentation on behalf of the FPKIPA Chair, and provide a report to the Chair for decision or referral to the full FPKIPA for a vote.

a. If the Chair has no concerns,

    i. The Chair reviews the MOA with the Affiliate and updates the MOA as appropriate (POC information as well as policy OIDs may have changed since the last certificate issuance.)

    ii. The Chair authorizes the FPKIMA in writing to re-issue the cross-certificate.

b. If the Chair does not believe the cross-certificate should be renewed,

- The Chair convenes a meeting of the FPKIMA and CPWG.
- The FPKIMA and CPWG work with the Affiliate and develop a report identifying issues and proposed resolutions and provide this report to the FPKIPA.
- The FPKIPA votes to renew or not renew the cross-certificate. Failure to resolve any open issues may result in termination of the MOA, and the cross-certificate will be allowed to expire, or the FPKIPA may vote to immediately revoke the current cross-certificate.

3. Upon receipt of the authorization, the FPKIMA arranges with the Affiliate to renew the cross-certificate.

4.4 UPDATE OF TECHNICAL ARCHITECTURE OR CROSS-CERTIFICATE(S)

If an Affiliate chooses to update its technical architecture, including its Identity Management Card Management System, updates must be provided to the FPKIPA for a determination if the updated architecture affects the terms of the MOA or the technical interoperability between the FBCA and the Affiliate PKI. Examples of changes to an architecture that must be provided to the FPKIPA include, but are not limited to the addition of new CAs, changes to Affiliate PKI repositories that introduce or eliminate support for different protocols or that might affect interoperability, changes to PIV-I Issuers that would require the Issuers to retest their PIV-I card compatibility.

If the FPKIMA chooses to make significant changes to the FPKI Trust Infrastructure, updates must be provided to the FPKIPA and all Affiliates for a determination as to whether the updated architecture affects the terms of the MOA, or technical interoperability between the FPKI Trust Infrastructure and any Affiliate PKIs.

Updating of cross-certificates may be requested by the CPWG, the FPKIMA, or the Affiliate to modify information contained in the certificate. All requests for modification to cross-certificate profiles are provided to the CPWG for review and approval.

Activities:

1. If an Affiliate desires to modify its technical architecture,

    a. The Affiliate notifies the FPKIPA of the desired modification.

    b. If applicable, the FPKIPA notifies the FPKIMA of the desired change and solicits feedback on the impact of the change to the FBCA relationship.

c. The CPWG reviews the desired changes and any feedback from the FPKIMA, and determines whether the desired technical architecture changes will bring the Affiliate out of compliance with its MOA and/or its cross-certification mapping. In such a case, the CPWG will notify the FPKIPA and the Affiliate of the findings. The CPWG will work with the Affiliate to resolve any issues.

- If a new MOA is required, the Affiliate POC submits a revised MOA to the FPKIPA, who forwards it to the FPKIPA Attorney.
- The FPKIPA Attorney and Applicant POC negotiate the revised MOA. The FPKIPA Attorney ensures that all relevant documentation is included in the MOA. The FPKIPA Chair and a senior official from the Affiliate sign the revised MOA.

d. Failure to resolve any open issues may result in termination of the MOA, and the cross-certificate will be allowed to expire, or the FPKIPA may vote to immediately revoke the current cross-certificate. The FPKIPA will notify the Affiliate of the results of any vote

2. If the FPKI Trust Infrastructure technical architecture is to be modified, the FPKIMA documents the changes in a Change Request. For any significant change that might affect the relationship between the FPKI Trust Infrastructure and Affiliate PKIs, the FPKIMA will provide the Change Request to the FPKIPA and all Affiliates for a determination as to whether the updated architecture affects the terms of the MOA, or technical interoperability between the FPKI Trust Infrastructure and any Affiliate PKIs.
3. If a change to the cross-certificate profile is desired,
   a. The party desiring the change to the certificate notifies the CPWG of the desired change in writing with a justification for the requested change.
   b. The CPWG notifies the FPKIMA and Affiliates of the desired change and solicits feedback of any impacts the desired change will have.
   c. The CPWG reviews the desired change and any feedback received and sends a recommendation to the FPKIPA to approve or reject the proposed certificate profile change.
   d. If the FPKIPA votes to accept the proposed change to the certificate profile, the updated certificate profile is published and sent to the FPKIMA and all Affiliates with a timeline by which implementation is required.
   e. If required, the FPKIMA and Affiliates arrange to update and issue new cross-certificate(s) compliant with the updated certificate profile.

