FBCA: Cross-Certification Evaluation Framework

Version 5.0

September 10, 2024

IMPORTANT NOTES AND CONCEPTS ABOUT THIS DOCUMENT

The Federal Public Key Infrastructure (FPKI) exists for the benefit of the US Federal Government, to facilitate interoperability through authentication, digital signature (integrity and non-repudiation), and encryption (confidentiality). Cross-certification depends on a compelling business case for the US Government. The FPKI will review business cases periodically to ensure that they continue to support their stated purpose. Meeting all pre-conditions and completing all phases does not automatically grant approval or authorization by the US Government for cross-certification.

The FPKI Policy Authority (FPKIPA) recognizes that the cross-certification process is a complex undertaking and will support and guide Applicants as much as possible. Applicants should ensure that they have the necessary resources available to properly navigate the process in a timely and competent manner.

This document provides a general framework for conducting FPKI cross-certification. This framework includes pre-conditions for being considered as an applicant, the cross-certification process, maintenance of the cross-certified status, and circumstances for terminating the cross-certification relationship.

Document Control Grid

Document Owner	Federal Public Key Infrastructure Policy Authority
Contact	fpki@gsa.gov
Document Title	FBCA Cross-Certification Evaluation Framework

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
9/24/15	4.0	Complete document review and restructuring. Renamed from Criteria and Methodology. Streamlined document and moved long activities to appendices. Restructured Phase/Step/Activity concept. Added information to document introduction to ensure document objectives are defined.	John F. McClure, Christine Owen, Matt King, Dave Silver
11/10/15	4.1	Added new bridge requirements related to testing and membership.	Matt King & CPWG
09/10/2024	5.0	Major restructure and update of document. ● Expanded scope from only Bridge applicants to all applicants (except SSPs)	Diana Proud-Madruga, Rob Sherwood, and Max Funk

		● Diagrams ○ Cross-Certification Lifecycle ○ Cross-Certification Process ○ Detailed workflow diagrams for each phase ● Added descriptions of each phase ○ Clarified applicant and Bridge applicant responsibilities. ● Introduced Maintenance and Off Boarding activities ○ Details are in the AR Requirements document [AR Reqs] ● Cleaned up and simplified the Cross-Certification Application Template and added it as an appendix.	

TABLE OF CONTENTS

1 INTRODUCTION

This document identifies the eligibility criteria and defines the methodology for attaining and maintaining cross-certification between the U.S. Federal Government's Federal Bridge Certification Authority (FBCA) and external Public Key Infrastructures (PKIs) or PKI Bridges.

This document refers to PKIs and PKI Bridges seeking cross-certification as "Applicants." If they successfully complete the cross-certification process, they are referred to as "Affiliates."

Adherence to this framework does not automatically grant any Applicant approval for cross-certification.

1.1 BACKGROUND

The Federal Public Key Infrastructure (FPKI) was established by the E-Government Act of 2002. The Federal PKI has grown into a diverse PKI ecosystem of certification authorities (CAs) for U.S. Federal Government, U.S. and foreign government agencies, and U.S. commercial participating PKIs.

The Federal Bridge CA (FBCA) facilitates trust by establishing certificate policy comparability and subsequent technical interoperability between different federal agencies and external Affiliates. The FBCA certificate policy is mapped to participating PKI certificate policies so comparability and trust can be established between the two domains.

The US Federal Government seeks to realize the full benefits of public key cryptography through cross-certification of Applicants. To that end, the FPKIPA has established parameters to prioritize cross-certification activities and allocate resources appropriately.

FBCA Cross-certificates are issued and revoked by the FPKI Management Authority (FPKIMA) at the discretion of the FPKIPA. When the FBCA issues a cross-certificate to a non-federal entity, it does so for the benefit of the U.S. Federal Government.

The FPKIPA will use any information submitted during the application process solely to determine if interoperability is appropriate and beneficial to the U.S. Federal Government.

1.2 DOCUMENT SCOPE

This document provides requirements and procedural guidance for PKI Providers and PKI Bridges seeking cross-certification with the FBCA.

This framework and cross-certification guidelines should be read in conjunction with the Federal Bridge Certification Authority Certificate Policy [FBCA CP].

Certification activities between the Federal Common Policy CA (FCPCA) and PKI Shared Service Provider CAs are out of scope of this document. See the Shared Service Provider Program Guide [SSP Program Guide] for additional information regarding SSP applications.

1.3 INTENDED AUDIENCE

This document is intended for PKI Providers and PKI Bridges who offer products and services that facilitate PKI-based authentication, digital signature, and encryption in support of trusted

digital transactions with the U.S. Federal Government and thus are interested in all aspects of cross-certification with the FBCA.

2 The Cross-Certification Lifecycle

The Cross-Certification Lifecycle depicts the 4 stages needed to achieve and maintain a mutually reliable trust relationship between the FBCA and the Applicant from beginning to end as shown in Figure 1. This lifecycle starts with stage 1 where the applicant demonstrates compliance with all prerequisites necessary to be considered eligible for cross-certification.

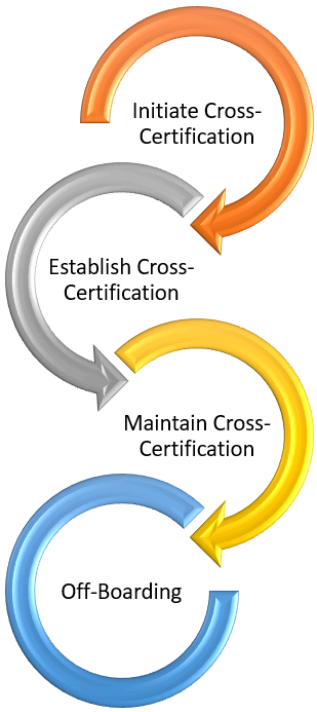

Figure 1 - The Cross-Certification Lifecycle

In stage 2 of the Lifecycle, once eligibility has been demonstrated and approved, the applicant must successfully complete the Cross-Certification process (Figure 2) consisting of four phases. These phases specify required activities undertaken by the FPKIPA, FPKIPA working groups, the FPKIMA, and the Applicant to ensure comparability.

Once cross-certified, an Affiliate moves into stage 3 of the Lifecycle, maintenance. Maintenance activities are designed to demonstrate ongoing compliance with all cross-certification requirements needed to renew a cross-certificate. A full description of maintenance activities and requirements are found in the Annual Review Requirements document.

