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

or

Citizen and Commerce Class Common Certification Authority (C4CA)

Version 2.2 – October 22, 2008

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) or Citizen and Commerce Class Common Certification Authority (C4CA)

Revision History Table

Date	Version	Description	Author
4/10/07	2.0	First Released Version	CPWG
4/14/08	2.01	C4 audit requirements edit	Judith Fincher
4/30/08	2.1	C4 Crits and Methods-edit	Dr. Peter Alterman
10/22/08	2.2	C4 Crits and Methods edit to update dates, references, terminology	Brant Petrick, Judith Fincher, Matt King

TABLE OF CONTENTS

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. Government's Federal Bridge Certification Authority (FBCA) and the Citizen and Commerce Class Common CA (C4CA) by external entity Public Key Infrastructures (PKI) and PKI bridges.

1.2 BACKGROUND

In December 2000, the Federal Chief Information Officer's Council approved the FBCA Certificate Policy. 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 PKI operates in accordance with the standards, guidelines and practices of the Federal PKI Policy Authority (FPKIPA) and of the Federal Identity Credentialing Committee (FICC).

Subsequently, the FPKI Architecture was expanded to include the following Certification Authorities: the Federal PKI Common Policy Framework CA (FCPF), the C4CA, and three e-Governance CAs.

The FCPF CA 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 FCPF Certificate Policy (CP) for the purpose of providing PKI services to Federal Agencies. The FCPF CA is cross certified with the FBCA at medium, medium hardware and high assurance. Information about becoming a PKI Shared Service Provider can be found at http://www.idmanagement.gov/fpkipa/drilldown_fpkipa.cfm?action=ssp.

The e-Governance CAs support the E-Authentication Program Management Office by issuing SSL/TLS server certificates to federated credential service providers. The e-Governance CAs are not cross-certified with any other CA in the FPKI Architecture. Additional information about the e-Governance CAs can be found at http://www.idmanagement.gov/fpkipa.

The C4CA operates at its own unique level of assurance and is not cross-certified with any other CA in the FPKI Architecture. Two kinds of C4 policies exist, one which entitles external entity PKIs to cross-certify with the C4CA for up to six months and one which allows an external entity PKI to cross-certify indefinitely. This document identifies the process for external entity PKIs to cross-certify indefinitely. The C4 CP is extremely lightweight and excellent for entry-level PKIs. Certificates issued by C4CAs are equivalent to E-Authentication Level 2 electronic identity credentials.

Figure 1 below shows a simplified layout of the Federal PKI Architecture.

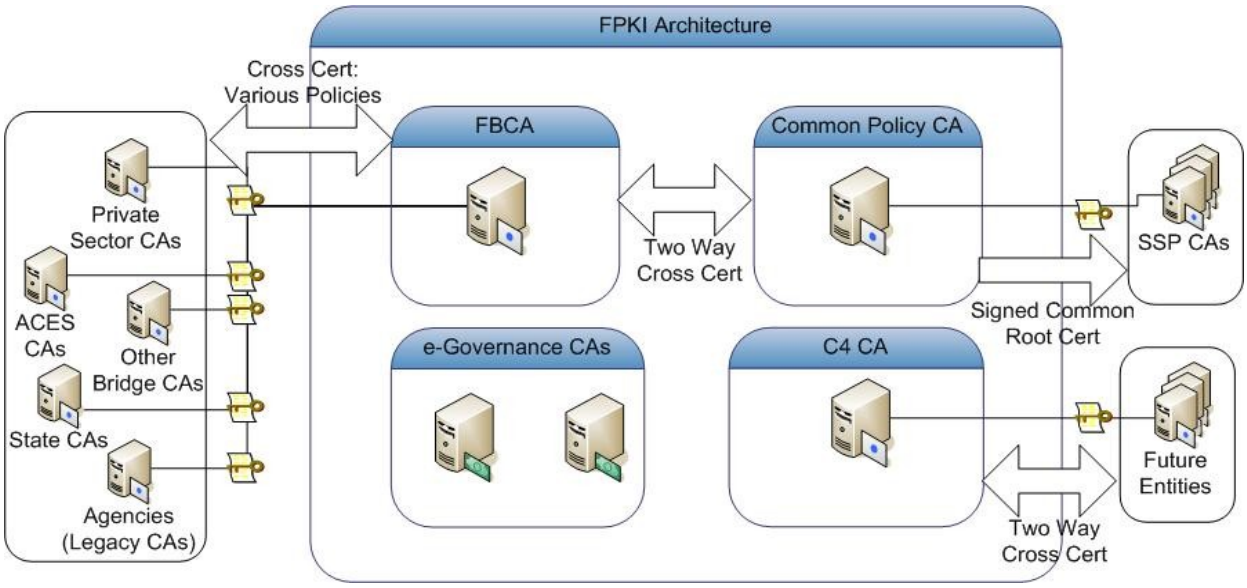

Figure 1: Federal PKI Architecture

1.3 FEDERAL PKI POLICY AUTHORITY

The FPKI Policy Authority (FPKIPA), operating under the authority of the Federal CIO Council, sets policy governing operation of the FBCA, the FCPF CA, the C4CA, and the e-Governance CAs. It also approves applicants for cross-certification with the FBCA and for cross-certification with the C4CA. The "Federal PKI Policy Authority Charter For Operations" [FPKI CHART] identifies the operations of the FPKIPA.

Figure 2 shows the organization of the Federal PKI PA and its working groups.