4.5 UPDATE OF AFFILIATE PKI DOCUMENTATION

Affiliates may choose to update their CP or other documentation referenced in their MOA. Since the approval to cross-certify with the FBCA is based on the information contained in this documentation, changes to Affiliate PKI documentation, with the exception of maintaining compliance with changes to the [FBCA CP], require a review by the CPWG and possible acceptance vote by the FPKIPA to ensure that the changes do not affect Affiliate PKI

compliance with [FBCA CP] requirements. This review should take place prior to implementing any changes.

In addition to updates to CP information, Affiliate Bridges must notify the FPKIPA if any of the following changes:

- Affiliate Bridge criteria and methodology or equivalent.
- Affiliate Bridge charter.
- Community served by the Affiliate Bridge.
- Any waivers issued by the Affiliate Bridge to any of its member PKIs.
- Affiliate PKI Technical Interoperability Testing process or document.
- For PIV-I Issuers only, PIV-I Card Interoperability Test process or document.

Activities:

1. The Affiliate provides proposed document changes to the FPKIPA for review and discussion. The Affiliate may choose to provide a draft copy to the FPKIPA for review prior to finalizing the changes, but the Affiliate must still provide the final accepted version of the document to the FPKIPA.
2. The CPWG reviews the proposed document changes and makes a report to the FPKIPA.
3. The FPKIPA Chair communicates the decision to the Affiliate POC.
   a. If the determination is that the changes have no effect on compliance, the Chair notifies the Affiliate POC and provides a copy of the updated documentation to the FPKIMA for archival.
   b. If the determination is that the changes affect the compliance of the Affiliate PKI, the Chair requests a meeting with the Affiliate POC to discuss alternatives for resolution within 30 calendar days. If the Affiliate POC addresses the FPKIPA concerns, no further action is necessary. Failure to resolve any open issues may result in termination of the MOA, and the cross-certificate will be allowed to expire, or the FPKIPA may vote to immediately revoke the current cross-certificate.

4.6 UPDATE OF FPKI DOCUMENTATION

The FPKIPA may deem it necessary to update the [FBCA CP] or other governance documentation (including this document), thereby placing new requirements on Affiliate PKIs. The extent of the impact on the Affiliate PKIs will be determined prior to implementation of the proposed change. Impacts to Affiliate PKIs may result in postponing proposed changes until Affiliate PKIs can come into compliance, a modification to the proposed change, or a decision not to make the proposed change. Failure to resolve any open issues may result in termination of the MOA, and the cross-certificate will be allowed to expire, or the FPKIPA may vote to immediately revoke the current cross-certificate.

Proposed changes to the [FBCA CP] will be provided to Affiliates as new or revised mapping tables. Affiliates will be required to complete the mapping tables indicating compliance actions to be taken and proposed timeframes, or objections to the proposed change.

Activities:

1. The FPKIPA, Affiliates, or Applicants may request changes to the [FBCA CP] or other governance documentation. Changes must be requested in writing and submitted to the FPKIPA following the [CP Change Proposal] template, and should be accompanied with a justification for making the change and the anticipated impact of the change. The impact should be indicated by providing the required delta to the mapping tables,
2. The FPKIPA forwards the change request to the CPWG.
3. The CPWG reviews the change request(s) and makes a recommendation for each request to accept it, accept it with changes, or reject it.
4. The CPWG finalizes the [CP Change Proposal] containing recommended changes. The [CP Change Proposal] is numbered for configuration control, and contains a set of delta mapping tables showing the impact of accepted changes. The CPWG forwards the numbered [CP Change Proposal] to the FPKIPA.
5. The FPKIPA forwards the [CP Change Proposal] to representatives from all Affiliate PKIs along with a response date. Affiliate responses should be sent to both the FPKIPA and CPWG lists. The suggested timeframe is a two week response date to receive information back in time for review at the next CPWG.
6. Each Affiliate must provide a response to the [CP Change Proposal] to the CPWG within 10 days. The response may include suggested modifications or an objection to the [CP Change Proposal]. The Affiliate is encouraged to consider the delta mapping tables to assess:
   a. If the Affiliate PKI documentation currently complies,
   b. If the current Affiliate PKI documentation does not specify compliance but Affiliate PKI practices do comply, the estimated level of effort to bring the documentation into compliance and the time frame required,
   c. If the current Affiliate PKI does not currently comply but would require changes to come into compliance, the estimated level of effort to bring the documentation and practices into compliance and the time frame required,
   d. If the proposed changes would not be applicable to the Affiliate PKI, and would therefore not require changes of the Affiliate,
   e. If the Affiliate PKI is unwilling or unable to comply with the proposed change, intends to vote against it, and understands that if the change is ultimately accepted, their MOA may no longer be compliant and a decision to terminate the cross-certified relationship may be required.

