FPKIPA

Federal Public Key Infastructure Policy Authority

Federal Public Key Infrastructure (FPKI) Annual Review Requirements

Version 1.2
May 6, 2022

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

Table of Contents

1. Introduction

The Federal Public Key Infrastructure Policy Authority (FPKIPA) is responsible for maintaining mutual 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 Entity participating in the FPKI.

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

1.1. Scope

All organizations operating a PKI cross-certified with the FPKI must submit an Annual Review Package to the FPKIPA.

This document describes the requirements and processes an Entity must satisfy to meet its FPKI Annual Review obligations.

Other obligations, such as a Shared Service Provider's (SSP) Authority to Operate (ATO), placed on specific members of the FPKI Community, may 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:

- Entities wishing to maintain a relationship with the FPKI, and
- Independent third-party Auditors who need information concerning the expected content of the Audit Opinion Letter

1.3. Participant Responsibilities

1.3.1 Entity Responsibilities

The Entity has the following responsibilities:

- Maintain ongoing conformance of their PKIs (see Appendix A)
- Ensure Annual Audits have been completed for all functions and elements of the PKI
- 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 coordinated due date

1.3.2 Auditor Responsibilities

The Independent Third-Party Auditor has the following responsibilities:

- Conduct an Audit in alignment with the requirements of Section 5
- Verify the practice documents comply with the appropriate policies
- Verify the operations of the Entity align with the documented practices
- Provide an Audit Opinion Letter (see Appendix B) covering the audit scope identified by the Entity

1.3.3 FPKIPA Responsibilities

The FPKIPA has the following responsibilities:

- Evaluate the submitted Annual Review Package
- Document policy and practice gaps between the Entity and the FPKI
- Provide an opportunity for the Entity to respond to/remediate findings
- Conduct a vote, based on the outcome of the Annual Review, to determine the continuing relationship with the FPKI.

1.4. Package Submission

The Annual Review Package must be submitted to fpki@gsa.gov in accordance with the FPKI Annual Review schedule.

Sensitive information may be submitted directly to the FPKIPA co-chairs.

2. Types of Entities

The FPKI community consists of the following types of PKI operators.

2.1. 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 certificate repository, issue Certificate Revocation Lists (CRLs), and operate Certificate Status Server(s). The federal agency customer may be responsible for the remaining activities collectively referred to as Registration (identity proofing, enrollment, certificate request processing, and card issuance) or these may 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 should 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 maintain a CPS describing how the [COMMON CP] requirements are met and the SSP operations must implement those requirements and conduct an associated audit of those practices.

The FPKIPA is responsible for approving the SSP's CPS and customer RPSs as a condition of their continued operations.

2.2. Affiliate PKI

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 organization'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 CP and asserted in a cross-certificate via the policy mapping field.

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

[1] Other digital certificate services may 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].

2.3. PKI Bridges

PKI Bridges operate as trust brokers for their own communities of interest and enable interoperability between their trust communities and the FPKI community. Bridges issue cross-certificates to the CAs in their trust communities. Each Bridge must maintain a CP that maps to the [FBCA CP] and is responsible for ensuring its member PKI domains operate under CPs comparable to its own. In addition to the CP, Bridges must maintain governance documentation that details its processes for cross-certifying new members and ensuring existing members continue to uphold the terms of Bridge membership.

3. Annual Review Package Elements

Each Entity CA must submit an Annual Review Package every year. This section briefly describes the elements of an Annual Review Package.

3.1. Assertion of Scope

An authorized representative of the PKI must provide a letter or memorandum on the Entity's letterhead or a digitally signed email, asserting that the Annual Review Package includes an audit or multiple audits that encompass all components of the PKI. The Assertion of Audit Scope must:

- Assert that the Annual Review Package represents a complete audit of the entire PKI and encompasses all relevant components, including any that may be 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,
- Include a list of the Audit Letters included in the Annual Review Package, and indicate which PKI components and functions are covered by each audit; all PKI components must be accounted for,
- Identify the period covered by 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 Entities must submit an assertion of scope with their Annual Review package.

