Federal Public Key Infrastructure (FPKI) Annual Review Requirements

Version 2.0
September 10, 2024

Revision History

Document Version	Document Date	Revision Details
1.0	April 11, 2017	Initial Release
1.1	September 29, 2021	Minor update to correct annual review submission email address
1.2	May 6, 2022	Document updated to: ● Reorganize related topics ● Remove redundant or out of scope items ● Reorganize and expand Appendices
2.0	September 10, 2023	Added process workflow and audit accountability information. Added maintenance and off-boarding information.

Table of Contents

1. Introduction

The Federal Public Key Infrastructure Policy Authority (FPKIPA) is responsible for maintaining trust throughout the FPKI. Organizations operating a PKI certified or cross-certified by either the Federal Common Policy Certification Authority (FCPCA) or the Federal Bridge Certification Authority (FBCA) are considered an Affiliate participating in the FPKI. In this document, the term "Affiliate" includes Shared Service Providers (SSPs), cross-certified external Bridges (a.k.a. Affiliate Bridges), or other cross-certified PKIs (a.k.a. Affiliate PKIs).

Each year, the FPKIPA reviews its relationship with each Affiliate to ensure the continued integrity and maintenance of the operating environment. This review process requires submission of an Annual Review Package, as outlined in this document.

Affiliates are responsible for performing continuous maintenance on their own PKI operating environments, and/or oversight on their Bridge members throughout the year. The annual review process provides evidence of those maintenance activities. See appendix A for a list of continuous maintenance activities.

1.1. Scope

All Affiliates MUST submit an Annual Review Package to the FPKIPA.

This document describes the requirements, artifacts, and processes an Affiliate must address to meet its FPKI Annual Review obligations.

Other requirements, such as a Shared Service Provider's (SSP) Authority to Operate (ATO) or FedRAMP certification, could be referenced here but are considered out of scope for the Annual Review process and this document.

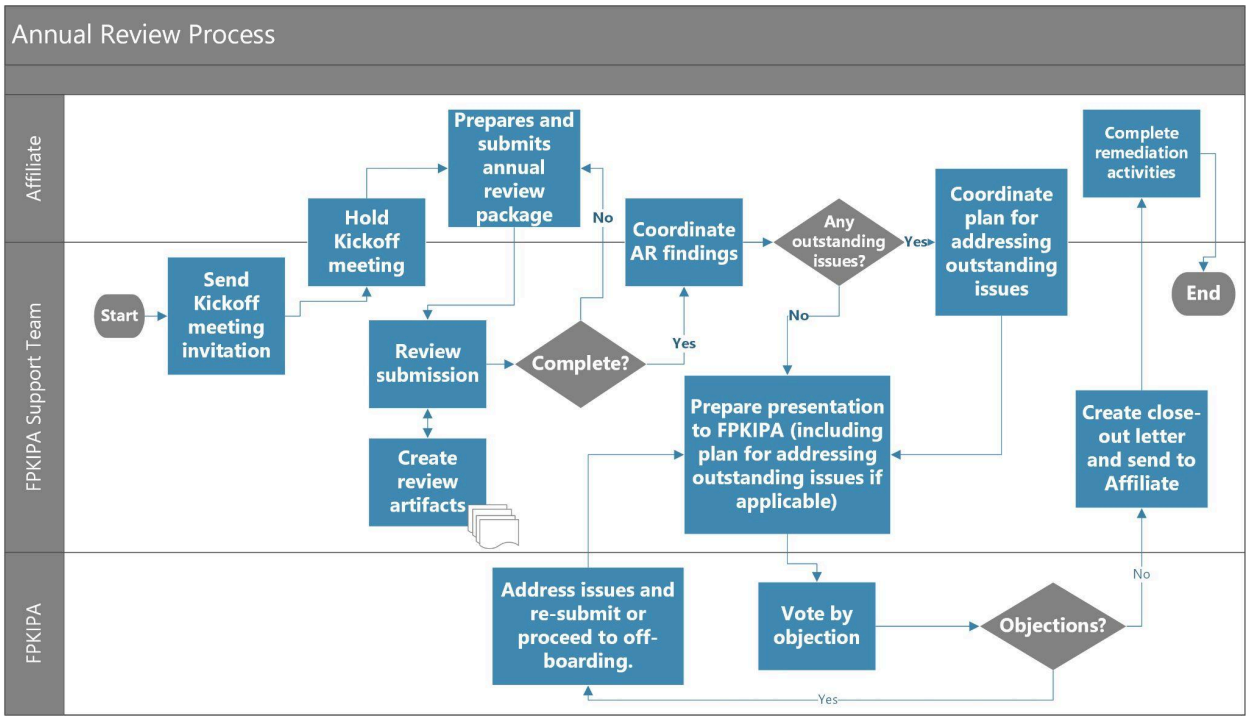
1.2. Audience

This document is intended for:

- All FPKI Affiliates, and
- Independent third-party Auditors who produce Audit Opinion Letters (See Appendix B).

2. Annual Review Process

2.1. Process Workflow



Assumptions:

- Affiliate is an approved member in good standing.
- An annual review documentation submission date has been agreed upon.

Process:

1. Kickoff Meeting - FPKIPA Support Team and Affiliate:
    a. Coordinate kickoff meeting specifics and send invitations.
    b. Hold Kickoff meeting:
        i. During the kickoff meeting, the FPKI Support Team reviews the submission artifact requirements with the Affiliate, provides information on any updates to the annual review process, and discusses findings from the previous year's review. The FPKIPA Support Team answers any questions the Affiliate has concerning the documentation requirements and the process.
2. Affiliate submits Annual Review package (see Section 3, Annual Review Package Elements):
    a. The Annual Review Package MUST be submitted to fpki@gsa.gov in accordance with the FPKI Annual Review schedule.
    Note: Sensitive information MAY be submitted directly to the FPKIPA co-chairs.
    b. FPKIPA Support Team reviews the package for completeness.
        i. Iterative - keep going back until complete.

