FPKIPA

Federal Public Key Infrastructure Policy Authority

Federal Public Key Infrastructure

Bridge Application Process Overview

Version 1.1

May 2, 2017

TABLE OF CONTENTS

1 INTRODUCTION

1.1 OBJECTIVE

This document provides a general framework for the Federal Public Key Infrastructure (FPKI) Bridge Application process. There are additional policies, guides, and documentation referenced throughout this document that provide additional detail and requirements for each process.

1.2 INTENDED AUDIENCE AND SCOPE

This document, issued under the authority of the Federal PKI Policy Authority (FPKIPA), is for use by personnel involved in cross-certification activities. This document should be read in conjunction with the Federal Bridge Certification Authority Certificate Policy [FBCA CP] and all other applicable documentation. Requests for information can be emailed to icam@gsa.gov.

1.3 GENERAL PRINCIPLES

Full benefits of public key cryptography can be best leveraged through widespread trust and the cross-certification of PKIs. The Federal Bridge Certification Authority (FBCA) is the primary vehicle for attaining this widespread trust for the Federal community. However, given the need to allocate resources carefully within the government, parameters must be established in order to prioritize cross-certification activities.

Cross-certificates issued by the FBCA are issued and revoked at the discretion of the FPKIPA. When the FBCA issues a cross-certificate to a non-federal entity, it does so at its own discretion for the benefit of the U.S. Federal Government. Any information submitted to the FPKIPA by an Applicant Bridge is for FPKIPA use in determining if cross certification is possible and desirable, and will be treated as proprietary in accordance with applicable non-disclosure agreements.

To assist in determining if the US Federal Government will consider an application, an Applicant Bridge shall submit a business case to the FPKIPA Chairs for approval. The business case shall outline how the cross-certification will benefit U.S. Federal Government.

1.4 DETERMINING BENEFITS OF A BRIDGE FOR THE FEDERAL GOVERNMENT

Bridge Certification Authorities (BCA) operate as trust hubs that facilitate interoperability between distinct communities of interest (COI) with established PKIs. BCAs do not issue certificates directly to users, nor are they intended to be used as trust points by the users of the PKI. Instead, their purpose is to establish trust relationships with different communities of interest. These relationships are combined to form a “bridge of trust,” enabling users from the different communities, with potentially different policy domains to interact with each other through the shared trust established by the BCA.

The FPKIPA assesses the COI represented by the Applicant Bridge and the use case(s) between these COI and Federal organizations in order to determine the return on investment to the government in establishing a cross-certification relationship with the Applicant Bridge.

2 APPLICATION AND EVALUATION PROCESS

The Application and Evaluation Process is designed to achieve a mutually-reliable trust relationship between the FBCA and the Applicant BCA. This section identifies the required steps to be executed by the various parties involved in the application process. Appendix A specifies the pre-requisites that must be met prior to an Applicant BCA's submission of an application for cross-certification. At any point during the cross-certification process the FPKI Chairs may inform the applicant that the application has been rejected if it is determined:

- There is insufficient benefit to the U.S. Federal Government in interoperating with the Applicant BCA
- There are sufficient risks or security concerns interoperating with the Applicant BCA
- The Applicant BCA's policies, process and procedures do not align with the FBCA

The Applicant BCA's application package (see Appendix B) shall include responses to all sections and all requested documentation shall be attached, unless otherwise indicated. The application package will be reviewed by the FPKI-Chairs and the FPKIPA.

After considering all inputs, if the decision is to proceed, the Applicant BCA will move on to the next phase. The next phase includes:

- Presentation of Business Case and Sponsorship to the FPKIPA
- Applicant Bridge Methodology Review
- Policy Mapping Analysis
- Technical Review and Testing
- Audit Review
- FPKIPA Vote on Cross-Certification
- Negotiation of Memorandum of Agreement
- Cross-certificate Issuance

Note: If the initial application is not approved, the Applicant BCA will be notified of the reasons why the request has been rejected.