3.2. Architectural Overview

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

For SSPs and Affiliate PKIs, 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.
- A list of the URLs for OCSP Responders and CRL Distribution Points included in certificates issued by the CAs. These URLs are most important for the CAs issuing subscriber certificates,
- For SSPs, a list of supported organizations (e.g., Departments or Agencies),

For Bridges, the overview must include:

- A logical diagram showing the CAs of the trust community associated with the Bridge.
- A list of URLs for CRL Distribution Points of the subscriber issuing CAs.

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

3.3. CA Inventory and Certificate Statistics

The Annual Review Package must include a list of Entity's CAs (for Bridges, this includes 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

The inventory must include a list of all certificate types issued by all subscriber issuing CAs identified in the entity CA list above. This list does not need to include certificate type for certificates that do not contain cross-certified policy OIDs or Certificates issued in support of CA internal operations.

Exemptions:
There are no exemptions for the CA Inventory and Certificate Type list by CA. All FPKI Entities must submit a CA Inventory and list of certificate types issued by each CA. Statistics should be included when available.

3.4. Current Policy and Practices Documents

Affiliates 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, provided they operate under the [COMMON CP].

Affiliates and Bridge PKIs are not required to submit practice statements (e.g., CPS, RPS, KRPS); however, audit letters must contain references to what practice statements were evaluated.

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

3.5. Registration Authority Agreement

SSPs must submit any Registration Authority Agreements 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:

Entities 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.

3.6. Audit Letter(s)

The Annual Review Package must include one or more Audit Letters that together encompass the entirety of the PKI scope.

If subcomponent audits were conducted over various time periods, the end of the audit period covered in a given subcomponent Audit Letter must be dated within the period covered by the Annual Review.

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

If multiple Audit Letters are submitted, each must be signed by its respective auditor. The Entity must clearly identify what CA(s) and/or PKI components and functions are covered by each audit letter in the Assertion of Scope 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. In addition, a cover letter must be provided that explicitly identifies which elements of the Architectural Overview are covered by which Audit Letter(s).

Exemptions:

There are no exemptions for the Audit Letter(s). All FPKI Entities must submit Audit Letter(s) with their Annual Review package.

Bridges are not required to include audit letters for their members, provided that the Bridge audit letter asserts the existence of letters for members, and confirms that reviews have occurred.

3.7. Audit Issues and Audit Remediation Plan

If findings are associated with the audit, the Entity must prepare a detailed report of the findings and a detailed Remediation Plan that includes:

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

This artifact is mandatory if any issues were identified in the audit, or if previously identified issues have not been resolved.

Exemptions:

If no issues were identified and all actions from previous audits have been completed, no remediation plan is required as part of the Annual Review package.

3.8. *Certificate Artifacts for Interoperability Testing*

Each PKI must submit production certificates as part of the Annual Review Package that are representative of all issued certificate types. The following criteria must be applied when compiling certificate sample packages:

- The PKI must submit at least one production sample of every type of end-user certificate with a valid path to the FCPCA. Samples must have been issued during the review period
- Types of certificate are indicated by the corresponding certificate usage (e.g., signature, encryption, authentication) and asserted policy
- 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
- 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 Entity's users.

The FPKI will conduct certificate testing and notify the Entity of any discrepancies. The Entity is responsible for incorporating these findings into the Annual Review Remediation Plan.

Bridges are expected to provide certificate samples from all of their members, as identified above.

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 their Annual Review package.

3.9. *PIV and PIV-I Card Issuer Configurations*

Entities issuing PIV/PIV-I credentials are required to submit the following information as part of their annual review:

- A list of all unique PIV Card Issuer (PCI) Configurations supported by the entity
- For each PCI configuration, a list of all organizations leveraging that configuration

A PCI configuration is a unique combination of the three following elements:

- the specific Card Management System (CMS) configuration,
- the specific Certification Authority (CA) and certificate template configuration, and
- the specific card stock being used.