3. FPKIPA Support Team begins detailed review of the package elements and:
    a. Create detailed review artifacts (Mapping report, Certificate compliance report, etc.).
        i. Each submission element is reviewed and the results of the review are documented in the appropriate artifact.
    b. Document any open issues.
        i. Any issues discovered during the review are documented and shared with the Affiliate
    c. Clarify questions regarding the submitted package that emerge during the review
4. FPKIPA Support Team completes review of the submitted package and coordinates issue handling with the Affiliate. This coordination can happen in real-time or via email:
    a. The Affiliate is given copies of the detailed review artifacts.
    b. The FPKIPA Support Team meets with the Affiliate to review the documented audit and annual review findings.
    c. The Affiliate is given the opportunity to ask questions to clarify the annual review findings.
    d. The Affiliate MAY provide a response to issues identified in the Annual Review as follows:
        i. Informal response: email or verbal response clarifying differences,
        ii. Formal written justification:
            1. If the Affiliate maintains that the identified issue is not a security or interoperability concern, it provides written justification by an agreed-upon date.
            2. The information from the written response could be included in the FPKI PA presentation.
        iii. Propose a mitigation strategy or mitigate the outstanding issue with immediate effect and provide updated documentation.
    e. If any of the responses vacate a finding, the documented results are updated and the updated documentation is provided to the Affiliate.
    f. Outstanding issues MAY be remediated before the PA presentation.
    g. For Annual Review issues not addressed before the PA presentation, the Affiliate creates an Annual Review Remediation Plan (ARRP) for addressing issues or adds these issues to the existing Audit Remediation Plan (AuRP), prior to subsequent Annual Reviews.
        i. The Affiliate agrees to update all remediation plans on an agreed upon schedule and share it with the FPKI Support Team.
        ii. The Affiliate agrees to periodic meetings or email updates to track progress.
    h. Recurrence of the same issues:
        i. As part of the next annual review results in a warning to the Affiliate from the PA management team.
        ii. Over three consecutive annual reviews will result in discussion at the FPKIPA meeting with the possibility of a “Not approved” recommendation.

i. The Affiliate is given the opportunity to review and provide feedback on the recommendation to be provided to the PA regarding the outcome of the FPKI FPKIPA Support Team's review of the Affiliate's AR package.

5. FPKIPA Support Team presents its findings with their recommendations at the FPKIPA meeting and posts the findings artifacts for FPKIPA member consideration on the FPKI AR connect.gov website:
    a. FPKIPA voting members vote by objection. If no objection is received, the FPKIPA Support Team's recommendation is accepted.
    b. If an objection is made, the FPKIPA Support Team enters into a discussion on ways to resolve the issue with the voting member who raised the objection and the Affiliate as needed.
6. FPKIPA Support Team issues a "Closeout letter" indicating that the AR is complete.
7. The Affiliate completes remediation activities as documented in their AuRP and ARRP, as required, before the next annual review.

This process is repeated annually.

3. Types of Affiliates

The FPKI community consists of the following types of Affiliates:

- Shared Service Providers
- Affiliate PKIs
- Affiliate Bridges

3.1. Shared Service Providers (SSPs)

An FPKI SSP operates a Certification Authority (CA) for certificate issuance on behalf of Federal agency customers[1] in compliance with the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework* [COMMON CP]. SSPs issue and revoke digital certificates, maintain a repository, maintain key escrow database, issue Certificate Revocation Lists (CRLs), and operate Certificate Status Server(s). The federal agency customer could be responsible for the remaining activities collectively referred to as Registration (identity proofing, enrollment, certificate request processing, and card issuance) or these could be performed by the SSP or another supporting organization.

The FPKI SSP MUST execute a formal Registration Authority Agreement (RAA) with any organization, including a federal agency customer, that provides Registration activities associated with the SSP's certificate issuance. The RAA MUST clearly identify which functions in the [COMMON CP] are the responsibility of the SSP and which are the responsibility of the federal agency customer or another supporting organization.[2] An example of responsibility that MUST be clearly spelled out is which organization is responsible for the annual RA Audit.

FPKI SSPs do not maintain their own CPs, but operate in compliance with [COMMON CP] and assert the [COMMON CP] policies in the digital certificates they issue. Each SSP MUST

[1] Other digital certificate services could be offered to Federal agencies by the SSP.

[2] The *FPKI Registration Authority Agreement Template and Guidance* [RAA] document provides specific guidance on the development of an RAA between an SSP and its Federal agency customer, along with the requirements for a Registration Practices Statement that specifies the requirements for conducting registration activities in accordance with the [COMMON CP].

maintain a CPS describing how the [COMMON CP] requirements are met and the SSP operations MUST implement those requirements and annually conduct an associated third-party independent audit of those practices.

The FPKIPA approves the SSP's CPS and customer Registration Practices Statements (RPS) as a condition of the SSP's continued operations.

3.2. Affiliate PKIs

Affiliate PKIs are cross-certified with the FPKI and maintain their own CPs, CPSs, and operational environments. The cross-certified trust relationship with the FPKI is based on a comprehensive mapping for comparability between the Affiliate's CP and the [FBCA CP].

Affiliate PKIs issue certificates to end-entities with policy identifiers mapped to Federal Bridge Certificate Policies. The mapped policies are documented in the Affiliate's CP and asserted in a cross-certificate via the policy mapping extension.

Some Affiliate PKIs are operated and maintained by Federal Agencies that also issue certificates in compliance with the [COMMON CP] as required by their use cases.

3.3. Affiliate Bridges

Affiliate Bridges operate as trust brokers for their own communities of interest and enable interoperability between their trust communities and the FPKI community. Affiliate Bridges issue cross-certificates to member CAs in their trust communities.

Each Affiliate Bridge MUST maintain a CP that maps to the [FBCA CP] and is responsible for ensuring its PKI members operate under CPs comparable to its own. In addition to the CP, governance documentation detailing the Affiliate Bridge's processes for cross-certifying new members and ensuring existing members continue to uphold the terms of Affiliate Bridge membership MUST be maintained.

3.4. Responsibilities

3.4.1. Affiliate Responsibilities

The Affiliate MUST meet the following requirements as part of the FPKI Annual Review Process:

- Maintain ongoing conformance of its PKI with its documentation (see Appendix A).
- Ensure Annual Third-Party Audits have been completed for all functions and elements of the PKI resulting in an Audit Opinion Letter (see Section 4.6 and Appendix B).
- Provide Auditor access to all appropriate documentation required to conduct the audit.
- Assemble and submit the Annual Review Package (see Appendix C) to the FPKIPA by the agreed upon date.
- Respond to FPKIPA queries regarding their Annual Review submission package.
- Address any findings or recommendations that result from the Annual Review.