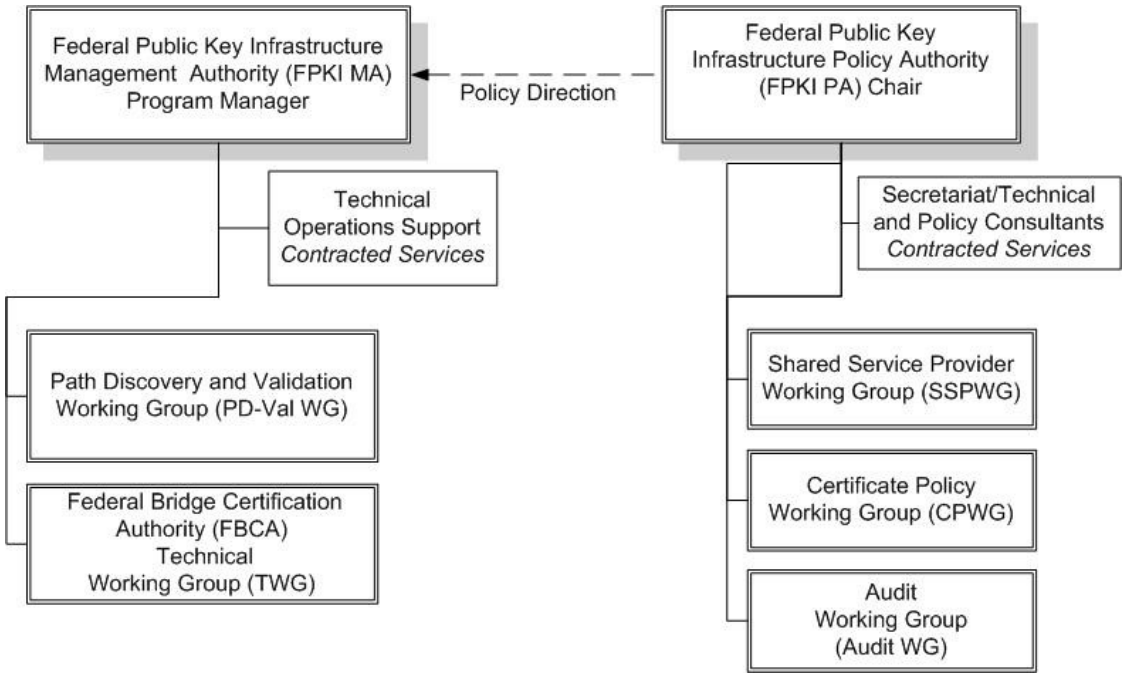

Figure 2: FPKIPA and Working Groups

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 or C4CA and external CAs. Cross certification activities between the Common Policy CA and Shared Service Provider CAs, and activities regarding the e-Governance CAs, 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 "X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)" [FBCA CP] or the "Citizen & Commerce Certificate Policy" [C4CA CP] depending on which CA the entity PKI is interested in cross-certifying with.

Readers can find further detail on the US Government FBCA at http://www.idmanagement.gov/fpkima/. 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 US Government FBCA or C4CA is not a right, nor should any discussions be considered a commitment to issue cross-certificates.*

Cross-certificates issued by the FBCA or C4CA are issued and revoked at the sole discretion of the FPKIPA. When the FBCA or C4CA 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 PKI is for the use of the FPKIPA in determining whether or not interoperability is possible and desirable.

Applicants must determine whether the FBCA or C4CA Certificate Policy (CP) meets the policy and legal requirements for issuing a cross-certificate to the FBCA or C4CA 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 certificate policy is not a substitute for due care and mapping of certificate policies by the applicant.

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

PKIs operated by US Government agency applicants must be certified and accredited in accordance with the requirements of OMB Circular A-130 Appendix III, NIST 800-53 and other relevant Federal IT security policies. PKIs run by non-US Government agency applicants are expected to satisfy equivalent IT security standards[1].

All applicants for cross-certification must obtain unique policy OIDs in the standard ISO object identifier registry from the appropriate commercial or national registration authority. US 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 PKI that has successfully completed all steps required to become cross-certified and has been issued a cross certificate by the FBCA or C4CA.

Applicant PKI: An entity requesting cross-certification with the FBCA or C4CA.

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.

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 Certificate Policy.

Certificate Policy Working Group (CPWG): A subordinate committee of the FPKIPA that is responsible for reviewing the CPs of Applicant PKIs; for performing the policy mapping of the submitted policies to the FBCA policy 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 certificate policy [RFC 2828]

Citizen and Commerce Class Common Certification Authority (C4CA): the U.S. Federal Government's mechanism for enabling trust domain at a level of assurance satisfying E-Authentication Level 2.

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

---

[1] The FPKIPA is drafting a document, which will discuss IT security standard equivalencies for private sector PKIs.

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 3 and 4.

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 or C4CA 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 FPKI MA, and the entity PKI to complete each step. The nine steps are:

- Step 1: Application Submission
- Step 2: Documentation Submission
- Step 3: Policy Mapping
- Step 4: Compliance Audit Review
- Step 5: Analysis of Operational Parameters
- Step 6: Technical Interoperability 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 will vote to accept or reject the application. If the application is accepted, the FPKIPA will request that the Applicant PKI submit the required documentation (Step 2). If the application is rejected, the Applicant PKI will be notified in writing of the decision and provided the reasons why the Application has been rejected. The FPKIPA may offer the Applicant PKI the opportunity to resubmit an amended application depending upon the reasons for initial rejection.

Once documentation has been submitted, the CPWG and FPKI Management Authority (MA) will then complete steps 3, 4, 5, and 6. The CPWG or FPKI MA will 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 denies the application, the Applicant PKI will be notified in writing of the decision and provided the reasons why the Application has been rejected. The Applicant PKI will also be notified of any recourse or other steps that can be taken to address the reason for denial. If the application is accepted, the Applicant PKI and the FPKIPA will negotiate a MOA (Step 8) and cross-certify (Step 9) with the FBCA or C4CA.

Figure 3 illustrates the process for cross certification.