Stage 4 of the Lifecycle involves discontinuing cross-certification via off-boarding. Off-boarding may be initiated by mutual consent or unilaterally by either party. Some reasons an Affiliate is off-boarded may include but are not limited to: a business decision by the Affiliate to terminate the relationship or a determination by the FPKIPA to revoke the cross-certification due to non-compliance. A full description of off-boarding activities and requirements can be found in the [AR Reqs] document.

3 Lifecycle Stage 1: Initiate Cross-Certification

This is the first "gate" the Applicant must pass to be considered for cross-certification with the FBCA. The Applicant PKI Provider or Bridge must:

1. Inform the FPKIPA of its intention to apply; and
2. Meet pre-conditions that show they are qualified to apply for cross-certification.

3.1 Pre-Conditions Tasks and Activities

The Applicant provides evidence, and the FPKIPA Support Staff verifies if they meet the pre-conditions and then informs the FPKIPA of their findings. Figure 2 shows a high-level workflow for this first step.

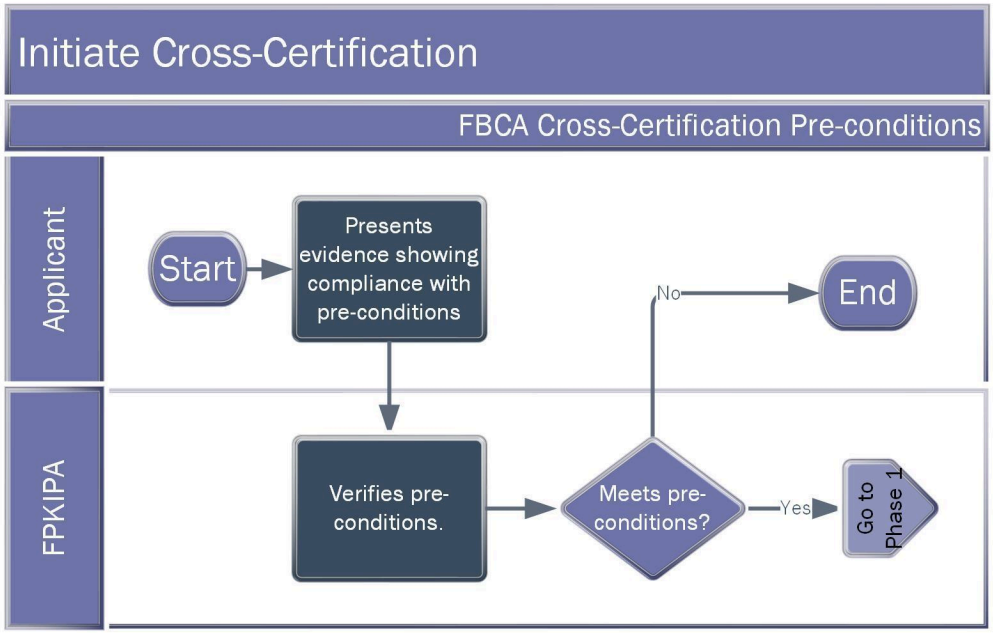

Figure 2 - Lifecycle Stage 1 Workflow

The following activities must be completed for the Pre-Conditions Process:

1. The Applicant initiates the process and sends documentary evidence showing that they met the precondition requirements. This evidence is sent to the FPKIPA Support Staff. This includes, at a minimum:
    a. Identification and proof of eligible applicant type (see 3.2 Applicant Types)
    b. For non-U.S. Government applicants:
        i. Evidence of the corporate status of the entity responsible for the PKI, and its financial capacity to manage the risks associated with operating the PKI.
        ii. A documented business case outlining the benefits and need for cross-certification, and a digitally signed letter from the federal sponsor, including contact information, attesting to the business case (see 3.3 Business Case).
    c. **Applicant Bridges** also must provide their charter or equivalent governance documents.
2. The FPKIPA Support Staff verifies all documentation to determine that the pre-conditions have been met. If the FPKIPA Support Staff determines that the pre-conditions:
    a. Have been met, and the FPKIPA concurs, then the Applicant is given approval to move on to the full application process.
    b. Have NOT been met, and the FPKIPA concurs, then the process ends. The Applicant has the option of modifying and resubmitting supporting documentation for the pre-conditions.

3.2 *Applicant Types*

Before an entity can be considered as an applicant for cross-certification, they must be able to show documented evidence, as verified by the FPKIPA legal counsel, demonstrating they are one of the following applicant types:

- U.S. Government Applicant - A U.S federal,. state, local, or tribal government CA or bridge.
- Non-U.S. Applicant - A non-U.S.-based government CA or bridge.
- External Organization Applicant - An external, private (commercial or non-profit) organization CA or bridge.
  - A Bridge PKI may support a much larger community than a non-Bridge PKI. As a result, the pre-conditions phase must provide information on the intended community served by the Applicant Bridge and the methodology that the Applicant Bridge uses to evaluate and cross-certify prospective members and ensure their ongoing compliance.
  - If the external entity is a bridge, it must have at least two members who are operating independent CAs that are cross-certified to the Applicant Bridge. Applicant Bridges must provide evidence:
    - that member PKIs are separate tax entities from the applicant bridge.
    - that identify members at the time of application and are required to notify the FPKIPA of bridge membership changes throughout the application process and at any time during their affiliation with the FPKI.
    - of the Bridge PKI Charter (or equivalent artifact) describing membership, conflict resolution, authority, and organizational relationships.

  Note: Shared Service Providers[1] are out of scope for this document. See the [SSP Program Guide] Page for additional information in the separate application process for SSPs.

3.3 *Business Case*

- Documentation of the business case includes a description of the benefits for the U.S. Federal Government to cross-certify with the Applicant.
  - This business case needs to be specific enough to allow the FPKIPA Support Staff and FPKIPA to easily determine the value, benefits, and the U.S. Federal Government's need for cross-certification. It should:

[1] Information on the PKI SSP Program can be found at https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/multiple-award-schedule-it/pki-shared-service-providers-program#:~:text=PKI%20Shared%20Service%20Providers%20Program%20includes,and%20cryptographic%20key%20service%20programs.

- Describe the community and estimated size of the user population served by the Applicant.
- What solution (e.g., certificate or credential types) are you offering this community that requires cross-certification?
- List any known or planned U.S. Federal Relying Party Application(s) that will leverage these subject certificates, and indicate what digital transactions (e.g., authentication, digital signature, or encryption) will be facilitated.
- Identify the U.S. Federal Government sponsor and describe the relationship between the Applicant and its sponsor.
- Describe the current operational status/practice of the Applicant PKI. For example:
  - Is this PKI service currently operational?
  - If operational, provide an estimate of the size of the community the Applicant PKI will bring to the FPKI.
  - List Applicant's foreign ties, if any.
  - **Applicant Bridges: If applicable, describe** the nature of the current digital transactions with the U.S. Federal Government.