   Each Affiliate is encouraged to send a representative to the CPWG meeting scheduled to review the [CP Change Proposal], and present the Affiliate position in regards to the above bullets. In lieu of a representative, the Affiliate PKI may send a written position to the CPWG in advance of the scheduled meeting.
7. Once the Affiliate responses have been received, the FPKIPA ensures all responses have been sent to the CPWG for review and consideration.
8. The CPWG reviews the responses and updates the [CP Change Proposal] as appropriate.
9. The CPWG provides the updated [CP Change Proposal] to the FPKIPA.

10. The FPKIPA votes to accept, reject, or modify the [CP Change Proposal].
11. The FPKIPA informs all Affiliates of the approved [CP Change Proposal] and the date by which compliance with the change becomes mandatory so that Affiliates can update their documentation and/or practices as needed to remain in compliance with [FBCA CP] requirements.
12. The FPKIPA updates the [FBCA CP] documentation with the approved change, including the implementation date, and publishes the updated CP and mapping tables on the FPKIPA web site. Notification of the publication is sent to all Affiliates.
13. After a [CP Change Proposal]'s implementation date, the Affiliate's next annual audit report will include documentation stating they are compliant. In addition, Affiliates must submit updated full or delta mapping tables, and an updated CP as appropriate.
14. With their next annual audit report, the FPKIPA reviews any Affiliate PKIs that have not provided updated mapping tables demonstrating compliance with the changes, including any that have requested an extension, and makes a determination whether to terminate the Affiliates PKI's MOA and revoke their cross-certificate.

4.7 PROBLEM RESOLUTION

Either party to the cross-certification arrangement may notify the other of problems and request resolution. Problem resolution procedures are specific to the problem encountered and the method of resolution will be agreed upon between the parties.

For technical problems, the Affiliate technical POC will work with the FPKIMA and the FPKI Technical Working Group (TWG) to resolve the issue(s). Any identified technical issues are documented in a monthly Problem Resolution Report.

For situations where the FPKIPA has reason to believe that the FBCA and/or an Affiliate PKI is not operating in compliance with its MOA or CP, the FPKIPA may request the Affiliate to perform an aperiodic audit and provide the resulting compliance audit letter specifically addressing the FPKIPA's concerns. All such requests shall be made for cause, and the cause shall be disclosed at the time of request.

In addition to requesting that an Affiliate Bridge perform an aperiodic compliance audit, the FPKIPA may request that the Affiliate Bridge request performance of an aperiodic compliance audit of one of its member PKIs. All such requests shall be made for cause, and the cause shall be disclosed to the Affiliate Bridge at the time of request.

4.8 TERMINATION

The relationship between the FPKIPA and an Affiliate may be terminated by either party.

In the event the Affiliate initiates termination, the Affiliate POC notifies the FPKIPA in writing of its intent to terminate the MOA, the reason(s) for seeking termination, and the desired termination date.

The FPKIPA initiates termination of the MOA with an Affiliate only for cause. Should the FPKIMA or the FPKIPA become aware that there has been a failure in the integrity of an Affiliate PKI, then the FPKIPA may terminate the MOA and revoke the cross-certificate of the

Affiliate PKI. The FPKIPA informs the Affiliate POC of the termination and revocation and notifies all Affiliate PKIs. Alternatively, and at its sole discretion, the FPKIPA may notify the Affiliate of the issue and provide a resolution date after which the MOA will be terminated if the issue is not resolved. The FPKIPA informs the other Affiliate PKIs of the issue and the timeframe provided for resolution.