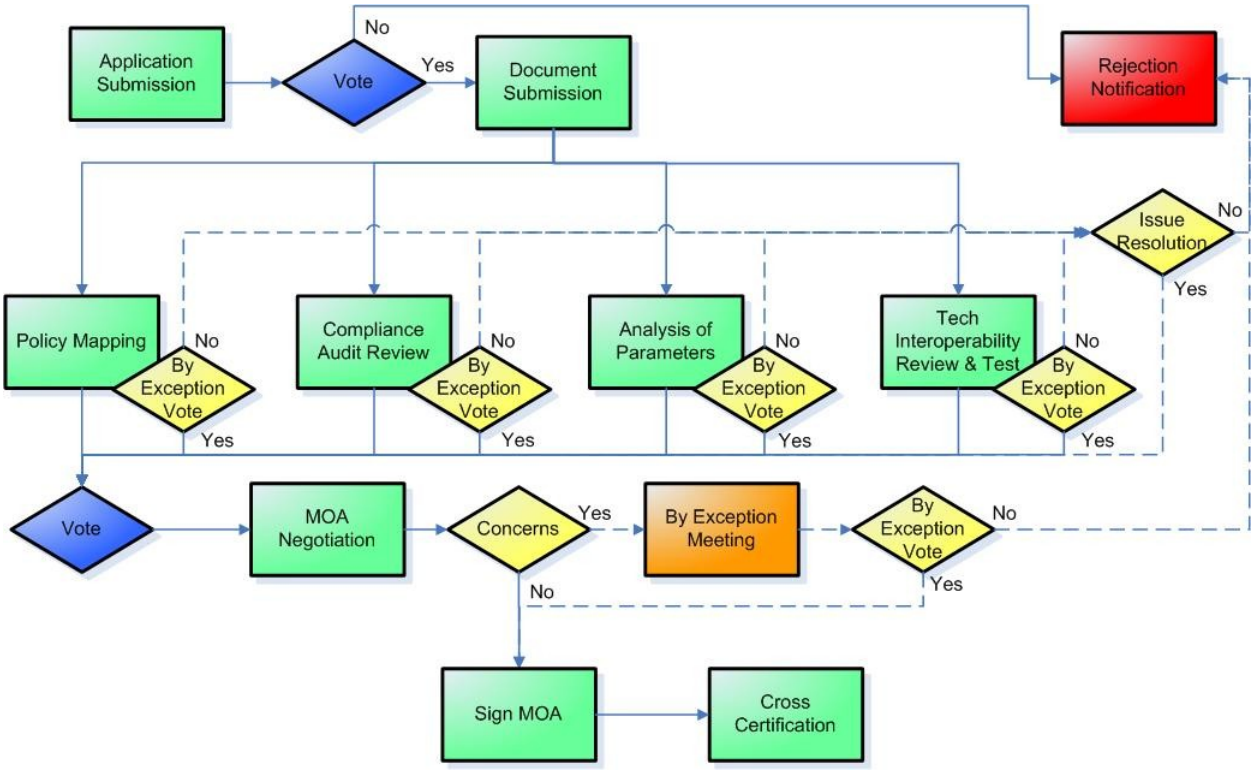

Figure 3: Cross Certification Process

2.1 STEP 1: APPLICATION SUBMISSION

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

To initiate the process of cross certification with the FBCA, an Applicant PKI must submit a formal application to cross certify. The application template is provided in Appendix A. The application must contain the following:

- Name and contact information (email address, phone number and address) for a principal POC and for a secondary POC
- Information on the Applicant's PKI and directory (CA product, PKI architecture, and directory product for repository)
- The proposed FBCA or C4CA 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 PKI 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 PKI.

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

- A US Federal Government entity
- A commercial or non-commercial organization where there are reasonable expectations from a US Federal Government entity that it would benefit from being able to do PKI-based transactions interactions with the applicant entity
- 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 PKI submits a formal written application to cross certify with the FBCA or C4CA to the FPKIPA Chair or Secretariat. Such application will use the format provided in Appendix A to ensure completeness, and be signed by an appropriate senior official of the Applicant organization.
2. The FPKIPA Secretariat schedules a review of the application at the next available FPKIPA Meeting.
3. Where provided, the Federal agency advocate is invited to the FPKIPA meeting where the application will be reviewed.
4. The FPKIPA reviews the application. For non-Government Applicant PKIs, the FPKIPA attorney advises the FPKIPA on the legitimacy and authority of the Applicant PKI organization and representation[2].
5. 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.
6. The FPKIPA Chair communicates the decision to proceed or not to proceed to the Applicant PKI POC and to the FPKIPA members.
   a. If the decision is to proceed,
      - The Applicant is instructed to provide required documentation to the FPKIPA point of contact as identified in Section 2.2, Step 2: Documentation Submission,
      - The FPKIPA Chair authorizes the Co-chairs of the CPWG to initiate mapping of the Applicant PKI's Certificate Policy(ies), review of compliance audit information, and analysis of Applicant PKI CP operational parameters

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

- The FPKIPA Chair authorizes the FPKI Management Authority (MA) to initiate technical review and testing.
- At the behest of Applicant PKI, 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 PKI 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: DOCUMENTATION SUBMISSION

The Applicant PKI must submit 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 http://www.idmanagement.gov/fpkipa/drilldown_fpkipa.cfm?action=fpki_poc. 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 B.

The Applicant PKI must demonstrate that the PKI is operated to a level of assurance comparable to the requirements in the [FBCA CP] or [C4CA 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 MAP] or [C4CA MAP]. Evidence of compliant operation must also be provided through an independent compliance audit performed by a qualified evaluator/auditor. Therefore, Applicant PKIs must submit the following:

- 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 PKI's Certificate Policies 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).
- Other documentation needed to show evidence of comparability between the Applicant PKI and the requirements in the FBCA or C4CA 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 set of mapping matrices along with the CP to expedite comparison with the FBCA or C4CA CP. For FBCA Applicant PKIs, mapping matrices must be completed for both the General and the appropriate assurance level(s). For C4, there is only one matrix. to complete.
- For the FBCA Applicant PKIs, 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 Appendix C. For C4, the signed letter attesting to the above is required, but comes from a cognizant authority within the Applicant PKI, such as a CEO, CIO, etc. No independent third party auditor is required.

Applicant PKIs must demonstrate that their PKI is technically compatible with the FBCA or C4CA. This technical information includes the architecture of the PKI to include the X.500/LDAP directory structure for interoperating with the FBCA or C4CA directory, and the configuration of certificates issued by the Applicant PKI. Applicant PKIs 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.
- 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 Architecture directory.
- 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 PROF]
- 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 PKI submits required documents to the FPKIPA Secretariat.
2. FPKIPA Secretariat forwards policy 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 FPKI MA. These documents are used by the FPKI MA 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 PKI CP to the FBCA or C4CA CP and evaluating the extent to which the applicant PKI demonstrates policies, practices, and procedures consistent with those of the FBCA or C4CA. The categories to be used for FBCA mapping are found in the FBCA general and assurance level specific mapping matrices [FBCA MAP]. The categories to be used for C4 mapping are specified in the C4CA mapping matrix [C4CA MAP]. This policy mapping exercise allows the CPWG to determine if the Applicant PKI CP is comparable to the appropriate CP at the requested level(s) of assurance. In some cases, FBCA or C4CA CP requirements may not be contained in the Applicant PKI CP, but are contained in other documents maintained by the Applicant PKI. In this situation, the

Applicant PKI 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.

When conducting the policy mapping exercise, the CPWG will bear in mind the following.

- There may be more than one section of the Applicant PKI CP that applies for each element in the mapping matrix.
- There may be differences in section headings between the Applicant PKI CP and the FBCA or C4CA CP.
- Some Applicant PKI CPs may have a different number of sub-fields for each element in the FBCA or C4CA CP.
- The Applicant PKI CP may refer to other documents, such as the CPS. If there is insufficient information present in the CP to address CP requirements fully, the referenced documents will be examined to determine comparability.
- There may be differences in terminology and usage. For example, the term "trusted" may have specific implications to one organization that do not carry over when compared to another organization's CP.