4 LIFECYCLE STAGE 2: ESTABLISH CROSS-CERTIFICATION

4.1 CROSS-CERTIFICATION PROCESS OVERVIEW

Cross-certifying applicant PKIs with the FBCA is a multi-phase process. This process is designed to achieve a mutually reliable assurance of identities asserted in the resulting PKI subject certificate. This section identifies the required tasks and associated activities for the various parties involved in the process.

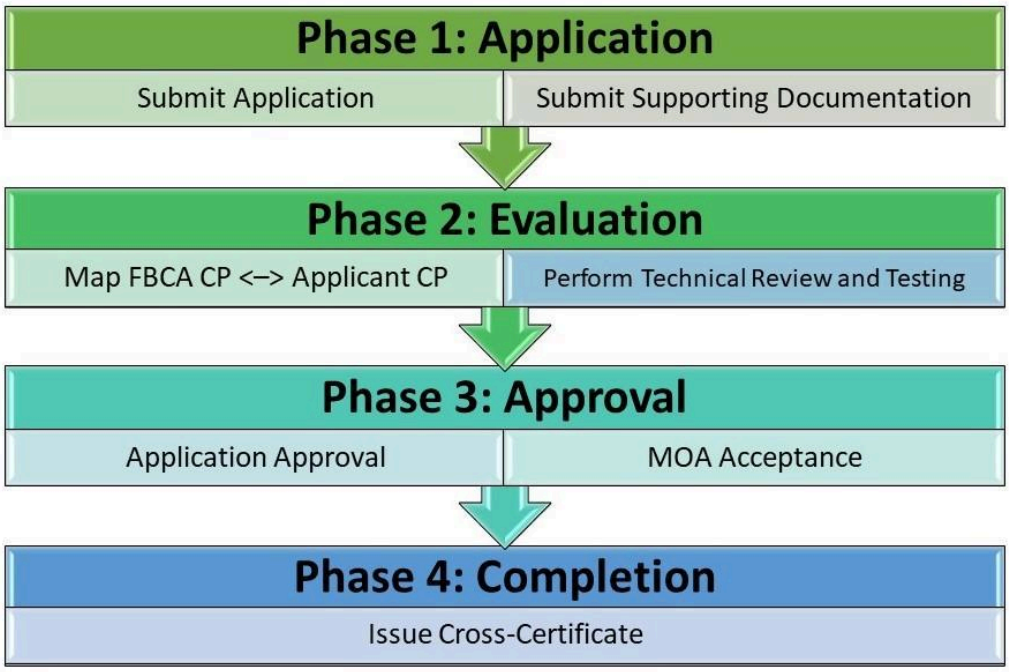

Figure 3 - The Cross-Certification Process

The process consists of four phases, each incorporating one or more tasks as depicted in Figure 3:

- **Phase 1: Application** – These tasks act as a second "gate" where the Applicant completes the rest of the application form and submits supporting artifacts.
- **Phase 2: Evaluation** – In this phase all supporting artifacts, along with a mapping of the Applicant certificate policies to the FBCA certificate policy (FBCACP), is evaluated to ensure comparability with U.S. Federal Government policies, procedures, and systems. The second task in this phase, "perform technical review and testing," demonstrates operational assurance and technical interoperability with FBCA. These tasks are performed iteratively until all issues and concerns are addressed.
- **Phase 3: Approval** – Final approval for cross-certification involves a final review and vote by the FPKIPA. The FPKIPA and Applicant PKI Provider may iterate within the final review to address any noted issues or concerns. An approval by the FPKIPA triggers the creation and execution of a Memorandum of Agreement (MOA).
- **Phase 4: Completion** – The FPKIPA, FPKIMA, and Applicant perform all remaining activities needed to sign and publish the cross-certificate.

4.2 *Phase 1 – Application*

Figure 4 - The Cross-Certification Phase 1 Tasks

Objective: Submit proof of certificate policy and operational comparability with the FBCACP.

This phase consists of two tasks, shown in Figure 4, which may be completed concurrently:

1. The Applicant submits the full cross-certification application.
2. The Applicant submits a complete set of supporting documents and materials that the FPKIPA needs to verify all the information in the application.

Figure 5 shows a high-level workflow for Phase 1.

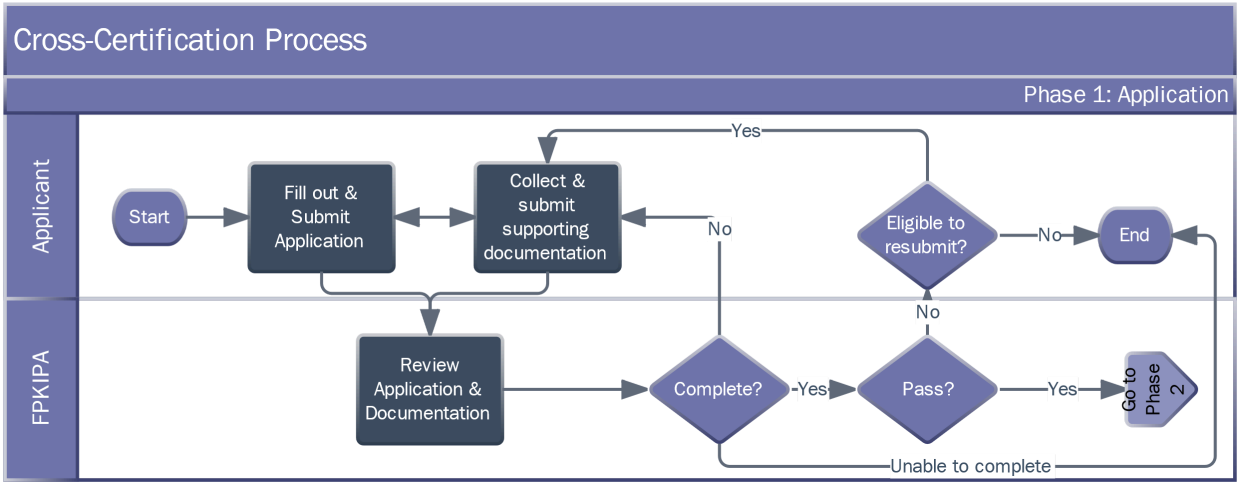

Figure 5 - The Cross-Certification Phase 1 Workflow

After having demonstrated compliance with the pre-conditions and received FPKIPA approval to move forward:

