FBCA Certificate Policy Change Proposal Number: 2018-02

To: Federal PKI Policy Authority (FPKIPA)

From: FPKI Certificate Policy Working Group (CPWG)

Subject: Proposed modifications to the FBCA Certificate Policy

Date: July 6, 2017

Title: Update FBCA CP to reference Annual Review Requirements

Version and Date of Certificate Policy Requested to be changed: X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA) Version 2.32, 4 April, 2018

Change Advocate's Contact Information: FPKIPA

Organization requesting change: FPKI Policy Authority

Change summary: Update the CP to reference FPKI Annual Review Requirements

Background:

The FPKI Audit Compliance Requirements has been superseded by the FPKI Annual Review Requirements. This change updates the FBCA CP to include the new document reference.

Specific Changes:

Insertions are underlined, deletions are in ~~strikethrough~~:

8. COMPLIANCE AUDIT & OTHER ASSESSMENTS

All Entity CAs are subject to an annual review by the FPKIPA to ensure their policies and operations remain consistent with the policy mappings in the certificate issued to the Entity by the FBCA.

The FPKIMA shall have a compliance audit mechanism in place to ensure that the requirements of this CP and the FBCA CPS are being implemented and enforced.

The Entity PKI PMA shall be responsible for ensuring audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated.

This specification does not impose a requirement for any particular assessment methodology.

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

The FBCA, Entity Principal CAs, CMSs, and RAs and their subordinate CAs, CMSs, and RAs shall be subject to a periodic compliance audit at least once per year for High, Medium Hardware, PIV-I Card Authentication, and Medium Assurance, and at least once every two years for Basic Assurance. Where a status server is specified in certificates issued by a CA, the status server shall be subject to the same periodic compliance audit requirements as the corresponding CA. For example, if an OCSP server is specified in the authority information access extension in certificates issued by a CA, that server must be reviewed as part of that CA's compliance audit.

~~As an alternative to a full annual compliance audit against the entire CPS,~~ The compliance audit of CAs and RAs ~~may~~ shall be carried out in accordance with the requirements as specified in the *FPKI ~~Compliance Audit~~ Annual Review Requirements* document [AUDIT].

There is no audit requirement for CAs and RAs operating at the Rudimentary level of assurance.

The FBCA and Entity Principal CAs have the right to require periodic and aperiodic compliance audits or inspections of subordinate CA or RA operations to validate that the subordinate entities are operating in accordance with the security practices and procedures described in their respective CPS. Further, the FPKIPA has the right to require aperiodic compliance audits of Entity Principal CAs (and, when needed, their subordinate CAs) that interoperate with the FBCA under this CP. The FPKIPA shall state the reason for any aperiodic compliance audit.

8.6 COMMUNICATION OF RESULTS

On an annual basis, the Entity PKI PMA shall submit an ~~audit compliance~~ annual review package to the FPKIPA. This package shall be prepared in accordance with the ~~"Compliance Audit Requirements"~~ *FPKI Annual Review Requirements* document and includes an assertion from the Entity PKI PMA that all PKI components have been audited - including any components that may be separately managed and operated. The package shall identify the versions of the CP and CPS used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in Section 8.5 above.

10. BIBLIOGRAPHY

AUDIT	FPKI ~~Compliance Audit~~ Annual Review Requirements ~~http://www.idmanagement.gov/fpki-documents~~ https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/annual-review-requirements.pdf

Estimated Cost: There may be an additional cost to organizations to fully comply with the FPKI Annual Review Requirements

Implementation Date: Organizations must comply with the Annual Review Requirements at their next annual review.

Prerequisites for Adoption:

None

Plan to Meet Prerequisites:

Not Applicable

Approval and Coordination Dates:

Date presented to CPWG: July 18, 2018

Date change released for comment: July 18, 2018

Date comment adjudication published: No comments received.

Date published: May 8, 2018.