Non-Compliance Management Framework For The Federal Public Key Infrastructure (FPKI)

Version 1.0.1

January 6, 2016

Revision History

Document Version	Change Date	Revision Details
1.0.0	12/17/15	Final Version
1.0.1	1/6/16	Updated Table 5, Certificate Policy Downgrade Illustrations to account for downgrade from FBCA High and Common High policies for completeness and accuracy

Table of Contents

1. INTRODUCTION

This document provides guidance for the FPKI Policy Authority (FPKIPA) for responding to situations where a cross certified member of the Federal Bridge Certification Authority (FBCA) is not meeting the requirements and obligations for being a member of the FPKI (see the Federal PKI Cross-Certification Evaluation Framework for a complete guide to these requirements). If a member does not comply with the requirements of membership, whether it relates to a policy requirement or some other membership requirement, it may not be prudent or practical simply to revoke the cross-certificate. This document presents a framework for addressing a full range of issues that may affect the cross certification/subordination relationship. It is designed to be used as a tool to guide the FPKIPA when dealing with these issues. The ultimate decision on how to address a specific situation lies with the FPKIPA. In serious, time-sensitive situations, such as serious security violations or Certification Authority (CA) compromise, the FPKIPA Co-Chairs may need to take emergency action and report their actions to the FPKIPA as part of a longer term mitigation plan.

In the sections that follow, the different issues that may affect the cross certified/subordinated relationship are categorized and each is given a suggested criticality. For every issue that arises, an analysis must be conducted to determine the potential risks. In addition, as new issues arise, other categories may be defined. A list of potential actions is also included with suggested timelines for implementation.

2. ISSUE RESPONSE CONSIDERATIONS

2.1 RELATIONSHIP TO FPKI

As indicated above, there are two primary types of relationships associated with the Federal PKI trust community:

- Subordination under the Federal Common Policy Certificate Policy (FCP CP) – this requires that the subordinated entity adopt the FCP CP and operate its PKI in strict compliance with that document, to include use of the policy OIDs defined in the FCP CP by the subordinate. A CA certificate is issued from the FCPCA to the subordinated entity signifying this subordinated relationship.
- Cross certification with the FBCA – this is a peer-to-peer relationship characterized by a mutual agreement between the FPKI and the cross certified entity that their policies and practices are comparable, which results in a mapping of policy OIDs and the issuance of cross certificates signifying cross-organizational trust. Cross-certified CAs fall into three categories:
    - *Bridge CAs* – Trust Hubs that, like the FBCA, exist to facilitate trust within a community of interest. They participate in the FPKI trust community in order to facilitate trust between the two communities of interest.
    - *Enterprise CAs* – Organizations that issue certificates to their own employees and affiliates. They participate in the FPKI trust community in order to extend the trust of their organizational certificates to a wider community and to enable their relying party applications to trust certificates issued by the wider community.
    - *Service Provider PKI* – Organizations whose primary purpose is to issue certificates on behalf of customer organizations and/or individuals. They participate in the FPKI trust community so that their customers will reap the same benefits as the Enterprise CAs.

2.2 BASIS OF TRUST

The trust relationship is based on a series of 'tests,' repeated annually to ensure continuing alignment.

Table 1: Trust Tests

For Subordination under Common Policy	For Cross Certification with the FBCA
Entity CPS comparison to FCP CP to determine Compliance	Entity CP mapping to FBCA CP to determine comparability
Annual Audit Review	Annual Audit Review
Interoperability Testing	Interoperability Testing
Smart Card Capabilities testing (PIV requirement)	Smart Card Capabilities testing (PIV-I requirement)
N/A	For Bridges Only: Cross-Certification Evaluation Framework Review

2.3 SECURITY VS. INTEROPERABILITY

There are two primary areas in which an issue that affects the current trust relationship may arise: Security and Interoperability.

- *Security* –Security issues arise when it is determined that a CA is not adhering to the requirements set forth in the applicable CP as determined by the Annual Audit; a cross-certified CA has revised its CP such that it alters the comparability and agreed policy OID mapping; or a subordinated CA has revised its CPS such that it is no longer compliant with the FCP CP. This is the more critical of the two and may require immediate action on the part of the Federal PKI to protect the trust fabric.
- *Interoperability* – Interoperability issues arise when the certificates issued by a CA are constructed in a way that prevents or interferes with relying party trust. Examples include setting a value to critical when it should be non-critical or including invalid pointers in the AIA or SIA fields. In some cases, deviations in certificate construction are by design and do not constitute interoperability issues.

The time at which an issue comes to light does not necessarily mark the point in time from which trust in certificates issued by the entity may be questionable. For example, if an annual audit uncovers questionable Registration Authority practices, certificates issued while those questionable practices were in effect may be untrustworthy. Therefore, some forensics may be required to determine when the deviation first occurred. All certificates issued after that time would be subject to whatever mitigation or get-well plan were implemented.