1. The Applicant completes and submits the full application form using the template found in Appendix A.
    a. Applicant **Bridges** MUST ensure that they cover all additional information earmarked for Applicant Bridges in the application.
2. The Applicant collects and submits all required supporting documents listed in Appendix A: Application Template.
    a. All documentation must be submitted electronically to fpki@gsa.gov.
        i. Signed documents should be submitted in PDF format.
    b. Minimum required documentation includes, but is not limited to:
        i. Applicant Certificate Policy (CP),

ii. Applicant PKI Logical Architectural Overview, including protocols and namespace control,
iii. Independent Audit Letters for the Applicant PKI to include auditor methodology, qualifications, and audit results,
1. For additional information on independent third-party compliance audits see section 4.2.2 or for Applicant Bridges section 4.2.3.
iv. All CA certificates issued by the Applicant PKI or cross-certificates issued by the Applicant Bridge,
v. End-Entity Certificate samples for comparable policies to be cross-certified,
vi. Public repository information for the Applicant PKI (e.g., CDP, AIA, SIA, and OCSP URLs).

c. Additional documentation that MAY be requested of the Applicant includes:
i. Applicant Certification Practice Statement (CPS), Registration Practice Statement (RPS), or Key Recovery Policy (KRP),
ii. Certificate templates,
iii. Any Industry or Federal letters of certification for the Applicant PKI infrastructure (e.g., WebTrust, FedRAMP, etc.).

3. FPKIPA Support Staff inventory and initially review the application and documents for completeness.
a. If any documentation is missing or incomplete, FPKIPA Support Staff will provide feedback to the Applicant and the Applicant may choose to submit updated or additional documentation to address feedback.
b. See section 4.2.1 for additional operation parameters required for Bridge Applicants.
4. The above steps may be repeated until FPKIPA Support Staff either determines that the Applicant has provided a complete application or is not able to address the remaining issues.
a. Once the application is completed successfully, the Applicant moves on to Phase 2 – Evaluation.
b. If the Applicant is not able to address outstanding issues, or the FPKI Support Staff determines that the process is taking too long, the process stops.

4.2.1 Additional Operational Parameters for Bridge Applicants

Because Applicant Bridges have their own processes for accepting member PKIs, the analysis of operational parameters is critical for FBCA-to-Bridge cross-certification and must include, at a minimum:

- A review of the methodology the Applicant Bridge uses to process its Applicant PKIs and
- A review of the stipulations that the Applicant Bridge requires to be included in the MOA or other governance documentation that it signs with its member PKIs.

If the applicant organization intends to operate both the Bridge and an issuing CA as a member of the Bridge community, there must be clear evidence in the governance documentation how any potential conflict of interest between these functions is mitigated.

4.2.2 Independent Third-Party Audit

To ensure that the certificate policy (CP) accurately reflects the technical implementation and operational environment of an Applicant PKI, an independent third-party audit is required. The independent third-party auditor must have extensive knowledge of PKI systems and conduct audits as a regular on-going business activity. Specific FPKI qualification requirements for the evaluator/auditor are found in [FBCA CP] Section 8.2, *Identity and Qualifications of Assessor*, and Section 8.3, *Assessor's Relationship to Assessed Entity*.

The Applicant must submit its most recent PKI Compliance Audit Opinion Letter which must include verification of how Applicant practices meet the requirements specified in their own CP and listed in the application (Appendix A). An Applicant may submit multiple audit opinion letters, as needed to ensure all components have been accounted for. The Applicant must provide a written statement that all components of the Applicant PKI or Bridge are covered in the audit opinion letters.

The FPKIPA Support Staff may request additional information, including the practices statements, bona fides of the third-party auditor, or details and mitigation strategies for any findings mentioned in the PKI Compliance Audit Opinion Letter.

Specific requirements for the contents of the Audit Opinion Letter are provided in the FPKI Annual Review Requirements Document [AR Reqs] Audit Opinion Letter Checklist.

4.2.3 Additional Audit Requirements for Bridge Applicants

It is important for Bridge governing organizations to know that external Bridge member PKIs are also acting in compliance with their CPs and CPSs. Therefore, an Applicant Bridge's audit opinion letter must include a statement that current audit opinion letters for each member PKI, which show conformance to their CPSs and CPs, are on file.

A member PKI "Day Zero" audit, where an opinion is rendered on all aspects of the PKI except the subscriber issuance process (if it has yet to be established), may be an acceptable artifact for a member PKI only, not the Bridge Applicant.

4.3 PHASE 2 – EVALUATION

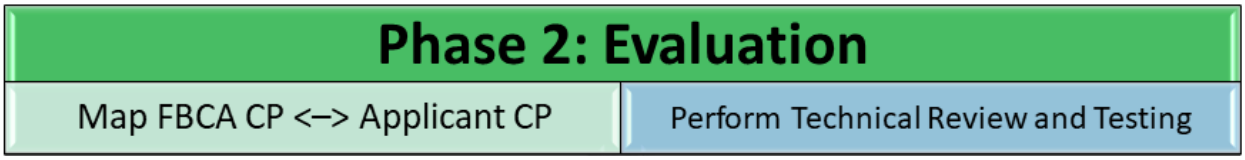

Figure 6 - The Cross-Certification Phase 2 Tasks

Objective: the FPKIPA/FPKIPA Support Staff evaluates the Applicant-supplied information to ensure comparability with U.S. Federal Government policies, procedures, and systems.

This phase consists of two tasks shown in Figure 6. The Applicant:

1. Submits a completed Policy Mapping Matrix that correlates the applicant's certificate policy requirements to FBCA CP requirements to provide a level of assurance for policy comparability.
2. Performs technical reviews and testing to demonstrate technical and operational compatibility with FBCA.

Figure 7 shows a high-level workflow for Phase 2.