2.1 PRESENTATION OF BUSINESS CASE & SPONSORSHIP TO FPKIPA

The presentation of the business case and identity of the Sponsor are required by Sections 6 and 7 (respectively) of the application. The FPKIPA Chairs will request the Applicant Bridge and Federal Sponsor make a formal in-person presentation to the FPKIPA to discuss the use case and benefits. Appendix C of this document provides detail on the responsibilities of the Sponsor.

2.2 BRIDGE METHODOLOGY ASSESSMENT

The Applicant Bridge shall have a formal documented process. The FPKIPA shall review the Applicant Bridge's processes for on-boarding, governing and overseeing PKI members who cross-certify. At a minimum, the processes shall address audits, certificate policy approval, testing (interoperability and security), MOAs, applications for new members, and on-going oversight and governance of existing cross certification relationships. The review will determine if the Applicant Bridge's processes provide the degree of assurance in the integrity of the Bridge's community to warrant participation in the Federal trust community.

Note: An organization should never operate both the Bridge and an issuing CA that is cross certified to its own Bridge. That is a clear conflict of interest.

2.3 Policy Mapping Review

Policy mapping is the analysis of comparing and contrasting the Applicant Bridge CP to the [FBCA CP]. The Applicant Bridge shall submit its CP for review by the FPKIPA. The CP shall be constructed in accordance with RFC 3647. The FPKIPA will compare the Applicant Bridge CP to the FBCA CP to ensure the operational environment and requirements leveraged on its members are comparable to the operational environment and requirements of the FBCA.

2.4 Technical Review And Testing

There are three components to the technical review and testing. These include:

- Technical Interoperability Testing
- PIV-I Card Testing Operational Capabilities Demonstration
- Certificate Analysis Inspection

For ***Technical Interoperability Testing,*** the Applicant Bridge shall demonstrate that its Bridge CA is technically compatible with the FBCA. The Applicant's PKI architecture, trust relationships, repository configurations, and the conformance or interoperability of the Applicant PKI certificates to the FPKI Profile and FIPS 186 will be reviewed. The objective is to:

- Determine whether there can be a successful generation and exchange of conformant cross-certificates
- When applicable, determine the directory interoperability, which includes identifying and resolving any incompatibilities between the technologies of the FBCA and Applicant BCA's PKI products, and minimizing the risk of introducing incompatibilities with current infrastructure
- Ensure Applicant BCA repositories are correctly configured to support path discovery and validation (PDVAL) in a complex FPKI environment

The FPKI Community Interoperability Test Environment (CITE) [FPKI CITE] is established to provide the FPKI community with a test environment to (a) identify and resolve issues, and (b) ensure proper functionality, prior to deployment to the production environment. It is configured as a duplicate of the Production FPKI Trust Infrastructure. Personnel representing the Applicant Bridge shall work with the FPKIMA to complete the technical interoperability testing.

The Applicant Bridge shall establish a test-bed that mirrors its operational environment and configure it in accordance with [FPKI CITE]. Any costs incurred by the Applicant Bridge resulting from establishing a test-bed and participating in technical interoperability testing shall be the responsibility of the Applicant Bridge. The Applicant Bridge shall maintain the test-bed and connectivity to the Community Interoperable Test Environment (CITE)after completion of the application process, so as to provide an environment for testing repository patches and new applications prior to deployment in the production environment. Technical interoperability testing, at a minimum, shall demonstrate that:

- Network communications are successfully using all required protocols.
- If applicable, the directories of the FPKI and the Applicant Bridge CA are interoperable.
- The cross-certificate request is correctly constructed by the FBCA and exchanged and recognized by the Applicant.
- The cross-certificate request is correctly constructed by the Applicant Bridge CA, exchanged with the FBCA, and recognized by the FBCA.
- A test transaction, using a test subscriber certificate of the Applicant Bridge CA, can be successfully validated
- The FBCA and the Applicant Bridge CA can share revocation information.

The PIV-I Card Testing Operational Capabilities Demonstration is reserved for Applicant Bridges seeking cross certification with the FBCA at the PIV-I policy levels.