Practice Note: If the difference between CMS configurations is limited to minor variations of the PIV physical topography (e.g. agency name or issuing organization) these CMS configurations are equivalent from the perspective of a PCI configuration. Only one representative PIV/PIV-I credential needs to be tested.

The GSA performs card testing through the FIPS201 Evaluation Program. When test reports are prepared by the FIPS201 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:
PKI Entities 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.

3.10. 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.

4. 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 entity are summarized in the following table:

Artifact	SSP	Affiliate PKI	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	No	No
RAA	If Applicable	If Applicable	No
Audit Letter(s)	Yes	Yes	Yes
Audit Issues and Audit Remediation Plan	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

5. Annual PKI Audit Requirements

An 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 that may be performed.

5.1. Audit Methodology

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

5.1.1 Documentation Review

Regardless of the audit methodology used, the following documentation must be included in the audit review:

- **CP** – The Auditor must list the appropriate version of the CP which was applicable to the period of performance of the audit and used as a basis for the compliance review.
- **CPS -** The Auditor must verify that the CPS implements the requirements of the appropriate CP in a satisfactory manner.
- **KRP/KRPS -** If entities perform key escrow and recovery activities, they must document the requirements and practices in a KRP and KRPS.
    - Note: Entities may adopt the FPKI KRP and implement a KRPS. Key recovery requirements and practices may be separate documents or incorporated in the CP/CPS.
- **Current FPKI MOA -** The Auditor must verify that the Entity is complying with all provisions and obligations detailed in the MOA. A statement to this effect should be included in the Audit Letter.
    - Note: If the Entity (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 Entity 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 Letter.
    - Note: In the event RA services are audited separately and by a different Auditor or group of Auditors, these separate Audit 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 Entity PKI.
- **Previous Annual Audit Letter and findings -** All Audits must include a review of the results of the previous Annual Audit Letter and findings, and verification that remediation of findings was completed satisfactorily.

5.1.2 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.

5.2. Types of Audit

5.2.1 Full Operational Audit

Entities operating within the FPKI must undergo a Full Operational Audit each year that includes evaluation of all operational practices encompassing the scope of the applicable CP and CPS. Included in this evaluation, the Auditor must review previous compliance audit findings for associated changes and corrective actions.

There is one exception to the Full Operational Audit that may be used depending on circumstances. This exception is called a Day-Zero Audit.

5.2.2 Day-Zero Audit

A PKI, other than a Bridge, applying to participate in the FPKI may submit its application with a Day-Zero Audit. An Entity currently participating in the FPKI may submit a Day-Zero Audit for a newly established CA in its 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 may be available.

Entities that choose to 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.

5.2.3 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, it must be accompanied by a signed statement from the Auditor that they evaluated the CPS for compliance with the CP and the operational practices against the CPS. This can be satisfied by a Management Assertion Letter from an authorized Entity 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 Entity CPS are in place and operational, and
- The PKI is operated in conformance with the requirements of all cross-certification MOAs executed by the organization.

The Management Assertion Letter must be appended to the Audit Letter. The Audit 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 Member Continuous Maintenance Requirements

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

Entities 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 entities stay abreast of ongoing issues and priorities that could impact their operations.