The results of the policy mapping exercise are recorded in the mapping matrix 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 an additional documentation used in the mapping process.

This document only describes the CP mapping process that is performed by the CPWG to determine the appropriate mapping from the FBCA or C4CA assurance levels to the Applicant PKI assurance levels for the cross certificate issued to the Applicant PKI. It is the responsibility of the Applicant PKI to perform a mapping exercise from the Applicant PKI to the FBCA or C4CA to determine the appropriate mapping for the cross certificate issued by the Applicant PKI.

Activities

> **Note:** *This is a participatory process. The Applicant PKI will be required to provide a knowledgeable and authorized representative to the CPWG for the Certificate Policy mapping process.*

1. The CPWG maps the Applicant PKI CP and any associated documentation to the levels of assurance identified by the Applicant PKI in the application, using the relevant mapping matrices. The number of matrices required depends on how many levels of assurance are being mapped. If the Applicant PKI has submitted preliminary mapping matrices, the CPWG may use these matrices, but will independently verify any claims of comparability.
2. The CPWG provides the Applicant PKI POC with the completed mapping matrices identifying any discrepancies.
3. The Applicant PKI addresses identified discrepancies by updating their CP or including additional documents and returns the updated documentation along with annotated mapping

matrices. If additional documentation is offered, the documentation must be referenced in the appropriate sections of the CP.

4. Steps 1-3 may be repeated as necessary until the CPWG either determines that the Applicant PKI has addressed all discrepancies or that the Applicant PKI is not able or willing to address remaining discrepancies.
5. 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, and forwards it to the FPKIPA Chair.
6. 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.
7. 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 FPKI MA for archival.
   b. If the decision is to reject,
      – The FPKIPA Chair notifies the Applicant PKI POC in writing of the decision, providing the reasons why the Application has been rejected and the Applicant PKI's recourse.
      – No further cross certification steps will be completed unless the Applicant PKI 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 SEC review. Specific FBCA qualification requirements for the evaluator/auditor are found in the FBCA X.509 Certificate Policy, Section 8.2, Identify and Qualifications of Assessor, and Section 8.3, Assessor's Relationship to Assessed Entity [FBCA CP]. Specific C4CA qualification requirements are found in the C4CA CP, Section B.8, Compliance Audit and other assessments. [C4CA CP]

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

The Applicant PKI 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 any CA components of the Applicant PKI. Evidence may include additional audit reports for various components of the Applicant PKI such as subordinate CAs and RAs.

For entity C4CAs, no formal third-party compliance audit is required (Section 8 "Compliance audit and other assessments" states *No stipulation*).

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 (except for C4) are provided in Appendix C: Auditor Letter of Compliance. The entity CA for C4 only requires a small sub-set of the audit requirements.

The FPKI MA is required to do a compliance audit of the C4CA and is responsible for the "topics covered by assessment" in Section B.8.4 of the C4CP.

Activities

1. The CPWG reviews the Applicant PKI Principal CA 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 PKI.
   - 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 PKI's Principal CA CPS conforms to the requirements of the Applicant CP.
   - States that the Applicant PKI'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
2. If the Applicant PKI Principal CA Auditor Letter of Compliance is not sufficient, the CPWG provides feedback to the Applicant PKI POC.
3. The Applicant PKI may choose to submit an updated Auditor Letter of Compliance and/or additional information to address CPWG feedback.
4. Steps 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 PKI 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 PKI 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 Certificate Policy Mapping Request and votes whether to accept or reject the recommendation in the Compliance Review Report concerning the adequacy of the Applicant PKI Auditor Letter of Compliance. 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 Auditor Letter of Compliance and the Compliance Review Report to the FPKI MA for archival.
   b. If the decision is to reject,
      - The FPKIPA Chair notifies the Applicant PKI POC in writing of the decision, providing the reasons why the Application has been rejected and the Applicant PKI's recourse.
      - No further cross certification steps will be completed unless the Applicant PKI satisfactorily resolves the identified issues.

2.5 STEP 5: ANALYSIS OF OPERATIONAL PARAMETERS

Applicant PKIs must demonstrate that their operational parameters are consistent with the parameters of the FBCA or C4CA CP and will not have an adverse affect on the FPKIPA or on 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 PKI 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 or C4CA. Although particular attention will be paid to CP Sections 1 and 9, heading sections and areas without specific FBCA or C4CA 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 PKI and request updated documentation addressing the identified concerns. Upon completion of the analysis, the CPWG documents its findings in the Operational Parameters Analysis Report.

Activities

1. The CPWG performs an analysis of the Applicant PKI CP and any other associated documentation provided by 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 or C4CA.

2. The CPWG informs the Applicant PKI of any identified concerns and requests updates to the documentation to address those concerns.
3. Steps 1-2 may be repeated as necessary until the CPWG either determines that the Applicant PKI has addressed all concerns or that the Applicant PKI is not able or willing to address remaining concerns.
4. Upon completion of the operational parameters analysis, the CPWG prepares an Operational Parameters Analysis Report and forwards it to the FPKIPA Chair.
5. If the CPWG identifies significant discrepancies in the 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 Certificate Policy Mapping Request 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 Operational Parameters Analysis Report to the FPKI MA for archival.
    b. If the decision is to reject,
        – The FPKIPA Chair notifies the Applicant PKI POC in writing of the decision, providing the reasons why the Application has been rejected and the Applicant PKI's recourse.
        – No further cross certification steps will be completed unless the Applicant PKI satisfactorily resolves the identified issues.

2.6 STEP 6: TECHNICAL INTEROPERABILITY REVIEW AND TESTING

Applicant PKIs must demonstrate that their PKI is technically compatible with the FBCA or C4CA. Technical compatibility is determined through a review of the technical information submitted by the Applicant PKI and through interoperability testing.

The FPKI MA 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 PROF] and [FIPS 186].

Technical interoperability testing is used to ensure technical interoperability between the FBCA or C4CA and the Applicant PKI. The objective of this phase 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 or C4CA and Applicant PKI products, and to minimize the risk of introducing incompatibilities with Affiliate PKIs.

The FPKI MA operates the Federal PKI Architecture Lab (test-bed), which includes FBCA and C4CA prototype systems on behalf of the US Government. It is configured to be a duplicate of

the Production FPKI architecture. Technical personnel representing the Applicant PKI will be required to work with the FPKI MA to complete the technical interoperability testing.