If PIV-I is requested by the Applicant Bridge, testing requirements to include processes and procedures shall be submitted to the FPKIPA for review and approval. In addition, a site visit is required by a third party auditor, or by the FPKIPA Chairs, to confirm the processes and procedures and for demonstrating the Bridge's ability to conduct PIV-I card testing accurately. The Bridge shall have at least one FIPS 201 certified PACS system listed on the APL configured correctly in Federal Identity Credential Access Management mode, conduct manual certificate analysis, and ensure the PIV-I card complies and with a passing report utilizing the 85B tool listed on idmanagement.gov. Reports shall be provided to the FPKIPA for review, and receive approval prior to issuing production PIV-I cards.

The Bridge shall conduct PIV-I testing on a yearly basis for each distinct card configuration with the PKI's in their COI issuing PIV-I cards.

For ***Certificate Analysis***, the Applicant Bridge shall provide documentation on how inspection of production end-entity certificates issued by its members is conducted for the FKIPA to approve. Successful end-entity certificate testing shall be completed prior to the FPKI cross-certificate issuance to the Applicant Bridge.

If the Applicant Bridge cross-certifies with other CAs that issue PIV-I subscriber certificates or have subordinate CAs that issue PIV-I subscriber certificates, the Applicant Bridge is responsible for ensuring successful interoperability testing has been completed, documented and approved by the FPKIPA before authorizing use of mapped PIV-I policy OIDs.

An Applicant Bridge may only cross-certify with other CAs that do not align with FPKI requirements if policy mappings used do not map to any Bridge policies that also map to FBCA policies and proper constraints are included in any such cross-certificates to disable any transitive trust.

Note: The CAs in a Bridges' COI shall not be cross certified or otherwise connected to the Federal PKI at more than one point. Specifically, aside from existing certificate renewals and rekey, not more than one distinct trust path shall be intentionally created from any CA or End

Entity to the Federal Common Policy CA. This policy ensures the simplest possible certificate path building and validation by eliminating unnecessary choices and the potential for undesirable loops.

2.5 Audit Review

The Applicant Bridge CP shall demonstrate its PKI operates in accordance to applicable certificate policies that provide a level of assurance comparable to the requirements in the [FBCA CP]. To do so, the Applicant Bridge shall undergo an independent third-party audit that determines the following:

- The Applicant Bridge Certification Practices Statement adequately addresses all of the requirements of the Applicant Bridge CP; and
- The Applicant Bridge operations and management correctly implement the CPS.

The Federal PKI will review the Audit Opinion Letter for confirmation that the Applicant Bridge is being operated and managed in accordance with its CP. For additional information on the Audit review, see the FPKI Annual Review Requirements, Section 4.

2.6 FPKIPA Vote on Bridge PKI Cross-Certification

The FPKIPA reviews the information and inputs gathered in the preceding steps. Once this process has been completed, the FPKIPA will vote on whether to cross-certify with the Applicant. If the decision is to approve cross-certification, the Applicant BCA and FPKIPA shall sign a Memorandum of Agreement (MOA).

2.7 Negotiation of Memorandum of Agreement (MOA)

The relationship between the U.S. Federal Government and an organization operating a Bridge CA shall be governed by the MOA, to be signed by an official authorized to bind the Applicant Bridge and by an FPKIPA Chair.

The FPKIPA will provide an MOA template tailored for the type of cross-certification requested by the Applicant Bridge that will be used as a starting point for negotiations. The MOA shall be signed only after all issues have been resolved to the satisfaction of the FPKIPA.

A copy of the fully-executed MOA will be provided to the FPKIMA and Applicant for archival.

2.8 Cross-Certificate Issuance

The FPKIPA provides a Worksheet to the Applicant Bridge requesting technical and POC information for the cross-certification. This information is used to populate the cross-certificate requests and perform the cross-certification process. Following a satisfactory review of the technical data, the production cross-certificates are issued and posted to the appropriate repositories.

This page intentionally left blank.