3.4.2. Auditor Responsibilities

The Independent Third-Party Auditor MUST meet the following requirements:

- Conduct an Audit in alignment with the requirements of Section 6
- Verify the practice documents comply with the appropriate policies
- Verify the operations of the Affiliate align with the documented practices

- Provide an Audit Opinion Letter (see Appendix B) covering the audit scope identified by the Affiliate

3.4.3. FPKIPA Responsibilities

The FPKIPA MUST meet the following requirements as part of the FPKI Annual Review Process:

- Facilitate a kickoff meeting with FPKI Affiliates approximately 30 days prior to the agreed-upon submission date.
- Evaluate the submitted Annual Review Package
- Document and communicate all findings based on policy and practice gaps between the Affiliate and the FPKI
- Track the status of any findings and provide an opportunity for the Affiliate to respond to/remediate findings
- Facilitate a FPKIPA vote, based on the outcome of the Annual Review, to determine the Affiliate's continuing relationship with the FPKI

4. Annual Review Package Elements

Each Affiliate MUST submit an Annual Review Package every year. This section briefly describes the elements of an Annual Review Package.

4.1. Assertion of Scope

An authorized representative of the PKI MUST provide a letter or memorandum on the Affiliate's letterhead or a digitally signed artifact, asserting that the documentation included in the Annual Review Package covers the entire scope of the PKI. The Assertion of Scope MUST:

- Assert that the Annual Review Package represents a complete accounting of the entire PKI and encompasses all relevant components, including any that are separately managed and/or operated.
- Identify PKI functions that are separately managed and operated (e.g., RA functions), along with the identity of the organization responsible for those functions.
- If the package includes more than one Audit Letter, include a list of the annual Audit Opinion Letters included in the Annual Review Package, and indicate which PKI components and functions are covered by each annual audit; all PKI components MUST be accounted for as described in this document (see Section 6.1.2).
- Identify the period covered by the audit that supports this Annual Review submission (usually the 12-month period ending with the submission of the Annual Review Package),
- Identify the current CP (if applicable) and CPS(s) by name and version number.

Exemptions:
There are no exemptions for the assertion of scope. All FPKI Affiliates MUST submit an assertion of scope with their Annual Review packages.

4.2. Architectural Overview

The PKI MUST provide a detailed description of the PKI components and their relationships.

The overview MUST include:

- A list and detailed description of the security-relevant components of the PKI (i.e., CA, CMS, CSS, RA, KRS, DDS etc.), identifying those that are separately managed and/or operated,
- Diagrams showing the logical network view and logical architectural view of the infrastructure with enough detail to show the security-relevant components of the PKI (i.e., CA, CMS/RA, CSS public repositories, etc.) and the physical/logical security associated with them. The diagram MUST depict and identify those components that are separately managed and operated, and their connectivity to the CA.
    - Bridge Affiliate diagrams MUST list their member CAs.
- A list of the URLs for OCSP Responders and CRL Distribution Points included in certificates issued by the CAs.
    - Bridge Affiliates MAY include a list of URLs for CRL Distribution Point of the cross-certified member CAs.
- SSPs MUST include a list of supported organizations (e.g., Departments or Agencies).

Exemptions:
There are no exemptions for the Architectural Overview. All FPKI Affiliates MUST submit an Architectural Overview with their Annual Review package.

4.3. CA Inventory and Certificate Statistics

The Annual Review Package MUST include a list of the Affiliate's CAs (for Bridges, this includes Bridge members) with a path to an FPKI CA. Information to be included in the inventory includes: CA name, its issuer name, its intended purposes, and any known federal government applications that leverage the CA's end-entity certificates.

Additional information regarding end-entity certificates MUST be provided, including:

- A list of certificate types issued by each CA,
- The number of certificates (by type or certificate policy) issued by each issuing CA during the review period, and
- The total number of active certificates (by type or certificate policy) supported at the time the package is prepared and submitted.

This inventory does not need to include the certificate type for certificates that do not contain Common Policy or cross-certified policy OIDs or certificates issued in support of CA internal operations.

Exemptions:
There are no SSP or Affiliate PKI exemptions for the CA Inventory and Certificate Type list organized by CA.

Affiliate Bridges MUST disclose their CA relationships and their own certificate statistics; however, their member CA statistics are not required as part of the FPKI Annual Review package.

4.4. Current Policy and Practices Documents

Affiliate PKIs and Bridges MUST submit the latest approved versions of their CPs for mapping to the FBCA CP. In addition, if the CA maintains a key escrow, the Key Recovery Policy MUST be submitted, unless key recovery requirements are incorporated into the CP.

SSPs MUST submit the current CPSs for a [COMMON CP] compliance analysis. A Key Recovery Practices Statement (KRPS) MUST also be submitted, unless KRPS requirements are incorporated into the CPS. In addition, for those SSPs who do not maintain their own RA functions, the associated RPS(s) MUST be included in the Annual Review Package.

To facilitate comparison to previously reviewed versions, the CP, KRP, CPS, RPS and/or KRPS MUST be submitted in MS Word format.

Exemptions:
SSPs are not required to submit a CP or KRP, since they operate under the [COMMON CP].

Affiliate PKIs and Bridges are not required to submit practice statements (e.g., CPS, RPS, KRPS); however, audit letters MUST contain references to the practice statements that were evaluated.

Note: Affiliates that operate under a CPS mapped to the FBCA CP (rather than an Affiliate CP) MUST provide that CPS.

4.5. Registration Authority Agreement

SSPs MUST submit any Registration Authority Agreements (RAA) they have executed with customers who are providing RA services as part of the overall service delivery. SSPs MAY redact sensitive commercial information from their agreements.

Exemptions:

Affiliates that do not depend on any third parties for RA services are not required to execute an RAA or provide one as part of their annual package.

4.6. Audit Opinion Letter(s)

The Annual Review Package MUST include one or more Audit Opinion Letters that together encompass the entirety of the PKI identified in the Assertion of Scope (see Section 4.1).

All subcomponent audits and audit opinion letters MUST be completed within the 12 months preceding this Annual Review submission.

Each Audit Opinion Letter submitted MUST contain all of the elements listed in Appendix B.