Interoperability testing is best conducted when both FPKI MA and the Applicant PKI use their test-bed systems. The Applicant PKI 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 the "Requirements for Test Environment" [FPKI REQ]. Any costs incurred by the Applicant PKI resulting from technical interoperability testing will be the responsibility of the Applicant PKI. The Applicant PKI 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 is described in the "FBCA Cross-Certification Technical Guide for Certificate Authority Vendors & Applicants" [FPKI TECH]. At a minimum, the technical interoperability test will demonstrate:

- Network connectivity can be achieved using all required protocols
- The directories of the FBCA or C4CA and the Applicant PKI are interoperable
- The cross-certificate is correctly constructed by the FBCA or C4CA, and exchanged and recognized by the Applicant PKI CA
- The cross-certificate is correctly constructed by the Applicant PKI CA, exchanged with the FBCA or C4CA, and recognized by the FBCA or C4CA
- Upon Applicant PKI request, a test transaction, using a test subscriber of the Applicant PKI, can be successfully validated
- The FBCA or C4CA and the Applicant PKI can share revocation information

The results of the interoperability testing, including a description of any deficiencies identified during the test, are documented in a Technical Analysis Report. 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 FPKI MA. The FPKI MA provides the Technical Analysis Report to the FPKIPA for discussion.

Activities

1. The FPKI MA reviews technical documentation provided by Applicant PKI for FBCA or C4CA compatibility; and to determine if any constraints need to be placed in any cross certificates issued by the FBCA to the Applicant PKI to manage trust with regards to other PKIs the Applicant PKI to whom they may have issued cross certificates.
2. The FPKI MA schedules an initial meeting with the Applicant PKI to discuss the technical interoperability process. The following occurs at this initial meeting.
   a. The FPKI MA provides information on the technical configuration of the FPKI Architecture Lab [FPKI TECH] to the Applicant PKI,

b. The Applicant PKI provides the FPKI MA with information on the technical configuration of the Applicant PKI to permit it and the FPKI Architecture Lab to interoperate at a technical level.

3. Having shared their respective technical data, the Applicant PKI and the FPKI MA undertake a test cross certification between their respective test-bed environments.
4. Upon completion of the interoperability testing, the FPKI MA 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, and forwards it to the FPKIPA Chair
5. If the FPKI MA identifies significant deficiencies in the Technical Analysis Report, the FPKI MA 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 Technical Analysis Report and votes whether to accept or reject the FPKI MA Technical Analysis Report recommendation. 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 Technical Analysis Report to the FPKI MA for archival.

   b. If the decision is to reject,

      – The FPKIPA Chair notifies the Applicant PKI POC in writing of the decision, providing the reasons why the Application has been rejected and the Applicant PKI's recourse.
      – No further cross certification steps will be completed unless the Applicant PKI 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 these 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
- Operational Parameters Analysis Report
- Technical Analysis 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, 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 PKI, 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 FPKI MA 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 PKI POC in writing of the decision, providing the reasons why the Application has been rejected and the Applicant PKI's recourse.
      – No further cross certification steps will be completed unless the Applicant PKI satisfactorily resolves the identified issues.

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

The relationship between the U.S. 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 PKI and by the FPKIPA Chair on the recommendation of the FPKIPA. Negotiation will be conducted as stipulated in the [FPKI CHART] and "By-Laws and Operational Procedures and Practices of the Federal PKI-Policy Authority" [FPKI BYLAW].

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 PKI. Additions such as conditions that have been identified during the application review process or incorporation by reference of additional documentation used to complete the policy mapping so that any changes to these associated documents will be communicated to the FPKIPA in accordance with the MOA must also be included.

The draft MOA provided by the Applicant PKI 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 PKI are sufficient to maintain membership in the FBCA or C4CA
- The obligations imposed on the FBCA or C4CA and its members are acceptable

- Any obligations imposed on relying parties of FBCA or C4CA member PKIs are acceptable
- Any conditions identified during the application review process have been included
- Applicant PKI documentation, including the CP and any other documents used to complete the mapping process, are incorporated by reference and the Applicant PKI is obligated to submit notice of any changes to these documents to the FPKIPA

The FPKIPA Attorney develops a MOA Report that is provided to the FPKIPA for review. If the FPKIPA identifies issues with the MOA based on the MOA Report, a meeting of the FPKIPA members' legal subject matter experts is convened to review proposed MOA text or resolve outstanding issues. Recommendations from this meeting, including any dissenting opinions, will be provided by the FPKIPA Attorney to the FPKIPA, and the FPKIPA will vote on the MOA. If no issues are identified, or if the FPKIPA votes to accept the MOA, the MOA is signed by the FPKIPA Chair and a senior official from the Applicant PKI.

Activities

1. The Applicant PKI POC submits a draft MOA to the FPKIPA, who forwards it to the FPKIPA Attorney.
2. The FPKIPA Attorney and Applicant PKI POC negotiate the MOA. The FPKIPA Attorney ensures that all referenced documentation described in the Policy Mapping Report is included in the MOA.
3. The FPKIPA Attorney develops a MOA Report and submits it to the FPKIPA.
4. The FPKIPA reviews the MOA Report.
5. If the FPKIPA identifies issues with the MOA Report, 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 FPKI Attorney works with the Applicant PKI POC to resolve issues and update the MOA.
   - The FPKI 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.
6. 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 PKI POC.
   - The senior official from the Applicant PKI 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 PKI senior official can sign first.*

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

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

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

2.9 STEP 9: CROSS CERTIFICATION

Once the MOA has been signed by the Applicant PKI 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 FPKI MA 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 PKI and the FPKI
- Identification as to whether the cross-certification is to be performed with the FBCA or C4CA
- 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 directories.

Activities

1. The FPKIPA provides a worksheet to the Applicant PKI requesting technical and POC information for cross certification.
2. The Applicant PKI returns the completed worksheet to the FPKIPA.
3. The FPKIPA prepares and issues a Letter of Authorization to the FPKI MA to initiate cross certification with the Applicant PKI.
4. The FPKI MA and the Applicant PKI take the necessary procedural and technical steps to issue the production cross certificate(s).
5. The FPKI MA and Applicant PKI (now an Affiliate PKI) post the cross certificate(s) to the FPKI and Affiliate PKI directories, respectively.

6. The FPKI MA 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 PKIs, or are necessary to justify the inherent added risks of bridge-to-bridge interoperation. For consistency, all phases and 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 phase 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 Applicant 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 Federal PKIPA 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?
- 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?

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 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 FBCA directory; and how Applicant Bridge member CA certificate and CRL information will be made available to FBCA members.
2. The FPKIPA submits the following documents to the Applicant Bridge.

