



# **Federal Public Key Infrastructure Affiliate Maintenance Process**

Version 1.0  
October 2016

## OVERVIEW:

This document provides guidance to Federal Public Key Affiliates:

- **Non Federal Issuer** : entities cross-certified with the Federal Bridge Certification Authority (FBCA)
- **Federal PKI Shared Service Providers**: entities subordinate under the Federal Common Root
- **Bridge**: entities cross certified to the FBCA designed to link PKIs that implement different certificate policies and communities. Bridges only issue certificates to member CAs, other bridge CAs and bridge Operators.

on how to meet annual requirements and thereby remain in compliance.

The Maintenance Process consists of three core group activities that reoccur over the course of an annual cycle. Please note not all activities are listed and specific testing requirements are based on approved policies (e.g., not all Bridges or NFI support PIV-I).



*Note: Responsibility differences for Affiliates throughout this document are noted by the legend: Non Federal Issuer, Federal PKI Shared Service Providers, and Bridge.*

## ONGOING AFFILIATE ACTIONS AND CONTROLS:

There are actions and controls that Affiliates must perform annually, as well as on a continuous ongoing basis, in order to ensure that they meet agreed-upon levels of compliance and trust. These activities include:

- **Policy Conformance** controls that ensure that Affiliate CP remains aligned with the Federal PKI Policy
- **Technical Architecture** controls to ensure technical interoperability between the Affiliate and the Federal FPKI
- **Participation in the Certificate Policy Working Group and FPKI Policy Authority** to stay abreast of ongoing issues and priorities
- **Testing** controls to ensure that issued PIV/PIV-I Cards and Certificates are secure and conformant
- **Contractual** controls to ensure that the MOA is kept current
- **Audit** selection and scheduling controls to ensure that compliance audits are performed annually

Control Area	Required Actions & Controls
<b>Policy Conformance</b>	<ul style="list-style-type: none"><li>– The FPKIPA may update the FPKI CP using the Change Proposal process, thereby creating new requirements for Affiliates. Affiliates are responsible for implementing comparable changes in their CP if required and will be verified as part of the audit process. If an Affiliate/Bridge needs additional time to implement comparable changes, a plan to conform, submitted with the audit, may be acceptable when the Affiliate's audit schedule overlaps with the time required to implement the changes.</li></ul>
<b>Technical Architecture</b>	<ul style="list-style-type: none"><li>– Updates made in the Affiliate's PKI (Identity Management Card Management System, etc.) must be provided to the FPKIPA to determine if changes affects the MOA or interoperability between the FPKI and the Affiliate's PKI. Examples include but are not limited to:<ul style="list-style-type: none"><li>• Addition of new Certification Authorities</li><li>• Changes to PKI repositories that introduce or eliminate support for different protocols</li><li>• Changes to PIV/PIV-I Issuers that would affect their certificates and/or cards</li></ul></li><li>– Updates will be assessed by the FPKIPA and CPWG. Failure to resolve issues may result in termination of the MOA/cross-certificate.</li></ul>
<b>Testing</b>	<ul style="list-style-type: none"><li>– For Affiliates that issue PIV/PIV-I cards, each PIV/PIV-I Card Configuration shall be tested annually. Card testing with the FIPS 201 Evaluation Program shall be scheduled and completed successfully prior to the annual audit. Affiliates shall also submit production certificates for all types issued for testing to the FPKIPA. Testing is conducted to</li></ul>

Control Area	Required Actions & Controls
--------------	-----------------------------

ensure interoperability and compliance with the Certificate Policy.

- |                    |   |
|--------------------|---|
| <b>Contractual</b> | <ul style="list-style-type: none"><li>- Affiliates are responsible for ensuring that they have an executed MOA, using the template that is currently posted on IDManagement.gov.</li><li>- <a href="#">Abide by the GSA IT Security Procedural Guide: Managing Enterprise Risk Security Assessment and Authorization, Planning, and Risk Assessment CIO-IT Security – 06-30</a> and all deliverables associated outlined in the document.</li><li>- Those providing PIV-I cards to Federal agencies need to comply with the <a href="#">GSA IT Procedural Guide: Managing Enterprise Risk Security Assessment and Authorization, Planning and Risk Assessment CIO-IT Security – 06-30</a> and all deliverables associated outlined in the document and obtain an Authority to Operate as well.</li></ul>      |
| <b>Audit</b>       | <ul style="list-style-type: none"><li>- Affiliates shall have annual audits conducted on all CAs in the Affiliate's PKI according to the requirements stated in the FPKI Audit Guidelines document and schedule published by the FPKIPA.</li><li>- An associated Plan of Actions and Milestones shall also be provided to resolve any issues identified by the auditor for commercial affiliates associated with the Federal Bridge or Common Policy Root CAs. For Federal Agencies, a redacted version of the POA&amp;M will be accepted</li><li>- At any point if security issues are identified and cannot be resolved the FPKIPA can choose to revoke the Affiliate's cross certificate.</li><li>- The FPKI may request any affiliate to conduct a compliance audit on any one of its entities.</li></ul> |