APPENDIX A - BRIDGE APPLICATION PRE-REQUISITE CHECKLIST

A Bridge PKI seeking cross-certification with the FPKI must meet the criteria listed below for their application to be considered:

Requirement	Yes/No
Given the definition of the Bridge and its purpose, demonstrate why it is beneficial for the U.S. Federal Government to cross-certify with the Applicant Bridge	
The Applicant Bridge must have a Federal sponsor that will benefit from interoperating with the PKI community the Bridge supports. The Federal sponsor must state its intention to trust and accept the certificates of the PKI Community represented by the Bridge once approved and sustain sponsorship throughout the application/approval process.	
The Applicant Bridge is operational with at least two operational PKI entities not governed by the applicant bridge or a Policy Management Authority where the Applicant is involved	
Identify the FBCA policy OIDs with which the Applicant Bridge is requesting cross-certification	
Submit a current Audit Letter issued to the applicant Bridge's existing operations as evidence of documented history of successful PKI operations.	
Provide a Certificate Policy in RFC 3647 format that demonstrates a level of assurance comparable to the requirements in the [FBCA CP]. (The FPKIPA will make final determination of comparability).	
For Applicant Bridges seeking PIV-I cross certification, be prepared to establish the capability to perform PIV-I card testing in accordance with GSA FIPS 201 Evaluation Program Card Testing requirements for an operational production PIV-I Card	
Submit a copy of the Bridge PKI Charter describing membership, conflict resolution, authority, and organizational relationships.	
Provide a description of the Applicant Bridge Architecture	
Describe the Applicant Bridge's Repository architecture including protocols, directory structure and the approach to namespace control for distinguished naming.	
Provide evidence of the corporate status of the entity responsible for the Bridge, and its financial capacity to manage the risks associated with operating the Bridge.	
Provide evidence of the applicant Bridge's knowledge, skills and abilities in the management and operations of a Bridge PKI, to include resumes of key staff, identifying roles, PKI experience and expertise, number of years in the field, etc.	
Submit a completed Application Package using the template found in the Appendix below.	

APPENDIX B - FPKI CROSS-CERTIFICATION APPLICATION

Application for Cross Certification with the Federal Bridge Certification Authority

Applicant's Date of Submission: Click here to enter a date

Approved by FPKIPA on: Click here to enter a date

1. Contact Information

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

2. Organization Information

Applicant Organization	
Applicant Organization Address	

3. Applicant Point of Contact (POC) Information

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

Organization Representative POC	Name and Title Postal Address with Zip Code Office Phone Number Office E-mail Address
Cross Certification Process POC	Name and Title Postal Address with Zip Code Office Phone Number Office E-mail Address
Technical POC	Name and Title Postal Address with Zip Code Office Phone Number Office E-mail Address

4. Benefits to Federal Government

Describe the business case that will benefit the Federal Government from cross-certification with the Applicant.

5. Desired Federal PKI Cross-Certification Policies

Check all that apply.

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

6. Applicant PKI and Repository Overview

Provide information about your PKI, its community of use, and the expected benefit to the Federal Government of cross-certification. Note that the applicant must have experience operating a Bridge PKI to cross-certify with the FBCA.

Applicant PKI Information Requested	***Applicant Response***
The following governance documentation should be identified here and submitted with the application: ● Certificate Policy ● Charter ● Membership requirements (for on-boarding and maintaining membership) ● Conflict resolution processes and procedures for the Bridge	
What authority allows the Applicant Bridge to speak and act on behalf of its membership?	
Describe the nature of the relationship between member PKIs and the Applicant Bridge	
What community of interest does the Applicant Bridge serve?	
How does the Federal Community currently rely on certificates issued by Bridge Member PKIs?	
Describe the Federal Relying Party Application(s) that expect(s) to benefit from the use of these certificates.	
Describe the relationship between the Applicant Bridge PKI and its U.S. Federal Entity Sponsor.	
Describe the current operational status/practice of the Applicant Bridge PKI. For example: ● Is this PKI service currently operational in the mode in which the Applicant intends to	

Applicant PKI Information Requested	*Applicant Response*
cross-certify? ● If possible, provide an estimate of the size of the community the Applicant PKI will bring to the FPKI	
List any foreign ties the Applicant Bridge has	