3. ISSUE RESPONSE ACTIONS

When an issue that affects the cross certificate or subordination relationship between the Federal PKI and one of its members is presented, there are a number of actions the FPKIPA can employ to mitigate the issue, dependent on what impact the issue has on the trust fabric. This impact can be expressed in terms of criticality, such that the greater the impact on the trust fabric, the greater the criticality. For the purposes of this discussion, criticality is separated into four categories:

- **Critical** – the issue does/may undermine the security of the FPKI trust fabric
- **Medium Impact** – the issue may result in an inappropriate level of trust in the affected end-user certificates
- **Low Impact** – the issue may result in some interoperability issues for relying parties processing affected end-user certificates
- **No Impact** – the issue has no material effect on the security or interoperability of the FPKI trust fabric

A relying party (RP) application makes the ultimate decision on which certificates to trust. The FPKIPA certifies that a given PKI meets FPKI criteria for trustworthiness. The way in which this is communicated to the RP application is via a cross-certificate which relies on the RP validating the entire certificate path. Note, that because the PA does not have direct communications with all RPs, out of band notifications of changes to that status may not reach all RPs who do not validate the certificate path across the FBCA.

Table 2 summarizes the action the FPKIPA may take in response to an issue, based on criticality of the issue.

Table 2: Criticality-Based Response

Criticality	Response		Description	Relying Party Impact
Critical	Revocation	Emergency Revocation	Conditions where the FPKIPA Chairs directs the FPKIMA to revoke a certificate due to a verified security risk to the trust community 1. Immediate revocation 2. Letter indicating action taken and remediation steps 3. E-mail Notification to FPKIPA and Relying Parties, other parties as appropriate	For Relying Parties utilizing path discovery and validation, impacted certificates are no longer trusted[1] and Relying Party users will not be able to authenticate to the application.

[1] If the certificate status information was cached, there may be a significant time delay before the non-compliant PKI is no longer trusted.

Criticality	Response		Description	Relying Party Impact
		Revocation Imminent	Conditions where revocation of a certificate is very likely (PA (or PA Chairs) makes final decision) due to a perceived/unverified security risk to the trust community 1) Warning letter issued with response deadline 2) Notify FPKIPA and call emergency meeting (where warranted) 3) E-mail Notification to FPKIPA and Relying Parties, other parties as appropriate	For Relying Parties utilizing direct trust, the Relying Party will be exposed to significant risk since they continue to trust certificates that cannot be validated without manual intervention to de-list the CA.
		Revocation Possible	Conditions where an issue will lead to revocation of a certificate if not resolved 1) Warning letter issued with response deadline 2) Notify FPKIPA 3) E-mail Notification to FPKIPA and Relying Parties, other parties as appropriate	
Medium Impact	Mapping Downgrade (FBCA only)		Conditions exist that may lead to a revised mapping of policies in the cross certificate issued by the FPKI 1. Notification letter issued with response deadline 2. Referred to CPWG for mediation and recommendation 3. Brief/final determination by FPKIPA	For Relying Parties utilizing path discovery and validation, trust in impacted certificates is modified.

Criticality	Response	Description	Relying Party Impact
	Compliance Issue Mitigation (FCP only)	A CP/CPS Compliance Issue is identified that alters the relationship between the Common Policy Root and the subordinated CA. 1. Notification Letter issued with response deadline 2. Referred to CPWG for mediation and recommendation 3. Notification/consultation with SSP customer agencies, if warranted 4. Brief/final determination by FPKIPA	For Relying Parties utilizing direct trust, the Relying Party will be exposed to possible risk since they continue to trust downgraded certificates without manual intervention to revise trust.
Low Impact	Interoperability Issue Mitigation	Conditions exist that interfere with relying party acceptance of the end-user certificates issued by a particular CA. 1. Notify Issuer 2. FPKIMA mediation 3. Determine additional requirements (CP/CPS revision, etc.) 4. Brief FPKIPA	For Relying Parties utilizing path discovery and validation or direct trust, impacted certificates MAY not be trusted.
No Impact	Acceptable Differences	Conditions where an issue is acknowledged and risk is accepted by all parties	No impact on RPs
	Certificate Policy Changes Required	Conditions where coordinated changes to CP are needed	Conditions where coordinated changes to CP may be needed

4. ISSUE EVALUATION GUIDE

Table 3 can be used as a tool by the FPKIPA to evaluate issues based on the category and criticality of each issue. This is not a strict algorithm, but a guide to help the FPKIPA in the decision making process. Other factors may significantly impact the urgency and criticality of a specific issue. Finally, more than one action can be taken if circumstances dictate. For example, it may be necessary to downgrade the mapping of a participating Entity while they execute an Issue Mitigation plan. To use the tool below, the FPKIPA can decide what category into which a particular issue falls and then decide, using the statements listed in the Description and Action columns, as a guide to assist in reaching consensus on the most appropriate response. The term "Boolean" in the Evaluation column is meant to indicate a binary result, while the term

"Subjective" is meant to indicate the criticality of the impact may be viewed differently depending on the applications of users involved.