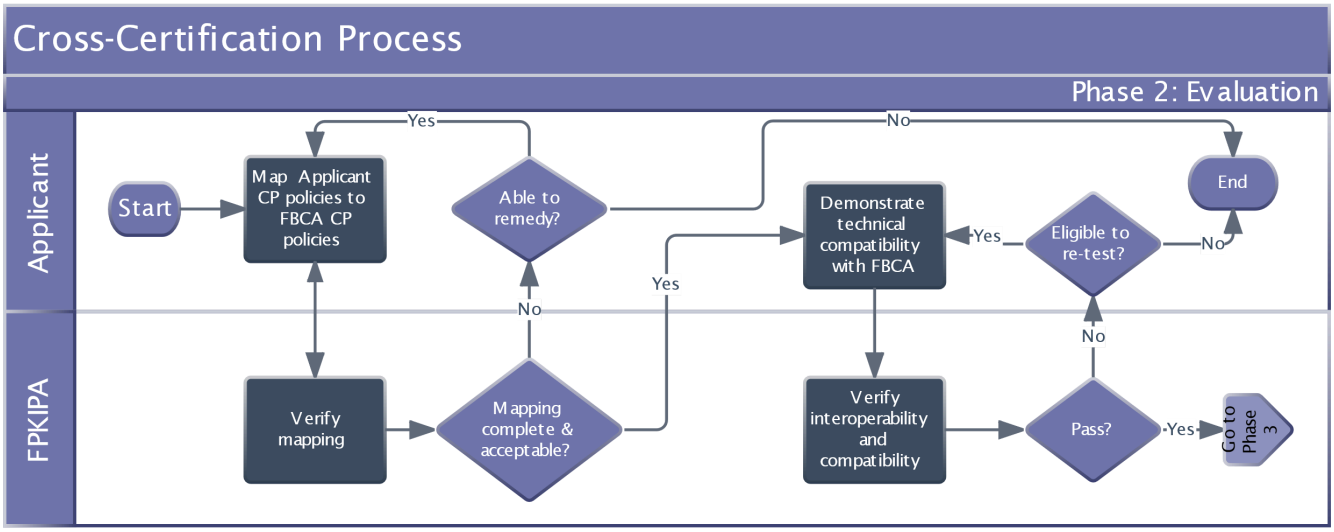

Figure 7 - The Cross-Certification Phase 2 Workflow

4.3.1 Submit and Verify CP Mapping Matrices Task

Policy mapping is the process of comparing the Applicant CP to the FBCACP and evaluating the extent to which the Applicant's documents and policies are comparable to those of the FBCACP. The FPKIPA Support Staff will provide the Applicant with the FBCA Mapping Matrix.

1. The Applicant will map all Applicant certificate policies to the FBCACP and compare/contrast the supporting requirements.
    a. In some cases, PKI 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 is included in any compliance audits and submit, those documents to FPKI.
    b. If the Applicant needs two-way cross-certification, the Applicant will also map the FBCA CP to their CP and determine its comparability.
2. The Applicant submits the completed Mapping Matrix, along with the Applicant's CP, to the FPKIPA Support Staff for review.
3. FPKIPA Support Staff will analyze the Applicant's mapping matrix and their CP. Findings will be discussed with the Applicant. The Applicant may choose to revise their CP to address negative findings. (For Applicant Bridge reviews, see section 4.3.1.1.)

4. Once the initial review is complete, FPKI Support Staff submits the Applicant CP, mapping matrix, and findings for a full CPWG review and FPKIPA approval.
    a. The Applicant is informed of any additional clarifications or requirements needed.
    b. If all requirements are met, the Applicant will move on to the technical review and testing.
    c. If requirements are not met, the FPKIPA will decide if the applicant may re-submit the mapping or terminate the application process.

4.3.1.1 Additional CP Mapping Information for an Applicant Bridge

When reviewing the mapping of an Applicant Bridge CP, the FPKIPA Support Staff will focus on two aspects of the CP:

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

The FBCA Mapping Matrix is written to evaluate CP requirements on an issuing PKI's CP, so these are the comparable requirements that a Bridge Applicant should levy on their members.

A review of the Applicant Bridge CP will also look at the requirements that the Bridge CP levies on itself to ensure these are comparable to the requirements in the FBCACP that dictate FBCA operations.

Unlike policy mapping, the Applicant Bridge must identify governance procedures and audit 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.

4.3.2 Perform Technical Review and Testing Task

The technical testing must demonstrate the ability of the FPKI community to validate certificates issued by CAs associated with the Applicant.

1. The Applicant and the FPKIPA Support Team schedule an initial meeting to discuss the technical interoperability process:
    a. Identify any constraints (e.g., basic constraints, policy constraints, name constraints) to be placed in any cross-certificates issued between the FBCA and Applicant.
    b. Applicants must create a test environment cross-certified with Community Interoperability Test Environment (CITE) to undergo Path Discovery and Validation (PDVAL), repository, and certificate profile conformance verification for test certificates.

i. For operational Applicants, pre-existing certificate interoperability testing will also be planned.

1. It is possible an organization that operates other PKIs, and therefore able to demonstrate technical knowledge of how to operate a PKI, might want to establish a PKI hierarchy that will be strictly for support of some federal government use. In that instance, there would be no point in the Applicant having issued any certificates prior to being accepted and cross-certified with the FBCA.

2. If the Applicant is seeking cross-certification as a PIV-I Issuer, it provides an operational equivalent sample card (using the test certificate path established during CITE testing) and uses the Card Conformance Tool [CCT] to perform a FIPS 201 evaluation of the PIV-I Card as directed by the FPKIPA. See the "PIV-I for Federal Agencies" [PIV-I Guidance] website for additional information on PIV-I use and requirements.

c. See section 4.3.2.1 for additional testing process information for an Applicant Bridge.

2. Upon completion of the interoperability testing, the FPKI identifies any concerns from the testing documentation review, a description of any deficiencies identified during the test, the anticipated consequences of the deficiencies, and a recommendation for acceptance or rejection.

3. In the event of technical review and testing failure, an Applicant can continue through the process three times during the course of a year. If the Applicant fails this task three times or this activity continues for longer than one year, the Applicant may be required to re-apply for cross-certification.

4.3.2.1 Additional Testing Process Information for an Applicant Bridge.

The testing process for an Applicant Bridge is like the testing for an FBCA Applicant PKI. However, interoperability testing with Applicant Bridges must ensure interoperability between other FBCA Affiliates and the Applicant Bridge member PKIs. Therefore, new Applicant Bridges must provide a production end-entity certificate issued by a member of the Applicant Bridge for FPKI Testing. Successful end-entity certificate tests must be completed prior to the FPKI cross-certificate issuance to the Applicant Bridge.

4.4 *PHASE 3 – APPROVAL*

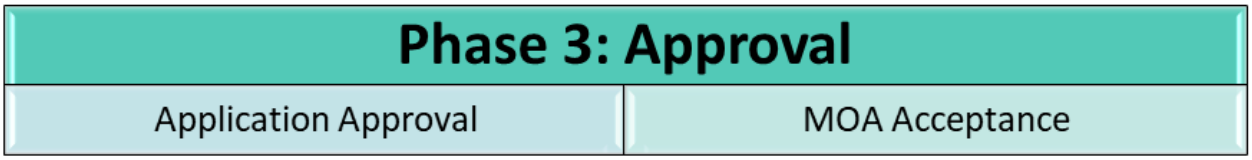

Figure 8 - The Cross-Certification Phase 3 Tasks

Objective: To review the results of the previous steps and determine whether to approve the issuance of a cross-certificate to the Applicant.