- The FBCA CP
- The FBCA CPS
- This criteria and methodology document
- The FPKIPA charter
- The FBCA MOA Template
- A compliance audit letter attesting that the FBCA is operating in compliance with the FBCA CP and its 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 FBCA directory provides CA and CRL information to its member PKIs

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. A statement in the external bridge's own audit report that audit reports for each member PKI were on file, current, and showed conformance to their CPSs and CPs, is sufficient

Additional Activity

The CPWG reviews the Applicant Bridge CA Compliance Auditor Report to ensure that it states that audit reports 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 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.*

1. The CPWG and GSA 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.
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 and criteria and methodology review in the Operational Parameters Analysis Report.

3.6 STEP 6: TECHNICAL INTEROPERABILITY REVIEW AND TESTING

The testing process for an Applicant Bridge is generally equivalent as the testing for an Applicant PKI. However, interoperability testing with Applicant Bridges requires ensuring interoperability is possible 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.

3.7 STEP 7: APPLICATION APPROVAL

No additional requirements.

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

Because Applicant Bridges 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 OR C4CA

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 or C4CA 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 following tasks described in this phase are not sequential and they will apply as circumstances warrant.

1. Participation in the FPKIPA as a voting member 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 or C4CA documentation
7. Problem resolution
8. Termination

4.1 PARTICIPATION IN THE FPKI POLICY AUTHORITY

Active participation in the FPKIPA by Affiliate PKIs 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 Affiliate PKIs are expected to participate in observer status at all FPKIPA meetings and discussions. Participation in FPKIPA meetings will ensure that Affiliate PKIs have a voice in proposed changes to the FBCA or C4CA.

Activities:

1. Affiliate PKI 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 PKI attends monthly FPKIPA meetings in person, via conference call, or via proxy (for voting members).
3. Affiliate PKI 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, C4CA, and all Affiliate PKIs. Each Affiliate PKI must submit a Principal CA 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 Appendix C. The following table indicates how often compliance audits are required.

Assurance Level	Frequency
C4CP	Entity CA – No stipulation C4CA – Once per year
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.

Activities:

1. The Affiliate PKI POC provides the Principal CA 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.
2. The CPWG reviews the Auditor Letter of Compliance, develops a Compliance Review Report recommending whether the letter is satisfactory, and provides the Compliance Review Report to the FPKIPA
3. The FPKIPA reviews the Auditor Letter of Compliance and the Compliance Review Report and votes whether the report is satisfactory.
4. The Chair of the FPKIPA communicates the decision of acceptability of the report to the Affiliate PKI POC.
   - If the report is acceptable, the Chair notifies the Affiliate PKI POC that the report is acceptable and forwards a copy of the report to the FPKI MA.
   - If the report is not acceptable, the Chair notifies the Affiliate PKI POC in writing of the rejection and the reason for rejection, along with a deadline for the Affiliate PKI POC to submit an updated report. Failure of the Affiliate PKI to submit an acceptable audit report within the specified time is reason for termination of the MOA and revocation of the cross certificate.

4.3 RENEWAL OF CROSS CERTIFICATE(S)

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

Activities:

1. Thirty days prior to expiration of an existing cross-certificate, the FPKI MA notifies the FPKIPA and the Affiliate PKI 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 Compliance Review Report

[3] Federal agencies may submit signed self assertions of an alternate review in lieu of audit reports if no changes or only minor changes have occurred during the prior year. A full compliance audit is required every third year. Non-federal agency PKIs must perform a full compliance audit every year.

- All Problem Resolution Reports since the cross-certificate was last renewed, if any
- All Change Management Reports since the cross-certificate was last renewed tracking the technical changes operated on the FBCA or C4CA, if any

2. The Chair of the FPKIPA reviews the documentation
   a. If the Chair has no concerns, the Chair authorizes the FPKI MA 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 FPKI MA and CPWG
      – The FPKI MA and CPWG work with the Affiliate PKI and develop a report identifying issues and proposed resolutions and provide this report to the FPKI PA
      – The FPKIPA votes to renew or not renew the cross-certificate. Failure to resolve any open issues will result in termination of the MOA and the cross-certificate will be allowed to expire.
3. Upon receipt of the authorization, the FPKI MA arranges with the Affiliate PKI to renew the cross-certificate.

4.4 UPDATE OF TECHNICAL ARCHITECTURE OR CROSS CERTIFICATE(S)

If an Affiliate PKI chooses to update its technical architecture, 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 or C4CA and the Affiliate PKI.

If the FBCA or C4CA updates its technical architecture, information concerning the changes will be provided to all Affiliate PKIs.

Updating of cross certificates may be requested by the CPWG, the FPKI MA, or the Affiliate PKI 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 PKI desires to modify its technical architecture,
   a. The Affiliate PKI notifies the FPKIPA of the desired modification.
   b. If applicable, the FPKIPA notifies the FPKI MA of the desired change and solicits feedback on the impact of the change to the FBCA or C4CA relationship.
   c. The FPKIPA reviews the desired changes and any feedback from the FPKI MA and votes whether the desired technical architecture changes will bring the Affiliate PKI out of compliance with its MOA.
   d. The FPKIPA notifies the Affiliate PKI of the results of the vote.
   e. If the FPKIPA vote is that the change will bring the Affiliate PKI out of compliance with its MOA, implementation of the modifications by the Affiliate PKI will result in termination of the MOA and revocation of the cross certificate.

2. If the FBCA or C4CA technical architecture is modified, the FPKI MA documents the changes in the quarterly Change Management Report. If any changes affect the relationship between the FBCA or C4CA and Affiliate PKIs, the FPKI MA notifies all affected Affiliate PKIs of the changes.
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.
   b. The CPWG notifies the MA and Affiliate PKI(s) 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 votes to approve or reject the updated certificate profile.
   d. If the updated certificate profile is approved, the FPKI MA and Affiliate PKI(s) arrange to update and issue the cross-certificate(s)

4.5 UPDATE OF AFFILIATE PKI DOCUMENTATION

Affiliate PKIs may choose to update their CP or other documentation referenced in their MOA. Since the approval to cross-certify with the FBCA or C4CA is based on the information contained in this documentation, changes to it require a review by the FPKIPA to ensure that the changes do not affect Affiliate PKI compliance with FBCA or C4CA 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

Activities:

1. The Affiliate PKI provides proposed document changes to the FPKIPA for review and discussion. The Affiliate PKI may choose to provide a draft copy to the FPKIPA for review prior to finalizing the changes, but the Affiliate PKI must still provide the final accepted version of the document to the FPKIPA.
2. The FPKIPA reviews the proposed document changes and makes a determination as to the continued compliance of the Affiliate PKI.
3. The Chair of the FPKIPA communicates the decision to the Affiliate PKI POC.
   a. If the determination is that the changes have no effect on compliance, the Chair notifies the Affiliate PKI POC and provides a copy of the updated documentation to the FPKI MA 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 PKI POC to discuss alternatives for resolution within 30 calendar days. If the Affiliate PKI POC addresses the FPKIPA concerns, no

further action is necessary. Failure to reach agreement will result in termination of the MOA and revocation of the cross certificate.