If multiple Audit Opinion Letters are submitted, each MUST be signed by its respective third-party auditor. The Affiliate MUST clearly identify what CA(s) and/or PKI components and functions from the Architectural Overview are covered by each Audit Opinion Letter in the Assertion of Scope (see Section 4.1) and MUST ensure that all PKI components and functions under the overall responsibility of the participating PKI Policy Management Authority (PMA), including those that are separately managed and operated, are included in the Annual Review Package.

Exemptions:
There are no exemptions for submission of the Audit Opinion Letter(s). All FPKI Affiliates MUST submit Audit Opinion Letter(s) with their Annual Review packages.

Bridges are not required to include audit letters for their members, provided that the Bridge Audit Opinion Letter asserts the existence of audit opinion letters for members.

4.7. Federal Authorization

Shared Service Providers that issue PIV cards to federal agencies MUST maintain an Authorization to Operate (ATO) based on an Assessment and Authorization process and approval by a senior agency official. An SSP MUST provide a current ATO letter, or FPKI acceptable certification based on NIST SP 800-37 and SP 800-53 (i.e., FedRAMP), signed by the agency authorizing official or board as part of its annual review package.

4.8. Audit Issues and Audit Remediation Plan

If any new or recurring issues are identified in the audit, the Affiliate MUST provide a detailed Audit Remediation Plan (AuRP) detailing the findings including:

- Actions that have or will be taken to remediate the issues/findings, and
- Expected completion dates.

Exemptions:
If no issues were identified by the current audit and all actions from previous audits have been completed, no AuRP is required as part of the Annual Review package.

4.9. Certificate Artifacts for Interoperability Testing

Each Affiliate MUST submit production certificates as part of the Annual Review Package that are representative of all issued certificate types. DER (binary) or PEM (Base-64) encoded production certificates are acceptable formats. The following criteria MUST be applied when compiling certificate sample packages:

- The Affiliate MUST submit at least one production sample of every type of end-user certificate with a valid path to the FCPCA.
- Types of certificate are defined by permutations of certificate usage and asserted policy (e.g., software signature, hardware signature, software encryption, hardware encryption)
- Where more than one issuing CA is in use, submit the full complement of certificate types issued by each issuing CA
- The submitted end-user certificates MUST have been issued within the review period (preceding twelve (12) months), and preferably within the 90 days prior to package submission.
    - Bridge Affiliates MAY submit end-user certificates issued outside the 12-month period if they were used during the most recent annual certificate testing of their members.
- The certificate file names MUST be sufficient to identify the type of certificate and its issuing CA,
- The certificates MUST be production certificates that are operational and in use by the Affiliate's users.

The FPKI will conduct certificate testing and notify the Affiliate of any discrepancies. The Affiliate is responsible for incorporating these findings into the AARP (see Section 2.1).

Exemptions:
If a specific certificate type was not issued by a given CA during the review period, this SHOULD be noted and no corresponding sample is required as part of the submission package.

CAs that remain operational only for maintenance purposes and have not issued any certificates during the preceding 12 months, MUST be identified as such and are exempt from submitting sample certificates with the Annual Review package.

Note: Sample certificates MUST have a path to the FCPCA/FBCA, OLT certificates or certificates that assert policies that are not mapped to FPKI policies are out of scope for the FPKI annual review process

4.10. PIV and PIV-I Card Issuer (PCI) Configurations

Affiliates issuing PIV/PIV-I credentials MUST submit to GSA FIPS201 Evaluation Program testing as part of their annual review.

The GSA performs card testing through the FIPS201 Evaluation Program. When test reports are prepared by the FIPS 201 Evaluation Program, the report itself does not need to be included in the submitted Annual Review package.

If a Bridge does its own PIV-I Card testing rather than using the FIPS201 Evaluation Program, it MUST include test reports for each identified PCI.

Exemptions:
Affiliates that do not issue PIV or PIV-I cards are exempt from submitting PIV or PIV-I test reports in the Annual Review package. Note that this exemption includes Derived PIV Certificates.

4.11. Bridge Governance Documents

Bridges MUST submit the governance documentation that details its processes for cross-certifying new members and ensuring existing members continue to uphold the terms of Bridge membership.

Exemptions:
SSPs and Affiliate PKIs are exempt from submitting Bridge Governance Document in the Annual Review package, as they are not applicable.

5. Submission Artifact Summary

The previous section (Section 3) described the total set of artifacts that could be present in an Annual Review Package. The specific submission requirements for each type of Affiliate are summarized in the following table:

Artifact	SSP	Affiliate PKI	Affiliate Bridge
Assertion of Scope	Yes	Yes	Yes
Architectural Overview	Yes	Yes	Yes
Current CP (.docx format)	No	Yes	Yes
Current CPS(s) (.docx format)	Yes	No	No
KRP	No	If Applicable	If Applicable
KRPS	If Applicable	No	No
RPS	If Applicable	If Applicable	No
RAA	If Applicable	If Applicable	No
Audit Opinion Letter(s)	Yes	Yes	Yes
Authorization to Operate	Yes	No	No
Audit Issues and Audit Remediation Plan	If Applicable	If Applicable	If Applicable
Remediation POA&M	If Applicable	If Applicable	If Applicable
Certificate Artifacts for Interoperability Testing	Yes	Yes	Yes
PIV and PIV-I Test Report	Yes	If Applicable	If Applicable
Bridge Governance Documents	No	No	Yes

6. Annual PKI Audit Requirements

An Independent Third-Party Annual Audit is designed to answer the following key questions:

- Do the practices described in the CPS meet the requirements documented in the CP?
- Do the observed practices followed by the CA comply with the provisions of the CPS?

The following sections describe the requirements for an Annual Audit and identify types of audits to be performed.

6.1. Audit Methodology

The FPKI is audit methodology agnostic; however, the audit methodology used MUST be identified and described in the Audit Opinion Letter.