This phase consists of two tasks shown in Figure 8:

1. FPKIPA vote for Application Approval
2. MOA Drafting and Execution

Figure 9 shows a high-level workflow for Phase 3.

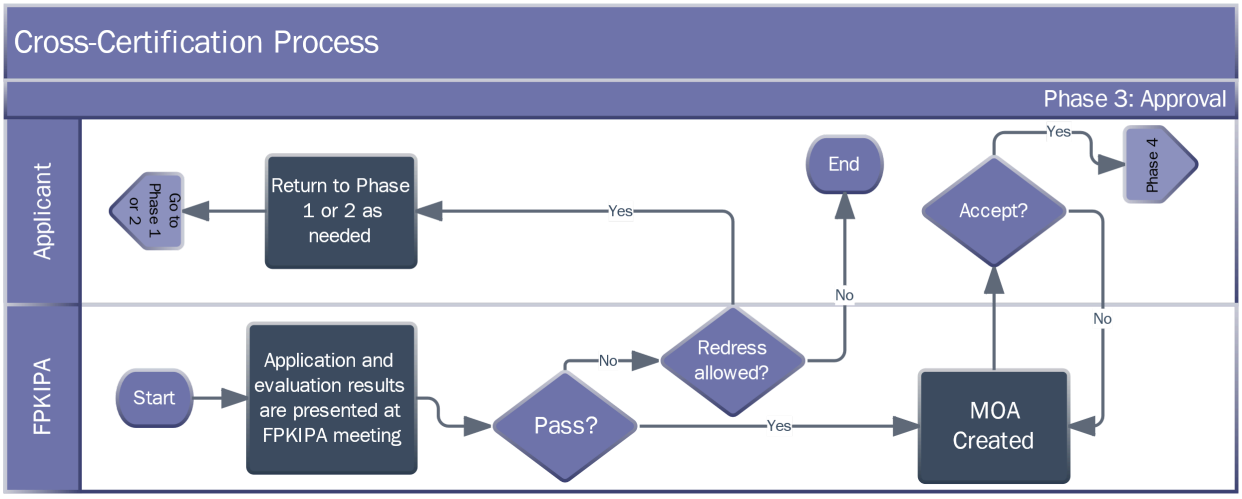

Figure 9 - The Cross-Certification Phase 3 Workflow

1. FPKIPA reviews the FPKIPA Support Staff findings from Phases 1 & 2 and discusses any remaining issues.
    a. If required, the FPKIPA Support Staff reviews remaining issues, including any conditions identified in previous requested votes, with representatives of the Applicant.
    b. FPKIPA Support Staff presents review findings, and all documentation for the Applicant's request to cross-certify, at an FPKIPA meeting.
2. Following the meeting, the FPKIPA votes on whether to cross-certify with the Applicant. The results of the vote are recorded in the minutes of the following FPKIPA meeting.

a. If the decision is to approve cross-certification – the FPKIPA notifies the Applicant in writing, providing instructions for completing the MOA (see section 4.4.1).
b. If the decision is to reject,
    i. The FPKIPA 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 until the Applicant satisfactorily resolves the identified issues.

4.4.1 Acceptance of Memorandum of Agreement (MOA)

The relationship between the U.S. Federal Government and a cross-certified organization is governed by the cross-certification MOA. The MOA is signed by an official authority from the Applicant and by one of the FPKIPA Co-Chairs.

Once the Applicant is approved for cross-certification:

1. The FPKIPA Support Staff updates the standard FPKIPA MOA template with the Applicant specific information and sends it to the Applicant.
2. The Applicant reviews the MOA and makes corrections as needed.
3. Once all information in the MOA is correct and mutually agreed upon, the Applicant digitally (preferred) or manually signs the MOA and sends it back to the FPKIPA Support Staff.
4. The FPKIPA Support Staff coordinates signing with FPKIPA Co-chairs and returns the completed MOA to the Applicant for archival.
5. Once all necessary signatures have been obtained, the process advances to Phase 4, Completion.

4.5 PHASE 4 – COMPLETION

Figure 10 - The Cross-Certification Phase 4 Task

Objective: To successfully issue cross-certificates.

This phase consists of one task shown in Figure 10:

1. Issue Cross-Certificate.

Figure 11 shows a high-level workflow for Phase 4.