7. Information on the Applicant Bridge PKI Architecture

Provide information about your Bridge PKI Architecture:

Architecture Information Requested	*Applicant Response*
Provide a list of those CAs under the Applicant Bridge's control that are either subordinate to, or have any other trust relationship with the Applicant's Principal CA. If any of those CAs provide certificates asserting object identifiers not covered in the Applicant CP, provide a description of the relationship between the CPs.	
Provide a list of CAs not under the Applicant Bridge's control that have any trust relationship (e.g., cross-certificate) with the Applicant's Principal CA or any CA under the Applicant's control that is subordinate to, or has any other trust relationship with, the CA the Applicant wants to cross-certify with the FPKI.	
Identify the following: ● CA Software utilized with an overview of the configuration ● CA OS and hardware utilized ● Directory Product utilized and any relevant configuration ● Network services and controls protecting the CA components	
Attach a PKI logical architecture diagram depicting the CA(s) within the Applicant's PKI and which CA(s) it wants to be cross-certified with the FBCA.	
Attach a detailed network diagram depicting the entirety of the Applicant Bridge components, their relationships and the network protection in place.	
Does the Applicant Bridge PKI community use a trust anchor within that PKI that requires FBCA	

Architecture Information Requested	*Applicant Response*
policies mapped to the Applicant Bridge PKI CP to provide mutual trust of FPKI certificates by the Applicant community?	
Provide any additional information that may be useful to the FPKI in evaluating this application, including up to the last three years of audit letters.	

8. Information on Applicant's Repository Architecture

Describe the Applicant's Repository architecture – what protocols will be supported for obtaining CA certificates and certificate status information. If applicable, describe the Applicant's Directory structure and how the Applicant will accomplish interoperability with the FBCA directory. Describe how the Applicant will ensure proper namespace control for distinguished naming. Include a description of any HTTP Repositories for CA certificates and CRLs and/or other certificate status services supported.

Applicant Repository Information Requested	*Applicant Response*
Does the Applicant intend to support a Directory for CRLs and CA certificates? (yes or no) If yes: a. Will the directory be accessible via X.500, LDAP or both? b. Will the Directory chain to the FPKI Directory? c. Will the Applicant's relying parties require the FPKI Directory to chain to the Applicant's Directory?	
Does the Applicant intend to support HTTP URIs for CRLs and CA certificates?	
Does the Applicant intent to support OCSP?	
Does the Applicant intend to support any other repository type? If so, please identify.	
Describe how certificate subjects will be named and how the Applicant Bridge will ensure proper namespace control of distinguished names.	
Attach a diagram of the Directory Schema	

9. U.S. Federal Entity Sponsor

Provide name and contact information of a U.S. federal entity sponsor.

Sponsor Name & Title	
Sponsor Department/Agency	
E-mail	
Phone	

10. Corporate Status

Provide evidence of the corporate status of the entity responsible for the PKI, and its financial capacity to manage the risks associated with operating the PKI. The nature and sufficiency of the corporate status and financial capacity will be determined at the discretion of the FPKIPA on a case-by-case basis.

11. Knowledge, Skills and Abilities

Provide evidence of the applicant Bridge's knowledge, skills and abilities in the management and operations of a Bridge PKI. Include resumes of key staff, identifying roles, PKI experience and expertise, number of years in the field, etc.

12. Signature

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

Applicant

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

Name:__________________________________

Title:__________________________________

Signature:______________________________

Date:__________________________________

Sponsor

I affirm I am an authorized representative of my Agency and agree to Sponsor the applicant listed.

Name:__________________________________

Title:__________________________________

Signature:______________________________

Date:__________________________________

APPENDIX C - FPKI SPONSORSHIP RESPONSIBILITIES

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

Federal Sponsor Responsibilities

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

APPENDIX D - DEFINITIONS

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

Bridge, Bridge CA : NIST Bridge Certification

Certification Authority (CA): An entity that issues X.509 certificates and vouches for the binding between the data items in a certificate [RFC 4949].