6.1.1. Documentation Analysis

Regardless of the audit methodology used, the following documentation MUST be analyzed as part of the audit:

- **CP** – The Auditor MUST list the version(s) of the CP applicable to the period of performance of the audit and used as the basis for the compliance review.
- **CPS** - The Auditor MUST identify the version(s) of the CPS in effect during the period of performance and verify that the CPS implements the requirements of the CP in a satisfactory manner.
- **KRP/KRPS** - If Affiliates perform key escrow and recovery activities, they MUST document the requirements and practices.
    - Such documentation MAY be incorporated into the CP and CPS or maintained in a separate KRP and KRPS. If a separate KRP and/or KRPS is maintained, the Auditor MUST identify the version(s) of the KRP and KRPS that were in effect during the audit period and verify that the KRPS implements the requirements of the KRP.
    - Note: Affiliates MAY adopt FPKI policy and implement a KRPS.
- **Current FPKI MOA** - The Auditor MUST verify that the Affiliate is complying with all provisions and obligations detailed in the MOA. A statement to this effect SHOULD be included in the Audit Opinion Letter.
    - Note: If the Affiliate (e.g. Bridge) maintains MOAs with other organizations, these are also within the audit scope and MUST be reviewed for compliance.
- **Current RAA** - Where applicable, the Auditor MUST verify an RAA has been executed between the Affiliate and the organization performing RA services and that the RA organization is complying with all provisions and obligations detailed in the RAA. A statement to this effect SHOULD be included in the Audit Opinion Letter.
    - Note: In the event RA services are audited separately and by a different Auditor or group of Auditors, these separate Audit Opinion Letters MUST be included in the Annual Review Package, unless they are listed as documents that were reviewed in the Audit Opinion Letter provided for the Affiliate PKI.
- **Previous Annual Audit Opinion Letter and findings** - Audits MUST include a review of the results of the previous Annual Audit Opinion Letter and findings, and verification that remediation of findings was completed satisfactorily.

Note: See Section 6.2.2 for WebTrust Audit requirements.

6.1.2. Use of Sampling

Sampling MAY be used as allowed by policy. If the Auditor uses sampling, all PKI components, PKI component managers, and operators for which the sampling applies MUST be considered in the sample. Samples MUST vary on an annual basis so that all PKI components eventually undergo auditing within a timeframe to be established. Each year, previous sampling results MUST be reviewed with an emphasis on determining whether discrepancies and deficiencies have been resolved.

6.2. Types of Audits

6.2.1. Full Operational Audit

Affiliates operating within the FPKI MUST undergo a full operational audit each year that includes evaluation of all operational practices. Included in this evaluation, the Auditor MUST review previous compliance audit findings for associated changes and corrective actions.

Under certain circumstances as allowed by FPKI PA, a Day-Zero Audit MAY be used as described below.

6.2.1.1. Day-Zero Audit

An Affiliate PKI or SSP currently participating in the FPKI MAY submit a Day-Zero Audit for a newly established PKI.

A Day-Zero Audit is used when a newly established CA has the policy, procedures, and resources to operate but has not accumulated sufficient operational evidence for evaluation against the appropriate CP/CPS. The Day-Zero Audit focuses on the policies and procedures associated with the new CA and the limited operational data that is available.

Affiliates that submit a Day-Zero Audit MUST complete a full operational audit, including a complete assessment of all operational practices, within one year of the Day-Zero Audit.

6.2.2. Special Provisions associated with a WebTrust for CA

The current WebTrust for CA audit methodology does not satisfy the FPKI requirements for ensuring the requirements of the associated CP are fully addressed. Therefore, when the WebTrust audit methodology is used, the audit opinion letter MUST include a statement from the Auditor that the CPS was evaluated for compliance with the CP and the operational practices are in accordance with the CPS. This can be satisfied by a Management Assertion Letter from an authorized Affiliate representative which states the following:

- The CPS conforms to the requirements of the CP,
- the PKI is operated in conformance with the requirements of the CPS,
- the PKI has maintained effective controls to provide reasonable assurance that procedures defined in Section 1 – 9 of the Affiliate CPS are in place and operational, and
- the PKI is operated in conformance with the requirements of all cross-certification MOAs executed by the affiliate.

The Management Assertion Letter MUST be attached to the Audit Opinion Letter. The Audit Opinion Letter MUST state that management's assertions have been evaluated and include an opinion as to whether they are fairly stated in relation to the PKI being audited.

Appendix A FPKI Affiliate Continuous Maintenance Requirements

This Appendix provides guidance for the on-going maintenance of an Affiliate's relationship with the FPKI. It is provided as a quick guide to aid in ensuring the continuing health of the FPKI trust community.

Affiliates MUST implement the following controls on a continuous basis and provide supporting documentation to the FPKI annually to ensure they meet agreed-upon levels of conformance and trust. Additionally, participation in the FPKIPA and the Certificate Policy Working Group (CPWG) helps Affiliates stay abreast of ongoing issues and priorities that could impact their operations.

Table A-1: Summary of Continuous Maintenance Requirements

Control Area	Required Actions & Controls
Policy Conformance – ensures Affiliate CP/CPS are aligned with FPKI Policy	– The FPKIPA updates [COMMON CP] or [FBCA CP] using the Change Proposal process. 1. Affiliates and Bridges MUST ensure their CPs continue to align with the FBCA CP as necessary. 2. SSPs andAffiliate PKIs that directly assert Common Policy OIDs MUST ensure their CPSs continue to comply with [COMMON CP]. 3. Affiliate Bridges and SSPs MUST ensure their members/customers stay aligned. – The FPKI reviews policy conformance during the Annual Review.
Technical Architecture – ensures technical interoperability between FPKI Affiliates	– Updates made to an Affiliate's technical architecture MUST be reported to the FPKIPA at the time the change is implemented. Examples of reportable updates include but are not limited to: ● Addition of new CAs ● Issuance or revocation of CA certificates ● Changes to PKI repositories that introduce new URLs for CRLs, OCSP, or CA certificates ● Changes to PKI repositories that introduce or eliminate support for different protocols ● Changes to PIV/PIV-I Issuers that would affect their certificates and/or cards – Impacts on security posture or interoperability are assessed by the FPKIPA. Failure to resolve issues identified by the FPKIPA could result in termination of the MOA/cross-certificate. – The FPKI reviews current architecture during its Annual Review even if no changes have been reported.