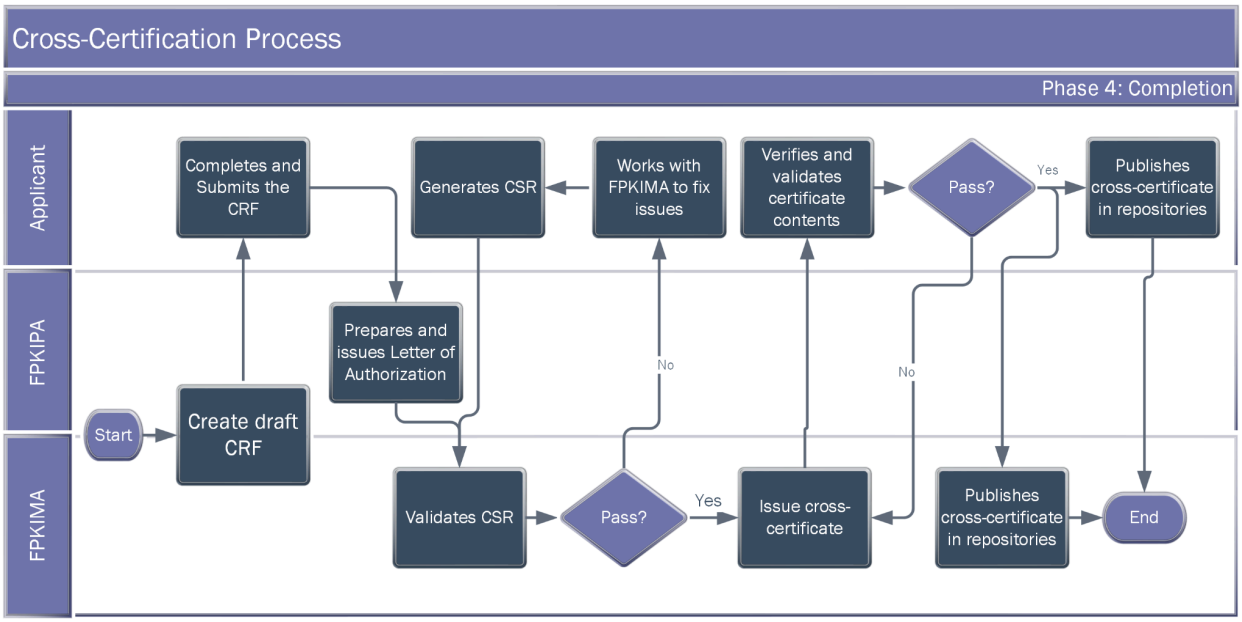

Figure 11 - The Cross-Certification Phase 4 Workflow

1. FPKIPA and FPKIMA Support Staff draft the Certificate Request Form (CRF) for the Applicant.
2. The Applicant completes the CRF, providing any missing technical and POC information, including the proposed contents of the cross-certificate.
    a. If an Applicant Bridge needs two-way cross-certification with FBCA, the Applicant Bridge requests a CRF from the FPKIMA, the following steps are repeated with the roles reversed.
3. The Applicant returns the completed CRF to the FPKIPA Support Staff.
4. The FPKIPA Support Staff prepares and issues a Letter of Authorization (LOA) to the FPKIMA for cross-certificate issuance and attaches the completed CRF.
5. The Applicant follows the directions from the FPKIMA to take the necessary procedural and technical steps for cross-certificate issuance by the FBCA and conducts QA on the resulting cross-certificate(s).
    a. The Applicant generates a Certificate Signing Request (CSR) and sends it to the FPKIMA.
    b. The FPKIMA validates the CSR and issues a certificate.
    c. The FPKIMA sends the certificate to the Applicant.
    d. The Applicant verifies and validates the certificate contents.
6. The FPKIMA and the Applicant (now an Affiliate) post the cross-certificate(s) to their respective repositories.

5 Lifecycle Stage 3: Maintain Cross-Certification

Objective: To ensure that a positive and trusted relationship based on policy and technical comparability and audit compliance is maintained between the FPKI and the Affiliate.

The Maintenance stage provides mechanisms for managing the relationship between the FBCA and its cross-certified Affiliates. A complete description of these maintenance activities can be found in Appendix A of the Annual Review Requirements Document [AR Reqs].

Affiliates are responsible for the following actions to maintain their relationships with the FPKI:

1. For all non-U.S. Federal Government Affiliates:
    a. Maintain relevance to the Federal Community:
        i. Continue to support the FPKIPA approved business cases.
        ii. Affiliate Bridges also need to maintain the minimum required membership as determined by the MOA.
2. Comply with the terms of the MOA:
    a. Provide and update Affiliate points of contact, as needed.
    b. Ensure independent audits are conducted at least annually, with no operational time period unaccounted for.
    c. Notify the FPKI of all changes to the Affiliate policies and operation as agreed in the MOA.
    d. Maintain required governance documents,
    e. Participate in the FPKIPA.
3. Maintain Technical Interoperability:
    a. Communicate updates to the Affiliate's PKI Technical Architecture,
    b. Renew, re-key, or modification of issued cross-certificates or subordinate certificates,
    c. Publish and maintain certificate related artifacts as specified in the certificate policy,
    d. Request renewal of FPKI issued certificates.
4. Comply with the FPKI Annual Review Requirements [AR Reqs].
5. Address any problems or incidents identified by the Affiliate or the FPKIPA.

6 Lifecycle Stage 4: Off-Boarding

The relationship between the FPKIPA and an Affiliate may be terminated by either party, triggering the off-boarding process. A full description of the off-boarding requirements and processes can be found in Appendix D of the Annual Review Requirements Document [AR Reqs].

Appendix A Application Template

Please sign and email an electronic copy of this form to FPKI@gsa.gov.

1. Pre-Conditions

a. Organization Information

Organization Name: _____

Organization Address: _____

_____

_____

b. Applicant Type (check one):

□	U.S. Government CA	□	U.S. Government Bridge
□	Non-U.S. CA	□	Non-U.S. Bridge
□	External Organization CA	□	External Organization Bridge
		Bridge Member #1: _____	
		Bridge Member #2: _____	

c. Applicant Points of Contact (POCs) Information

Provide POC information for the representative authorized to speak on behalf of the organization, the person who will support the cross-certification process, and the person who will address technical issues.

Organization Representative POC		**Cross-Certification Process POC**	
Name:		Name:	
Title:		Title:	
Email:		Email:	
Phone:		Phone:	
Address:	(□ Same as Organization)	Address:	(□ Same as Organization)

Technical POC

Name:	
Title:	
Email:	
Phone:	
Address:	(□ Same as Organization)

d. U.S. Federal Sponsor (not required for U.S. government applicants)

Provide name and contact information of a U.S. federal sponsor. (Note: the business case must be attested to by the U.S. Federal Sponsor in a digitally signed letter.)

Name: _____
Agency: _____
Title: _____
Email: _____
Phone: _____

e. Pre-conditions Supporting Documents/Evidence

Title	*Description*	*Check if done*
Federal Sponsor letter	For non-U.S. Government applicants, a digitally signed letter from the federal sponsor, including contact information, attesting to the business case.	□
Business Case	Documented business case outlining benefit and need for cross-certification	□
Repository Architecture	Documentation describing the Applicant's repository architecture including protocols, and the approach to namespace control.	□
Corporate Status	For non-U.S. Government applicants, evidence of the corporate status of the entity responsible for the PKI, and its financial capacity to manage the risks associated with operating the PKI.	□
Applicant Bridge Charter/Governance documentation	**Applicant Bridges** also must provide their charter or equivalent governance documents .	□

Note: end of pre-condition portion. Submit for initial validation.

2. Full Application

a. Desired Federal PKI Cross-Certification Policies

Check all that apply.

□	FBCA Rudimentary	□	FBCA Medium Commercial Best Practices
□	FBCA Basic	□	FBCA Medium Hardware Commercial Best Practices
□	FBCA Medium	□	PIV-I Hardware
□	FBCA Medium Hardware	□	PIV-I Card Authentication
□	FBCA Medium Device	□	PIV-I Content Signing
□	FBCA Medium Device Hardware		

b. Applicant PKI Policy Documentation

Applicant PKI Information Requested	*Description*	*Check if done*
Applicant Certificate Policy (CP)	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. Include the identification of which of the Applicant's certificate policies are to be considered for cross-certification to which FBCA certificate policies. NOTE: cross-certification at FBCA High assurance level is only authorized for government entity PKIs.	□
(If requested) Certification Practice Statement (CPS)	Participating PKI CA CPS	□