Table 3: Issue Evaluation Guide

Category	Description	Evaluation	Criticality	Notes	Actions
Assurance	The deviation reduces overall assurance levels for FPKI. A condition of reduced confidence levels result from the variation.	Subjective	Medium Impact	Quantification of assurance/confidence levels can be very challenging, as it may be contextually-based. Audit-related considerations may be appropriate here.	Issue Mitigation
Functionality	The deviation causes impaired functionality or otherwise creates operational disruptions within the FPKI trust fabric.	Subjective	Medium Impact	Operational disruptions should hold severity comparable to security due to potential adverse business impacts (e.g., agency mission, commercial activities). Availability considerations (e.g., tied to service levels) could also be included here.	Issue Mitigation Revocation: Possible
Integrity	The deviation results in a compromise of the integrity of dependent applications or functions,	Boolean	Critical	This could also include authenticity, non-repudiation and reliability considerations. Data corruption may also be a consideration here (versus as part of security criteria).	Revocation

Category	Description	Evaluation	Criticality	Notes	Actions
Interoperability	The deviation causes problems with data exchange between selected members of the FPKI ecosystem.	Subjective	Low to Critical	Differentiation between interoperability and functionality is important. Threshold of significance (e.g., by volume of transactions or number of members) could result in this becoming a critical consideration by virtue of being analogous to operational disruptions.	Certificate Policy Changes Required Acceptable Mapping Downgrade Issue Mitigation Revocation
Policy/Practice	The deviation violates established FPKI policies or required practices.	Subjective	Low-to Critical	Could also be applied to recommended (best) practices. This may need to be differentiated between policy as a critical criteria and practice as a non-critical criteria.	Certificate Policy Changes Required Acceptable Mapping Downgrade Compliance Issue Mitigation
Security	The deviation results in potential breach or loss of data.	Boolean	Critical	Possible refinement needed to differentiate PII-related data with separate incident handling protocols. This could also include confidentiality and (explicit) trust considerations.	Revocation

Category	Description	Evaluation	Criticality	Notes	Actions
Standards	Does the deviation result in failure to conform to established standards for [F]PKI implementation or operation.	Subjective	Low-to Critical Impact	Differentiation of adherence to standards may be necessary for Federal versus non-Federal entities.	Certificate Policy Changes Required Acceptable Mapping Downgrade Issue Mitigation

5. ISSUE RESPONSE TIMELINE

While individual circumstances dictate a true timeline, Table 4 includes recommendations for time-to-resolve depending upon the criticality of an issue.

Table 4: Time-to-Resolve Recommendations

Criticality	Time to Correct
Critical	As soon as practical
Medium Impact	6 months
Low Impact	1 year
No Impact	N/A

APPENDIX A: MAPPING DOWNGRADE

It may be necessary to downgrade the mapping of a Participating Entity's policies until the issues are resolved. This provides incentive for the Participating Entity to resolve the issue and also provides a mechanism to inform the RP that the Participating Entity's certificates should be trusted at a lower level of assurance. The actual impact to the Relying Party depends on how its system is configured and whether it uses the FCPCA as a trust anchor.

The specific issue should be considered when determining whether a downgrade in policy should be applied. Table 5 illustrates of how specific policies might be downgraded.

Table 5: Certificate Policy Downgrade Illustrations

Original Mapped Policy	Issue	Downgraded Mapped Policy	Impact on RP community
PIV-I Hardware	Evidence that appropriate identity source documents were not used when identity proofing subscribers. APL Card Stock not used.	Medium Hardware which is mapped to Common Hardware	No impact on an RP configured to accept common hardware which is the policy used by PIV signature & encryption
High		Medium Hardware	Likely to have an impact
Medium Hardware	Subscriber keys were not generated on FIPS 140 Level 2 Crypto devices	Medium	Adobe will no longer trust for signature, other RPs such as DoD may require medHW and above so would be impacted.
Medium	RA practices or Subscriber agreement did not meet medium requirements	Basic	Likely to have an impact
Basic		Rudimentary	Likely to have an impact
Common High		Common Medium Hardware	Likely to have an impact

Original Mapped Policy	Issue	Downgraded Mapped Policy	Impact on RP community
Common Medium Hardware	RA Practices did not conform to PIV requirements. Subscriber keys were not generated on FIPS 140 Level 2 Crypto devices	Common Policy	Adobe will no longer trust for signature, other RPs such as DoD may require medHW and above so would be impacted.
Common Policy		N/A	Since Common Policies are not mapped, there is no real way to downgrade these through a policy mapping. There would be no real way to recover short of a new CA.
Common Auth	RA Practices did not conform to PIV requirements. Background checks were not completed as required.	N/A	Since Common Policies are not mapped, there is no real way to downgrade these through a policy mapping. There would be no real way to recover short of a new CA.
PIV-I cardAuth	RA Practices did not conform to PIV-I requirements.	N/A	Since PIV-I cardAuth does not require a PIN to access, there is no “lower assurance” policy.
Common cardAuth	RA Practices did not conform to PIV requirements.	N/A	Since Common Policies are not mapped, there is no real way to downgrade these through a policy mapping. There would be no real way to recover short of a new CA, in addition, since Common cardAuth does not require a PIN to access, there is no

Original Mapped Policy	Issue	Downgraded Mapped Policy	Impact on RP community
			"lower assurance" policy.