4.6 UPDATE OF FPKI DOCUMENTATION

The FPKIPA may deem it necessary to update the FBCA CP, C4CA 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 of an Affiliate PKI to implement approved changes to the FBCA CP, C4CA CP, or other governance documents within the specified period is reason for termination of the MOA and revocation of the cross certificate.

Proposed changes to the FBCA CP or C4CA CP will be provided to Affiliate PKIs as new or revised mapping tables. Affiliate PKIs 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, Affiliate PKIs, or Applicant PKIs may request changes to the FBCA CP, C4CA CP, or other governance documentation. Changes must be requested in writing and should be accompanied with a justification for making the change and the anticipated impact of the change.
2. The FPKIPA forwards the change request to the CPWG. The FPKIPA may choose to hold change requests and process multiple change requests concurrently at half-yearly intervals to minimize impact on FBCA or C4CA and Affiliate PKI operations.
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 develops a Change Proposal containing recommended changes. The Change Proposal is numbered for configuration control, and contains a set of mapping tables showing the impact of accepted changes. The CPWG forwards the numbered Change Proposal to the FPKIPA.
5. The FPKIPA forwards the Change Proposal to representatives from all Affiliate PKIs along with a response date.
6. Each Affiliate PKI must provide a response to the Change Proposal. The response addresses the following for each change contained in the Change Proposal:
   - For each proposed change where the Affiliate PKI documentation complies, a completed copy of the revised mapping table with Affiliate PKI CP text referenced.
   - For each proposed change where the Affiliate PKI documentation does not specify compliance but Affiliate PKI practices do comply, a copy of the revised mapping table with an explanation of how the Affiliate PKI practices are compliant, and an indication of the time frame necessary for the Affiliate PKI to bring their documentation into compliance.

- For each proposed change where the Affiliate PKI practices do not comply, a copy of the revised mapping table with an explanation of current Affiliate PKI practices and a statement as to the level of effort required and timeframe for the Affiliate PKI to bring their practices and documentation into compliance. Alternatively, the Affiliate PKI may indicate its unwillingness or inability to comply with the proposed change, with the understanding that if the change is ultimately accepted, the MOA will be terminated and the cross certificate will be revoked.

7. Once the Affiliate PKI responses have been received, the FPKIPA forwards the responses to the CPWG for review and consideration.
8. The CPWG reviews the responses and updates the Change Proposal as appropriate.
9. The CPWG provides the updated Change Proposal to the FPKIPA.
10. The FPKIPA votes to accept, reject, or modify the Change Proposal.
11. The FPKIPA informs all Affiliate PKIs of the approved Change Proposal so that Affiliate PKIs can update their documentation and/or practices as needed to remain in compliance with FBCA or C4CA requirements.
12. When the implementation date for a Change Proposal is reached, the FPKIPA updates the documentation and publishes it. At this point, all Affiliate PKIs must be compliant. Affiliate PKIs that did not demonstrate compliance during the review period must resubmit updated mapping tables showing compliance.
13. The FPKIPA reviews any Affiliate PKIs that have not provided updated mapping tables demonstrating compliance with the changes, and makes a determination whether to terminate the Affiliate 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 PKI technical POC will work with the FPKI MA and the FBCA 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 an Affiliated PKI is not operating in compliance with its MOA or CP, the FPKIPA may request the Affiliate PKI 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 Federal PKI Policy Authority and an Affiliate PKI may be terminated by either party.

In the event the Affiliate PKI initiates termination, the Affiliate PKI 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 Federal PKI Policy Authority will initiate termination of the MOA with an Affiliate PKI only for cause. Should the FPKI MA 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 Affiliated PKI. The FPKIPA will inform the Affiliate PKI POC of the termination and revocation and notify all Affiliate PKIs. Alternatively, and at its sole discretion, the FPKIPA may notify the Affiliate PKI of the issue and provide a resolution date after which the MOA will be terminated if the issue is not resolved. The FPKIPA will inform the other Affiliate PKIs of the issue and the timeframe provided for resolution.

5 REFERENCE DOCUMENTS

Reference	Title	URL
C4CA CP	Citizen & Commerce Certificate Policy	http://www.idmanagement.gov/fpkipa/documents/citizen_commerce_cp.pdf
C4CA MAP	Mapping Matrix for the C4CA CP	http://www.idmanagement.gov/fpkipa/documents/C4CAmatrix.doc
FBCA APP	Application for Cross-Certification with the Federal Bridge Certification Authority	Appendix A. Also posted at: http://www.idmanagement.gov/fpkipa/documents/fpkipa_application.doc
FBCA AUD	FBCA Compliance Audit Requirements	Appendix C. Also posted at: 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 MAP	Mapping Matrices for the FBCA CP	http://www.idmanagement.gov/fpkipa/
FIPS 186	Digital Signature Standard (DSS)	http://csrc.nist.gov/publications/fips/
FPKI BYLAW	By-Laws and Operational Procedures and Practices of the Federal PKI-Policy Authority	http://www.idmanagement.gov/fpkipa/documents/FPKIPAbylaws.pdf
FPKI CHART	Federal PKI Policy Authority Charter for Operations	http://www.idmanagement.gov/fpkipa/documents/fpkipa_charter.pdf
FPKI CRIT	Criteria And Methodology For Cross-Certification With The U.S. Federal Bridge Certification Authority (FBCA) or Citizen And Commerce Class Common Certification Authority (C4CA)	This document is posted at: http://www.idmanagement.gov/fpkima/documents/crosscert_method_criteria.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.pdf
FPKI PROF	Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile	http://www.idmanagement.gov/fpkipa/documents/fpki_certificate_profile.pdf
FPKI REQ	Requirements for Test Environment	TBD
FPKI TECH	FBCA and C4CA Cross-Certification Technical Guide	http://www.idmanagement.gov/fpkima/documents/FBCA_C4CA_TechGuide.pdf
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

Appendix A CROSS CERTIFICATION APPLICATION TEMPLATE

Application for Cross Certification

Please sign and mail the completed application in hardcopy to the Chair of the Federal Public Key Infrastructure Policy Authority[4], and send an electronic copy to fpki.webmaster@gsa.gov.