Control Area	Required Actions & Controls
Policy Conformance – ensures Entity 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 must ensure their CPSs continue to comply with [COMMON CP]. 3. Bridges and PKI Service Providers must ensure their members/customers stay aligned as appropriate. – The FPKI reviews policy conformance during the Annual Review.
Technical Architecture – ensures technical interoperability between FPKI members	– Updates made to an Entity'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 may result in termination of the MOA/cross-certificate. – The FPKI reviews current architecture during its Annual Review even if no changes have been reported.
Testing - ensures issued certificates are interoperable and cards are secure and conformant	– Entities must maintain conformance or technical interoperability with the appropriate FPKI certificate profiles (as applicable). – Entities must submit sample production certificates to the FPKIPA for testing during the Annual Review. The submission must include a sample certificate for each certificate type issued by the CAs in the Entity's PKI (e.g.

	identity, signature, encryption, OCPS signing, content signing, etc.). – The FPKIPA reviews the credentials (PIV or PIV-I) for conformance to the certificate profiles (as appropriate). – For Entities that issue PIV/PIV-I cards, each PIV/PIV-I Card Issuer Configuration must pass testing by the FIPS 201 Evaluation Program. This testing requires participation by the holder of the PIV/PIV-I card. 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. – Entities 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 member organizations must have annual third-party audits conducted on their PKIs in accordance with the CP, CPS or 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 member organization CAs or Bridge Member CAs. – The FPKIPA reviews audit documentation during the Annual Review process.

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:

Category	Requirement	Description/Commentary
General	Signature	The audit letter(s) must be addressed to the participating PKI PMA and must be signed by the auditor. If there are multiple audit letters, do each contain a compliant signature? Note: The signature may be the corporate signature of the audit firm or the signature of the head of the independent office within the participating PKI organization (e.g., the organization's Inspector General)
Auditor Background Information[3]	Identity	Identity of the individual auditor(s) performing the audit. Note: If multiple audit letters are provided, is the individual auditor identified in each letter? Unlike the signature, corporate entity identification is not acceptable, auditors must be one or more identified individual(s).
	Competence	Competence, including any relevant certifications, of the individual Auditor(s) that perform compliance audits as required by the applicable CP and CPS.
	Experience	Experience of the individuals performing the audit in auditing PKI systems, or related IT systems as required by the applicable CP and CPS.
	Objectivity/ Independence	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.
Audit Scope	Letter Date	The Audit 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 PKI operational performance the audit covers (e.g., the 12 months that preceded the audit).

[3] The FPKIPA reserves the right to review the qualifications and experience of any Auditor whose Audit 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]).

	Audit Methodology	Whether a particular methodology was used, and if so, what methodology. If multiple audit letters are provided does each indicate a methodology? Note: if a “WebTrust for CA” audit methodology was used, a statement regarding evaluation of the CP/CPS and operational practices or the management assertions must also be included.
	PKI Components in Scope	Which entity 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 should 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 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 entities. Note: this is always applicable for cross-certified PKIs
	Findings	Report any and all findings related to the evaluation of the operational conformance of the audited component(s) to the applicable CPS(s).
		Report any and all findings related to the evaluation of the CPS for conformance to the associated CP.
		If one or more MOAs were reviewed, report any and all findings related to the evaluation of the component(s) conformance to the requirements of all MOAs executed by the participating PKI.
	Closure of Previous Audit Cycle Findings	If applicable, state that any findings from the previous audit were reviewed for closure. Note: this is always applicable if there were any findings reported the previous year
	Summary of Changes	If applicable, state whether a summary of changes from the previous year was provided.

		Note: this is likely applicable based on changes to the [FBCA CP] or [COMMON CP] within the audit period or findings in the previous year’s audit
	Opinion	Provide an audit opinion concerning the sufficiency of the PKI 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.

Guidance	Commentary
Assertion of Scope For PKIs with multiple components, state whether evidence of audit reports for all components has been provided.	Did the Entity 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 Entity 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 Entities must submit the current CP. Organizations subordinated under the FCPCA must submit the current CPS.	Was a .doc(x) version of the CP or CPS provided?
Audit 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?
Sample Certificates Because the FPKI relies on sample certificates to ensure the Entity PKI is compliant with profile requirements, interoperability, and reporting, sample certificates of all types	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?

issued within the last year must be submitted to the FPKIPA.	
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: Glossary

For a full list of terms please see Appendix D: Glossary of the [Common CP]

Appendix E: 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

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