c. Information on the Applicant PKI/Repository Architecture

Architecture Information Requested	*Description*	*Check if done*
Applicant PKI Logical Architectural Overview	Attach a PKI logical architecture diagram depicting the CA(s) within the Applicant's PKI, their trust relationships, including any external cross-certifications, and which CA(s) it wants to be cross-certified with the FBCA. Hierarchical DN relationships, if any, with other existing Participating PKIs (PKIs already cross-certified with the FPKI).	□
CA Certificates	List all CA certificates within the Applicant PKI or cross-certified by the Applicant Bridge	□
End-entity Certificate Samples	End-Entity Certificate samples for cross-certified policies showing the configuration of certificates issued by the Applicant PKI. Describe how certificate subjects will be named and how the Applicant will ensure control of distinguished names	□
.Public Repository Information	Does the Applicant intend to support HTTP URIs for CRLs and CA certificates? Does the Applicant intend to support OCSP? Does the Applicant intend to support any other repository type? If so, please identify.	□
(If requested) Certificate Templates		□
(If requested) Industry or Federal letters of certification	Any Industry or Federal letters of certification for the Applicant PKI infrastructure (e.g., WebTrust, FedRAMP, etc.)	□

d. Audit Information

Applicant Audit Information Requested	***Description***	***Check if done***
Independent Audit Opinion Letters	Recent and signed third-party Auditor Opinion 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. The Audit Opinion Letters must: ● Identify the Auditor. ● Identify the methodology used by the Auditor. ● Identify the time period covered by the audit (this should be no greater than 12 months). ● Identify the time period during which the audit was conducted. ● Identify the PKI components covered by the audit opinion. ● Identify which documents were examined during the audit. ● Include a statement that the Certification Practice Statement (CPS) was evaluated for its conformance to the requirements in the Certificate Policy and identify any discrepancies. ● Include a statement that the PKI operations are in accordance with the CPS and identify any discrepancies.	□

e. **Applicant Bridge Additional Information**

Applicant Bridge Information	*Description*	*Check if done*
Applicant PKI Membership Process	Documentation showing the evaluation methodology used by the Applicant Bridge to assess its own Applicant PKIs for membership. This documentation must include its requirements for member PKI demonstration of compliance through compliance audits.	□
MOA Template for Member PKIs	MOA Template or other information indicating the structure of the agreement between the Applicant Bridge and its member PKIs.	□
Audit Letter	Recent and 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.	□
PKI Bridge Architecture	Applicant PKI Bridge Architecture, including a list of current member PKIs (including Bridges), 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 FPKI members. This is required at the time of application submission.	□
Membership list	Documentation showing a current list of members (at least two), any changes to membership throughout the life of the relationship with the FPKI, and an auditor-affirmed list of members (included with the Annual Audit Letter).	□
Use-case, legal authority, and financial status	Application that includes a use-case to support Federal agencies, the Applicant Bridge's legal authority and financial ability, and the Applicant Bridge's relationship with its member PKIs.	□
Bridge member end-entity certificate sample	Documentation to show the capability of providing a production end-entity certificate issued by a bridge member for FPKI Testing.	□
Bridge member technical interoperability testing	Documentation showing the procedures for technical interoperability testing done for the Applicant Bridge PKIs members.	□
If seeking PIV-I policy levels, PIV-I Interoperability Testing documentation	For Applicant Bridges seeking PIV-I policy levels, documentation showing that the Applicant Bridge requires any applicant to be a PIV-I issuer must pass PIV-I interoperability testing with the FIPS 201 Evaluation Program [FIPS 201] prior to receiving a PIV-I cross-certification.	□

3. Signature

The application must be digitally signed and dated by a senior official (an officer or executive) authorized to speak on behalf of the organization operating the PKI and an authorized representative of the sponsoring agency.

Applicant	**Sponsor**

The above information is true and correct to the best of my knowledge and belief. Name:_____ Title:_____ Signature:_____ Date:_____	I affirm I am an authorized representative of my Agency and agree to Sponsor the applicant listed. Name:_____ Title:_____ Signature:_____ Date:_____

APPENDIX B Definitions

The following terms are used in this guideline. Some definitions have been provided for terms contained in the "Internet Security Glossary" [RFC 4949].

Affiliate: 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 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 4949].

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 4949]. A PKI may adopt more than one CP.

Certificate Policy Working Group (CPWG): A subordinate committee of the FPKIPA that is responsible for reviewing the mapping of the Applicant CPs with the [FBCA CP] and making recommendations regarding the Applicant to the FPKIPA.

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 4949].

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 4949].

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 a CA in one PKI issues a public-key certificate to a CA in another PKI. [RFC 4949].

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 4949].

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 4949].

Federal Bridge Certification Authority (FBCA): The PKI Bridge that enables certificate policy comparability and subsequently technical interoperability between different federal relying parties and Affiliates.

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 4949].

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 4949]. 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 4949].

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

APPENDIX C FPKI Sponsorship Responsibilities

Below are the responsibilities of an agency that is sponsoring an applicant for Cross-Certification with the FPKI.

Federal Sponsor Responsibilities

1. A statement of sponsorship must be from an FPKI Member Agency, in good standing with the FPKI, submitted through its appointed PA representative. Non-Member Federal Organizations may partner with FPKI Member Agencies to obtain sponsorship for their business partners.
2. The statement must be from an organization that will derive significant benefit from the cross-certification (with an assertion of CIO buy-in).
3. The statement must describe a reasonable expectation of benefit for the Government that justifies the effort and the initial and ongoing commitment of resources to establish and maintain the applicant cross-certification.
4. Additional supporting sponsors and statements from the same or other agencies are acceptable and encouraged.
5. The primary sponsor must remain directly involved in the applicant evaluation process.
6. The primary sponsor must reaffirm sponsorship at the conclusion of the evaluation process (prior to PA approval of the cross-certification package).

APPENDIX D References

Reference	Title	URL
AR Reqs	Federal Public Key Infrastructure (FPKI) Annual Review Requirements	https://www.idmanagement.gov/docs/fpki-annual-review-requirements.pdf
CCT	Card Conformance Tool (CCT) and Certificate Profile Conformance Tool (CPCT)	https://www.idmanagement.gov/fpki/#compliance-test-tools-for-annual-reviews
FBCA CP	X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)	https://www.idmanagement.gov/docs/fpki-x509-cert-policy-fbca.pdf
FIPS 201	Personal Identity Verification (PIV) of Federal Employees and Contractors	https://csrc.nist.gov/pubs/fips/201-3/final
PIV-I Guidance	PIV-I for Federal Agencies	https://www.idmanagement.gov/university/pivi/
RFC 4949	Internet Security Glossary	http://www.ietf.org/rfc/rfc4949.txt
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	http://www.ietf.org/rfc/rfc3647.txt
SSP Program Guide	Shared Service Provider Program Guide	https://www.idmanagement.gov/gsapkissp/