Control Area	Required Actions & Controls
Testing - ensures issued certificates are interoperable and cards are secure and conformant	– Affiliates MUST maintain conformance or technical interoperability with the appropriate FPKI certificate profiles (as applicable). – The FPKIPA reviews the certificates for conformance to the certificate profiles (as appropriate). – For Affiliates that issue PIV/PIV-I cards, each PIV/PIV-I Card Issuer Configuration MUST pass testing by the FIPS 201 Evaluation Program. The holder of the PIV/PIV-I card MUST participate in the testing. Remote testing can be conducted by using the Card Conformance Tool (CCT) and sending the resulting logs and test artifacts to the FIPS 201 Evaluation Program.
Governance – helps to ensure elements of the MOA are upheld	– SSPs MUST maintain a valid Authorization to Operate through the GSA Federal Information Security Modernization Act (FISMA) Assessment process. – Affiliates that issue PIV-I cards on behalf of Federal agencies MUST meet all of the requirements of the customer agency's FISMA Assessment process and maintain a valid Authorization to Operate. – Bridges MUST establish and maintain processes for governance and oversight of their cross-certified members as the FPKIPA reviews governance documentation during the Annual Review process.
Audit – ensures audits are conducted annually and the integrity of the governance processes are maintained	– FPKI Affiliates MUST have annual third-party audits conducted on their PKIs in accordance with the CP, CPS and other operational documentation, and submit the resulting Audit Opinion Letters for review according to the schedule published by the FPKIPA. – The FPKIPA reserves the right to request that an organization conduct an out-of-cycle compliance audit on any of its CAs. – The FPKIPA reserves the right to request additional detail related to the audits of Affiliate CAs or Bridge Member CAs. – The FPKIPA reviews audit documentation during the Annual Review process.

The following sections describe these requirements in more detail.

A1. Maintain Relevance to the Federal Community

The FPKIPA exists to support the needs of the federal government. Continuing membership of non-U.S. Federal Government Affiliates is based on the affiliates continued support of federal use cases.

A1.1. Support the approved business cases that were the basis for approval of the cross-certificate application

If an Affiliate was accepted on the basis of an approved business case, the Affiliate MUST continue to support the business case or submit and get approval for a new business case. If the affiliate no longer supports an approved business case, the affiliate's relationship with the FPKI could be terminated.

A1.2. Maintain the minimum required membership

For Affiliate Bridges, the value of their participation to the federal government is based on maintaining an active membership base. For an Affiliate Bridge to remain active, they MUST maintain the minimum number of members as specified in their MOA.

A2. Comply with the terms of the MOA

All Affiliates MUST comply with all terms and conditions of their MOA. Failure to maintain compliance is grounds for termination of the relationship.

A2.1. Perform annual independent audits

Annual audits MUST be conducted by all Affiliates and MUST cover the full scope of the affiliate's technical PKI architecture (e.g., CAs, public repositories, etc.), including elements of the architecture that are not managed directly by the affiliate themselves. Examples of additional elements MAY include:

- Audits of Registration Authority functions supported by customers
- Audits of Card Management Systems integrated with affiliates
- Key escrow and recovery functions

A2.2. Provide all mandatory notifications

Affiliates MUST notify the FPKIPA of certain events that are relevant to the community as a whole. These events are defined in the MOA and the FBCA and Common CPs. Failure to provide notifications could result in termination of the relationship with FPKI.

A2.3. Maintain required governance documents

Changes to the FBCA or Common CP have an "implementation date" by which all Affiliates MUST update their CPs and CPSs and make any changes necessary to account for the new requirements. These changes will be validated during the annual review process.

Independent changes (i.e., changes not related to a change in the FPKI CPs) to an Affiliate's governance documentation MUST be communicated to the FPKIPA if that change affects the technical architecture of the CA, the identity validation processes, other critical security requirements, or could impact the comparability of mapped policies. In all other cases, the Affiliate SHOULD notify the FPKIPA of changes to the Affiliate CP.

A2.4. Participate in the FPKIPA

Active participation in the FPKIPA by Affiliates helps ensure decisions made by the FPKIPA benefit the entire FPKI member community. Participation in FPKIPA meetings will ensure Affiliates have a voice in proposed changes to the FBCA or Common CP. All Affiliates are encouraged to participate in FPKIPA working groups, such as the Certificate Policy Working Group (CPWG), which deals with the development of PKI policies, and the FPKI Technical Working Group (TWG), which deals with technical PKI issues.

A3. Maintain technical interoperability

Technical interoperability is critical for the smooth functioning of PKI across the federal government and with partner organizations. Each Affiliate MUST ensure that it supports technical interoperability as required by its governing documents and MOA with the FPKIPA.

A3.1. Communicate updates to technical architecture

In addition to the mandatory notices defined in section 3.2.2.2, Affiliates SHOULD communicate any changes to their technical architecture or system configurations that could impact technical interoperability. Examples of these changes include:

- Changes to certificate profiles, such as support for additional extensions or non-standard assertions.
- For PIV-I Issuers, changes to card configuration
- Changes to Issuing CA names
- Changes to the location of public repositories such as CRL distribution points or AIA/SIA publication URLs.

Advanced notification of these changes ensures that federal relying parties are able to continue processing certificates.

A3.2. Renew, re-key, modify, or revoke cross-certificates or subordinate CA certificates

Affiliates will issue, renew, re-key, or modify cross-certificates, or subordinate certificates, as needed to support their infrastructures and maintain interoperability with the FPKI.

Affiliates MUST notify the FPKIPA of these activities as specified in the MOA and FPKI Certificate Policy.

Updates to cross-certificates issued by the Affiliate to the Federal Bridge (a.k.a. “return cross-certificates”) could be requested by the FPKIPA or FPKIMA. Affiliates MUST respond to these requests in a timely manner, as defined in the MOA.

A3.3. Publish and maintain certificate related artifacts as specified in the certificate policy

Affiliates MUST publish and maintain all certificate related artifacts as specified in their certificate policy. CA Certificates issued by the affiliate MUST be published in PKCS #7 compliant certificate bundles, in accordance with FPKI policy requirements. Expired or revoked certificates SHOULD be removed from these bundles in a timely manner.

A3.4. Request renewal of FPKI issued certificates

When required, the affiliate MUST request renewal of certificates issued to them by the FPKI. The Affiliate SHOULD complete a Certificate Request Form (CRF) at least two months prior to the expiration date on the cross-certificate to be renewed and coordinate all certificate signing requests with the FPKIMA team.

For additional information or questions, contact FPKI@gsa.gov.

A4. Comply with the Federal Public Key Infrastructure (FPKI) annual review requirements

Participating PKIs MUST submit an Annual Review Package as described in this document.