Certificate Policy (CP): A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements [RFC 4949]. A PKI may adopt more than one CP. CP also refers to the document containing the rules for one or more certificate policies.

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

Certificate Revocation List (CRL): A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire [RFC 4949].

Certification Practice Statement (CPS): A declaration by a CA of the details of the system and practices it employs in its certificate management operations A CPS is usually more detailed and procedurally oriented than a CP [RFC 4949].

Cross-Certificate: A certificate issued by one CA to another CA for the purpose of establishing a trust relationship between the two CAs. And stating the policy mapping between certificate policies in the issuing CA's CP to those in the subject CA's CP.

Cross-certification: The act or process by which two CAs each certify a public key of the other, issuing a public-key certificate to that other CA [RFC 4949].

Digital Signature: A value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity [RFC 4949].

Directory: A database server or other system that provides information, such as a digital certificate or CRL, about an entity whose name is known [RFC 4949].

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

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

FPKI Support Staff: The contractors and employees that support the FPKIPA and take direction from the FPKIPA Co-Chairs. This group includes the FPKIPA Secretariat.

Public Key Certificate: A digital certificate that binds a system entity's identity to a public key value, and possibly to additional data items; a digitally-signed data structure that attests to the ownership of a public key [RFC 4949].

Public Key Infrastructure (PKI): A system of CAs that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography [RFC 4949]. As used in this document, PKI also includes the entire set of policies, processes, and CAs used for the purpose of administering certificates and keys. The term also designates the person or organizational unit within an entity responsible for the following:

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

(b) Management of:

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

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

Repository: A system for storing and distributing digital certificates and related information (including CRLs, CPSs, and certificate policies) to certificate users [RFC 4949].

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

APPENDIX E - REFERENCE DOCUMENTS

Reference	Title	URL
Compliance Audit Requirements	Annual Review Requirements	https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/annual-review-requirements.pdf
Certificate Policy Mapping Report	Mapping Recommendation for Entity Certificate Policy to the specified Federal Bridge Certification Authority (FBCA) policies Template	https://www.idmanagement.gov/cpwg/
FBCA Audit Letter	Annual Review Requirements	https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/annual-review-requirements.pdf
FBCA CP	X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)	https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FBCA-Certificate-Policy-v2.31-06-29-17.pdf
FBCA CPS	X.509 Certification Practice Statement (CPS) For the Federal Bridge Certification Authority (FBCA)	https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-cps-redacted.pdf
FCPCA CP	X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework	https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-common-policy.pdf
FICAM Roadmap and Implementation Guidance	Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance	https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FICAM_Roadmap_and_Implem_Guid.pdf
FIPS 186	Digital Signature Standard (DSS)	http://csrc.nist.gov/publications/fips/
FPKI CITE	Requirements for Test Environment	https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FPKI_CITE_v1_0_4.pdf
FPKI MOA	An MOA used by the U.S. Federal PKI Policy Authority for cross-certifying with U.S. federal agencies and other U.S. federal entities, with U.S., state, and local governments and U.S. private sector Entities, and with Governments of other Nations	See sections 2.6 and 2.7.
FPKI Profile	Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile	https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-profiles.pdf

Reference	Title	URL
FPKI Security Controls of NIST SP 800-53	Federal Public Key Infrastructure (FPKI) Security Controls Profile of Special Publication 800-53 Security Controls for PKI Systems	https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-overlay-sp-800-53.pdf
FPKIPA Charter	Federal PKI Policy Authority Charter for Operations	https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FPKIPA_charter_1.0_Final.pdf
PIV-I Card Test Report	Personal Identity Verification Interoperable (PIV-I) Test Report For <Organization Name> Template	https://www.idmanagement.gov/piv-i_test_report_template-1/
PIV-I Profile	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards	https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-pivi-cert-profiles.pdf
PIV-I Test Plan	Personal Identity Verification – Interoperable (PIV-I) Test Plan	https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/PIV_I_Test_Plan.pdf
RFC 4949	Internet Security Glossary	http://www.ietf.org/rfc/rfc4949.txt
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	http://www.ietf.org/rfc/rfc3647.txt