5 REFERENCE DOCUMENTS

Reference	Title	URL
Application Template	Application for Cross-certification with the Federal Bridge Certification Authority	http://www.idmanagement.gov/fpkipa/documents/fpkipa_application.doc
Bridge Operational Parameters Analysis Report	Operational parameter review of Applicant Bridge documentation Template	http://www.idmanagement.gov/fpkipa/documents/Operational_Parameters_Review_Template-Applicant_Bridge.doc
Compliance Review Report	Entity Compliance Audit Review Template	http://www.idmanagement.gov/fpkipa/documents/Compliance_Review_Report_Template.doc
CP Change Proposal	FPKI Certificate Policy Change Proposal Template	http://www.idmanagement.gov/fpkipa/documents/FPKI_Certificate_Policy_Change-Proposal_Template.doc
Crits and Methods	Criteria and Methodology For Cross-Certification With the U.S. Federal Bridge Certification Authority (FBCA)	http://www.idmanagement.gov/fpkima/documents/crosscert_method_criteria.pdf
Certificate Policy Mapping Report	Mapping Recommendation for Entity Certificate Policy to the specified Federal Bridge Certification Authority (FBCA) policies Template	http://www.idmanagement.gov/fpkipa/documents/CPWG_mapping_recommendation_template.doc
FBCA Audit Letter	FBCA Compliance Audit Requirements	http://www.idmanagement.gov/fpkipa/documents/audit_guidance.pdf
FBCA CP	X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)	http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf
FBCA CPS	X.509 Certification Practice Statement (CPS) For the Federal Bridge Certification Authority (FBCA)	http://www.idmanagement.gov/fpkipa/documents/FPKIA_CPS.pdf
FBCA Mapping Matrix	Mapping Matrices for the FBCA CP	http://www.idmanagement.gov/fpkipa/documents/FPKI_CertificationApplicantRequirements.docx http://www.cio.gov/fpkipa/drilldown_fpkipa.cfm?action=pa_mappingmatrices
FCPCA CP	X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework	http://www.idmanagement.gov/fpkipa/documents/CommonPolicy.pdf
FICAM Roadmap and Implementation Guidance	Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance	http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf

Reference	Title	URL
FIPS 186	Digital Signature Standard (DSS)	http://csrc.nist.gov/publications/fips/
FPKI Bylaws	By-Laws and Operational Procedures and Practices of the Federal PKI-Policy Authority	http://www.idmanagement.gov/fpkipa/documents/FPKIPAbylaws.pdf
FPKI CITE	Requirements for Test Environment	http://www.idmanagement.gov/fpkima/documents/CITE_Participation_Guide.pdf
FPKI MOA	Template for use by the U.S. Federal PKI Policy Authority for cross-certifying with U.S. federal agencies and other U.S. federal entities, with U.S. state and local governments and U.S. private sector Entities, and with Governments of other Nations	http://www.idmanagement.gov/fpkipa/documents/moa_template.doc
FPKI Profile	Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile	http://www.idmanagement.gov/fpkipa/documents/fpki_certificate_profile.pdf
FPKI Security Controls of NIST SP 800-53	Federal Public Key Infrastructure (FPKI) Security Controls Profile of Special Publication 800-53 Security Controls for PKI Systems	http://www.idmanagement.gov/fpkipa/documents/FPKI_Profile_SP80053_PKI_Security_Controls.pdf
FPKI Security Controls of NIST SP 800-53A	Federal Public Key Infrastructure (FPKI) Security Controls Profile of Special Publication 800-53A	http://www.idmanagement.gov/fpkipa/documents/FPKI_Profile_SP80053A_PKI_Assessment_Guidance.pdf
FPKI TECH	FBCA and C4CA Cross-Certification Technical Guide	http://www.cio.govwww.idmanagement.gov/fpkiafpkima/documents/FBCA_C4CA_TechGuide.pdf
FPKIPA Charter	Federal PKI Policy Authority Charter for Operations	http://www.idmanagement.gov/fpkipa/documents/fpkipa_charter.pdf
PIV-I Card Test Report	Personal Identity Verification Interoperable (PIV-I) Test Report For <Organization Name> Template	http://www.idmanagement.gov/fpkipa/documents/ PIV-I_Test_Report_Template.doc
PIV-I Profile	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards	http://www.idmanagement.gov/fpkipa/documents/pivi_certificate_crl_profile.pdf
PIV-I Test Plan	Personal Identity Verification – Interoperable (PIV-I) Test Plan	www.idmanagement.gov/documents/PIVI_Test_Plan.pdf
PKI Operational Parameters Analysis Report	Operational parameter review of Applicant PKI documentation Template	http://www.idmanagement.gov/fpkipa/documents/Operational_Parameters_Review_Template-Applicant_PKI.doc
RFC 2828	Internet Security Glossary	http://www.ietf.org/rfc/rfc2828.txt
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	http://www.ietf.org/rfc/rfc3647.txt
Technical Analysis Report	Technical Interoperability Report for <Entity> Template	http://www.idmanagement.gov/fpkipa/documents/Technical_Interoperability_Test Report_Template.doc
Triennial Audit Letter	Triennial Compliance Audit Requirements	http://www.idmanagement.gov/fpkipa/documents/TriennialAnnualAuditGuidance.pdf