A5. Address any problems or incidents identified by the Affiliate or the Federal PKI Policy Authority

Either party to the cross-certification agreement 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 two parties. The FPKI Incident Management Procedures will be consulted as issues arise to determine if the issue needs to be handled by the processes described in that document.

For technical problems, the Affiliate's technical POC will work with the FPKIMA and the FPKI Technical Working Group (TWG) to resolve the issue(s).

For situations where the FPKIPA has reason to believe that an Affiliate is not operating in compliance with its MOA or CP, the non-compliance management procedures in the FPKI Incident Management document are followed until the issue is resolved. 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 could request that the Affiliate Bridge request 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 the request.

A6. Provide and update appropriate Affiliate points of contact

Communication between the Affiliate and the FPKI requires the FPKIPA and FPKIMA to have the names and contact information for critical points of contact on file. The Affiliate MUST provide the FPKIPA with points of contact and MUST ensure that these are kept up to date.

Points of contact MUST include:

- The entity-authorized official (i.e. the MOA signatory authority) who accepts responsibilities on behalf of the affiliate organization,
- Policy POCs who participate in the FPKIPA and manage the affiliate certificate policies, and
- Technical POCs for the PKI infrastructure

Affiliates MAY also provide support contact information, such as helpdesks.

Appendix B Audit Opinion Letter Checklist

This appendix provides additional guidance, questions, and comments that will assist in determining whether the Audit Opinion Letters are acceptable. Note that final determination is the responsibility of the FPKIPA. All Audit Opinion Letters will include the following as listed in Table B-1.

Table B-1: Audit Opinion Letter Checklist

Category	Requirement	Description/Commentary
General	Signature	The Audit Opinion Letter(s) MUST be addressed to the Affiliate and MUST include at least one of the following: ● The personal signature of the auditor, ● Corporate signature of the audit firm, or ● The signature of the entity-authorized official (see Section 6).
Auditor Background Information[3]	Identity	Identity of the individual auditor(s) performing the audit. Note: If multiple Audit Opinion Letters are provided, the specific auditor personnel MUST be identified in each letter. Unlike the signature, corporate Affiliate identification is not acceptable, auditors MUST be one or more identified individual(s).
	Competence	Include any relevant certifications of the individual auditor personnel as required by the applicable CP and CPS.
	Experience	Include the experience of the individual auditor personnel in auditing PKI systems, or related IT systems as required by the applicable CP and CPS.
	Objectivity/ Independence	Describe the relationship of the Auditor(s) to the participating PKI and the organization operating the component(s) being audited. This relationship MUST clearly demonstrate the independence of the Auditor(s) as required by the applicable CP and CPS.

[3] The FPKIPA reserves the right to review the qualifications and experience of any Auditor whose Audit Opinion Letter is submitted as part of an Annual Review Package. To be qualified, an Auditor must meet all the requirements documented in Section 8.2 of the appropriate FPKI CP ([FBCA CP] or [COMMON CP]).

Category	Requirement	Description/Commentary
Audit Scope	Letter Date	The Audit Opinion Letter MUST be dated no earlier than the end of the period of performance covered by the audit.
	Audit Date	The date(s) the audit was performed.
	Period of Performance	The period of operational performance the Affiliate's audit covers (e.g., the 12 months that preceded the audit).
	Audit Methodology	Each Audit Opinion Letter MUST identify the methodology used for the audit. **Note**: When using "WebTrust for CA" audit methodology: a statement, or management's assertion, regarding evaluation of the CP/CPS and operational practices MUST also be included.
	PKI Components in Scope	Which Affiliate PKI component(s) were audited (CAs, CSSs, CMSs, and RAs).
	Documents Reviewed	Which documents were reviewed as a part of the audit, including document dates and version numbers. If portions of the PKI Policy are documented separately from the CP (e.g. a separate Key Recovery Policy & Practice Statement) these documents MUST also be reviewed as part of the audit. Card Test Reports and MOAs SHOULD be included in the documentation lists when applicable. Note: at a minimum CP and CPS MUST be identified.
Audit Results	Statements concerning the Audit	A statement that the operations of the audited component(s) were evaluated for conformance to the requirements of its CPS.
		A statement that the CPS was evaluated for conformance to the associated CP.
		If applicable, a statement that the operations of the component(s) were evaluated for conformance to the requirements of all cross-certification Memorandum of Agreement (MOAs) executed by the participating PKI with other Affiliates. Note: this is always applicable for cross-certified PKIs
	Findings	Report all findings related to the evaluation of the operational conformance of the audited component(s) to the applicable CPS(s).
		Report all findings related to the evaluation of the CPS for conformance to the associated CP.

Category	Requirement	Description/Commentary
		If one or more MOAs were reviewed, report all findings related to the evaluation of the component(s) conformance to the requirements of all MOAs executed by the Affiliate.
	Closure of Previous Audit Cycle Findings	If applicable, state that findings from the previous audit were reviewed for closure. Note: this is always applicable if there were any findings reported the previous year
	Opinion	Provide an audit opinion concerning the sufficiency of the Affiliate's operations (by audited component if necessary) in relation to the corresponding CP and CPS.

Appendix C Annual Review Package Review Checklist

This Appendix provides additional guidance, questions, and comments that will assist in determining whether Annual Review Packages are complete. Note that final determination is the responsibility of the FPKIPA.

Table C-1: AR Package Review Checklist

Guidance	Commentary
Assertion of Scope For PKIs with multiple components, state whether evidence of Audit Opinion Letters for all components has been provided.	Did the Affiliate provide a cover letter that articulates the components of the PKI that are in scope for the Annual Review? Does the letter state that all components of the PKI are covered by the Audit Opinion Letters included in the annual review package? Note: for a Bridge, is it clear what organization is responsible for the operations of each CA? Does the Bridge operate any issuing CAs?
Architectural Overview The architectural diagram SHOULD provide enough detail to show the security relevant components and identify the components that are separately managed and operated.	Did the Affiliate provide an Architectural Overview and was there an accompanying diagram showing sufficient detail to assess the components, responsible parties and security posture of the PKI?
CA Inventory and Certificate Statistic	Was a list of all CAs provided, identifying each by common name, issuer, and listing the certificate types it issues? Did each CA in the list contain statistics regarding all certificates by type, issued within the Audit period and does it also include a total count of active certificates by type?
Current CP or CPS Cross certified Affiliates MUST submit the current CP. Affiliates subordinated under the FCPCA MUST submit the current CPS.	Was a .doc(x) version of the CP or CPS provided?
Audit Opinion Letter(s)	Do the Audit Opinion Letters cover all components of the PKI? Do the Audit Opinion Letters cover all of the requirements in Appendix B?
Audit Issues and Remediations	Was a list of Audit findings provided and is there a remediation plan and timeline associated with each issue?