Organization Information

Organization Name: _____

Organization Address: _____

_____

_____

Contact Information

Please provide name and contact information for a primary and alternate point of contact.

Primary POC	**Alternate POC**
Name: _____	Name: _____
Title: _____	Title: _____
Email: _____	Email: _____
Phone: _____	Phone: _____
Address:	Address:
_____	_____
_____	_____
_____	_____

PKI and Repository Information

Please provide information about your PKI and repository. Note that the PKI must be operational to cross-certify with the FBCA or C4CA. PKI information must include the CA product(s) supported, the design of the PKI (e.g., single CA, hierarchical with a Root, mesh), which CA within the PKI will be designated as the Principal CA for cross-certification, and whether the PKI has issued or has plans to issue cross certificates with any other PKIs. Repository information must include the directory product(s) used.

[4] See http://www.idmanagement.gov/fpkipa/drilldown_fpkipa.cfm?action=fpki_poc for address information for the FPKIPA Chair

Desired Federal PKI Cross Certification Level(s)

Please check all that apply.

	C4CA		FBCA Medium Hardware
	FBCA Rudimentary		FBCA High (for U.S. Federal government entities only)
	FBCA Basic		FBCA Medium Commercial Best Practices
	FBCA Medium		FBCA Medium Hardware Commercial Best Practices

Statement of Mutual Interest (not required for U.S. federal entities or state governments)

- Please provide a brief statement describing why cross certification is in the interest of the Federal Government

U.S. Federal Entity Advocate (if available, not applicable for U.S. federal entities)

Please provide name and contact information of a U.S. federal entity advocate if available. A federal advocate is not required for consideration of the application, but will be contacted if provided to provide additional evidence of mutual interest.

Name: _____

Agency: _____

Title: _____

Email: _____

Phone: _____

Corporate Status (not required for government applicants)

Please provide 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. 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.

Signature

The application must be signed by a senior official (an officer or executive) of the organization operating the PKI.

The above information is true and correct to the best of my knowledge and belief.

Name: _____

Title: _____

Signature: _____

Appendix B 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 PKI's Certificate Policies 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.
- ☐ Principal CA Certification Practice Statement (CPS).
- ☐ Other documentation needed to show evidence of comparability between the Applicant PKI and the requirements in the FBCA or C4CA 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 set of mapping matrices along with the CP to expedite comparison with the FBCA or C4CA CP. For FBCA Applicant PKIs, 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. A template for the contents of this audit letter is provided in Appendix C.

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 Architecture directory.
- ☐ Configuration of certificates issued by the Applicant PKI.
- ☐ Capability of Applicant PKI to produce certificates conforming to the "Federal PKI Certificate Profile" [FPKI PROF]
- ☐ 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.

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 FBCA directory; and how Applicant Bridge member CA certificate and CRL information will be made available to FBCA members.

Appendix C AUDITOR LETTER OF COMPLIANCE

Compliance Audit Requirements

In order to evaluate a compliance audit, the following background information is required.

- Identity of the Auditor and the individuals performing the audit;
- Competence of the Auditor to perform audits;
- Experience of the individuals performing the audit in auditing PKI systems;
- Relationship of the Auditor to the entity that owns the PKI being audited. This relationship must clearly demonstrate the independence of the auditor from the entity operating or managing the PKI.

The following information regarding the audit itself is required.

- The date the audit was performed.
- Whether a particular methodology was used, and if so, what methodology.
- Which documents were reviewed as a part of the audit, including document dates and version numbers.

In addition to this background, the entity should ensure that, as part of the audit, an audit summary is prepared, signed by the auditor, reporting on the following elements after conducting the compliance audit:

- State that the operations of the entity PKI's Principal CA were evaluated for conformance to the requirements of its CPS.
- Report the findings of the evaluation of operational conformance to the Principal CA CPS.
- State that the entity PKI's Principal CA CPS was evaluated for conformance to the entity PKI's CP.
- Report the findings of the evaluation of the Principal CA CPS conformance to the entity PKI CP.
- For PKIs with multiple CAs, state whether audit reports showing compliance were on file for any additional CA components of the entity PKI.
- State that the operations of the Entity PKI's Principal CA were evaluated for conformance to the requirements of all current cross-certification MOAs executed by the Entity PKI with other entities.
- Report the findings of the evaluation of the Principal CA CPS conformance to the requirements of all current cross-certification MOAs executed by the Entity PKI.

As the FBCA CP is neutral as to audit methodology, and does not prefer one methodology over another, any audit approach is acceptable to it provided that these points are addressed.

Audit methodologies that focus on validating specific management assertions (such as WebTrust for Certification Authorities) should include the substance of the following in the management assertions:

1. The Entity-CPS conforms to the requirements of the Entity-CP
2. The Entity-CA is operated in conformance with the requirements of the Entity-CPS;
3. The Entity-CA has maintained effective controls to provide reasonable assurance that:
    - Procedures defined in Section 1 (Introduction) of the Entity-CPS are in place and operational.
    - Procedures defined in Section 2 (Publication and Repository Responsibilities) of the Entity-CPS are in place and operational.
    - Procedures defined in Section 3 (Identification and Authentication) of the Entity-CPS are in place and operational.
    - Procedures defined in Section 4 (Certificate Life Cycle) of the Entity-CPS are in place and operational.
    - Procedures defined in Section 5 (Facility Management and Operations Controls) of the Entity-CPS are in place and operational.
    - Procedures defined in Section 6 (Technical Security Controls) of the Entity-CPS are in place and operational.
    - Procedures defined in Section 7 (Certificate, CARL/CRL and OCSP Profiles Format) of the Entity-CPS are in place and operational.
    - Procedures defined in Section 8 (Compliance Audit and other Assessments) of the Entity-CPS are in place and operational.
    - Procedures defined in Section 9 subsections 9.4.4 (Privacy of Personal Information – Responsibility to Protect Private Information) and 9.6.3 (Representations and Warranties – Subscriber Representations and Warranties) are in place and operational.
4. The Entity-CA is operated in conformance with the requirements of all current cross-certification MOAs executed by the Entity-CA.

Note: *The FBCA does not require and will not consider any statements with respect to the entity PKI's suitability for cross certification with the FBCA or conformance to the FBCA certificate policies. Such a determination is exclusively the purview of the FPKIPA and its working groups.*