Reference	Title	URL
Worksheet	Applicant Information for LOA Template	http://www.idmanagement.gov/fpkipa/documents/Applicant_Information_for_LOA_Template.doc

APPENDIX A DOCUMENTATION SUBMISSION CHECKLIST

Policy Documents

- ☐ Certificate Policy (CP) in the IETF RFC 3647, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" [RFC 3647], unless prior approval to submit in other format has been granted.
- ☐ Identification of which of the Applicant's CPs are to be considered for cross-certification at which assurance levels. NOTE: cross-certification at FBCA High assurance level is only authorized for government entity PKIs.
- ☐ *Applicant FPKI Certification Evaluation Requirements* [FBCA Mapping Matrix] document.
- ☐ Principal CA Certification Practice Statement (CPS).
- ☐ Other documentation needed to show evidence of comparability between the Applicant PKI and the requirements in the [FBCA CP].
- ☐ If an alternate CP format is submitted, or if the CP is not sufficient to show comparability to all CP requirements, the Applicant must submit a completed *Applicant FPKI Certification Evaluation Requirements* [FBCA Mapping Matrix] document along with the CP to expedite comparison with the [FBCA CP]. Mapping matrices must be completed for both the General and the appropriate assurance level(s).

Compliance Audit Documents

- ☐ Signed third-party Auditor Letter of Compliance summarizing the results of an audit of the PKI operations that attests to the Applicant's claim that its PKI is operated in accordance with its CPS, and that the CPS implements the requirements of the CP.

Technical Documents

- ☐ Applicant PKI Architecture including a designated Principal CA and a list of subordinate CAs or cross-certified CAs within the PKI.
- ☐ List of CAs that have any other trust relationship with the Applicant PKI Principal CA, such as cross-certifications with other PKIs external to the Applicant PKI and the FPKI.
- ☐ X.500/LDAP directory relationships and hierarchical DN relationships, if any, with other existing Affiliate PKIs (PKIs already cross-certified with the FPKI).
- ☐ Directory structure the Applicant PKI will use to interoperate with the FPKI Trust Infrastructure directory, if applicable, and information about repositories used by the Applicant PKI to support the configuration of certificates issued by the Applicant.
- ☐ Configuration of certificates issued by the Applicant PKI.
- ☐ Capability of Applicant PKI to produce certificates conforming to the "*Federal PKI Certificate Profile*" [FPKI Profile].
    1. For PIV-I policy level Applicants conformance with "X.509 Certificate and Certificate Revocation List Extensions Profile for Personal Identity Verification Interoperable Cards" [PIV-I Profile] is also required.

- ☐ Statement of whether algorithms used by the Principal CA or by any other CA in the Applicant PKI architecture are executed in conformance with the "Digital Signature Standard" [FIPS 186]. If not, specify the standard with which it complies.

Additional Bridge Requirements

The following documents are only required to be submitted by Applicant Bridges.

- ☐ Documentation showing the criteria and methodology used by the Applicant Bridge for it to assess its own Applicant PKIs for membership. This documentation must include its requirements for member PKI demonstration of compliance through compliance audits.
- ☐ Documentation showing the methodology for ensuring that member PKIs continue to operate in compliance with their agreements with the Applicant Bridge.
- ☐ MOA Template or other information indicating the structure of the agreement between the Applicant Bridge and its member PKIs.
- ☐ Signed third-party Auditor Letter of Compliance that also includes an indication that the Applicant Bridge has sufficient information on file showing that its member PKIs are operating in conformance with their CPs and CPSs.
- ☐ Applicant PKI Bridge Architecture, including a list of current member PKIs (including Bridges), and directory structure indicating how the Applicant Bridge PKI will interoperate with the FPKI directory, if applicable, and information about repositories used by the Applicant PKI Bridge to support the configuration of certificates issued by the Applicant Bridge; and how Applicant Bridge member CA certificate and CRL information will be made available to FBCA members.