Guidance	Commentary
Sample Certificates Because the FPKI relies on sample certificates to ensure the Affiliate PKI is compliant with profile requirements, interoperability, and reporting, sample certificates of all types issued within the last year MUST be submitted to the FPKIPA.	Was a list of all certificate types issued by all issuing CAs provided? Is there at least 1 sample production certificate provided for each identified certificate type and can the appropriate certificate profile be identified for each certificate type and sample?
PIV or PIV-I Test Reports	If appropriate, was a list of all PIV or PIV-I card test reports provided? Was a list of PCI Configurations included, if applicable? Are the PIV/PIV-I Test Reports available to the reviewer?
Bridge Governance Documents (Bridges ONLY)	Are governance documents (e.g., criteria & methods) included in the package, and do those documents outline the processes for certifying new members and maintaining current relationships?

Appendix D Off-Boarding Requirements

The following information, though not a part of the Annual Review Requirements, is provided for awareness and as a reference for participating PKIs. The FPKIPA could initiate termination of the MOA and off-boarding with an Affiliate. Some potential triggers for FPKIPA initiation of off-boarding procedures include:

- FPKIPA awareness of an Affiliate security or MOA violation
  - Annual Review negative outcome
  - Incident response failure
  - Failure to update certificate policies and practices in light of FPKI CP updates
- Affiliate no longer meets the approved business case
  - Non-U.S. Federal Government Affiliate business case no longer benefits the government's defined use cases (e.g., government customer revokes sponsorship)
  - Affiliate Bridge doesn't have adequate membership (as specified in their MOA) or organizational separation between an Affiliate Bridge and its member PKIs are not sufficient.

The following describes the generic process the FPKIPA would take in response to the above triggers:

1. Upon discovery of the failure, the FPKI Incident Management Plan [IMP] is invoked
   a. If it is a CA key compromise, emergency revocation would be done.
   b. Research is conducted to determine the nature of the failure.
2. An incident report as detailed in the [IMP] is completed and coordinated (Affiliate, FPKIPA/FPKIMA, etc.)
3. The report is brought to the FPKIPA for discussion and a vote to either remediate or revoke.
   a. In the case of remediation, the FPKIPA notifies the Affiliate of the decision and provides a resolution date after which the MOA will be terminated if the issue is not resolved. The FPKIPA notifies all members of the decision to remediate and the timeframe provided for resolution.
   b. In the case of revocation, the FPKIPA informs the Affiliate's POC and notifies all members of the timeframe for completing the revocation.
4. If the decision is revocation, or remediation fails:
   a. Termination of the MOA is coordinated by the FPKIPA Support Team
   b. The FPKIMA will revoke the cross-certificate
   c. The FPKI community is informed of the revocation and/or need to distrust anchors
   d. SSPs will:
      i. Revoke any existing subordinate or end-entity certificates (or ranges of possible certificate serial numbers)
      ii. Destroy private keys

   Note - Affiliate Bridges or Affiliate PKIs MAY be limited to FBCA cross-certificate revocation. Once the cross-certificates have been revoked, whether they continue their own operations is outside the purview of the FPKI.

In other cases, the Affiliate may initiate termination of the relationship with the FPKI. Potential triggers for Affiliate initiation of off-boarding procedures include:

- Business/profitability impact
- Notification by the Affiliate to the FPKIPA of a merger or acquisition by another party that leads to disqualification from FPKI participation (e.g., hostile foreign ownership, etc.)
- Other external factors that lead a Affiliate to voluntarily terminate MOA

In the event the Affiliate initiates off-boarding, the Affiliate POC notifies the FPKIPA in writing of:

- Its intent to terminate the MOA,
- The reason(s) for seeking termination, and the desired off-boarding timeline.

Additionally, an SSP will work with the FPKIPA to:

- Develop a plan for off-boarding that includes the following steps:
    - Determine the PKI scope, including:
        - A list of impacted issuing and/or intermediate CAs,
        - An inventory of end entity certificates (by type or expiration),
        - A list of impacted parties/customers, and
        - Documented customer migration plans (as needed),
    - Determine the off-boarding model
        - Terminate - includes issuance termination and validation service maintenance timelines, and requires complete, final certificate revocation;
            - Issuance termination defines when the last subscriber certificates will be issued and the latest date of validity
            - Validation services (e.g., OCSP and CRLs) will need to remain in place potentially after key termination depending on the longest validity of subscriber certificate
            - Termination instances generally require destruction of private keys and maintenance of relevant archives. Depending on the type of Affiliate, the archives MUST be maintained either internally or handed over to a government customer.
        - Decommission - no longer actively issuing new end-entity certificates:
            - The Affiliate and FPKIPA Support Team create a plan to support existing certificates through expiration and archives as required by policy. If the Affiliates can no longer host the revocation data, they MAY need to relinquish private signing keys to an identified Government customer.
    - Finalize planning (as needed)
        - Plan for revocations/renewals
        - Plan for key and/or archive handover (as needed)
        - Plan for continued certificate validation support (as needed)
        - Plan for continued security support (as needed)
        - Plan for continued archive support (as needed)
    - Document planning outcomes in an updated and executed MOA
    - Execute the plan

Appendix E Glossary

For a list of terms not defined in the body of this document, please see Appendix D: Glossary of the [Common CP]

Appendix F References

[COMMON CP] X.509 Certificate Policy for the U.S. Federal PKI Common Policy
https://www.idmanagement.gov/docs/fpki-x509-cert-policy-common.pdf

[FBCA CP] X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)
https://www.idmanagement.gov/docs/fpki-x509-cert-policy-fbca.pdf

[IMP] Incident Management Plan
https://www.idmanagement.gov/docs/fpki-imp.pdf

[RAA] FPKI Registration Authority Agreement Template and Guidance
https://www.idmanagement.gov/docs/fpki-ssp-raa.docx