



**FBCA Certificate Policy Change Proposal Number:** 2010-02

**To:** Federal PKI Policy Authority  
**From:** Certificate Policy Working Group  
**Subject:** Proposed modifications to the Federal Bridge CA Certificate Policy  
**Date:** January 7, 2010  
**Title:** § 8.1 and 8.4

**Version and Date of Certificate Policy Requested to be changed:**

X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA), Version 2.12, February 11, 2009.

**Change Advocate's Contact Information:**

Name: James Schminky  
Organization: U.S. Department of the Treasury  
Telephone number: 202-622-2446  
E-mail address: james.schminky@do.treas.gov

**Organization requesting change:** Federal PKI Certificate Policy Working Group

**Change summary:** This change proposal modifies the current requirements for compliance audits. Specifically, this change proposal will permit the compliance audit against the full CPS to be conducted over three years as long as some of the key controls are examined annually.

**Background:** To further align federal policy to emerging industry trends and lessons learned about reasonable compliance audit that ensure trust and assurances are being maintained.

**Specific Changes:** Specific changes are made to the following sections: 8.1, 8.4

Insertions are underlined, deletions are in ~~striketrough~~ text:

**8.1 COMPLIANCE AUDITS & OTHER ASSESSMENTS**

*Modify Section 8.1 as follows:*

The FBCA, Entity Principal CAs and RAs and their subordinate CAs and RAs shall be subject to a periodic compliance audit at least once per year for High, Medium Hardware, 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 be carried out in accordance with the requirements as specified in the Triennial Audit Guidance document located at <http://www.idmanagement.gov/fpkipa/>.

~~For entity PKIs operated by federal agencies and entity PKIs operated under federal contract, alternative reviews may be substituted for full compliance audits under exceptional circumstances. The conditions that permit an alternative review are as follows:~~

- ~~(1) If no changes to policies, procedures, or operations have occurred during the previous year, an assertion to that effect, signed by the cognizant executive (CIO or equivalent), is acceptable in lieu of a full compliance audit.~~
- ~~(2) If no significant changes to policies, procedures, or operations have occurred during the previous year, a delta compliance audit is acceptable in lieu of a full compliance audit.~~
- ~~(3) However, a full compliance audit (see section 8.4) must be completed every third year regardless.~~

~~Practice Note: Examples of significant changes include but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to CA and or RA operating procedures; (iii) installation of a new or upgraded hardware platform or firmware component; and (iv) modifications to the certificate policy. This is consistent with the requirements that trigger a full C&A in NIST SP 800-37.~~

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 Federal PKI Policy Authority 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 Federal PKI Policy Authority shall state the reason for any aperiodic compliance audit.

## **8.4 TOPICS COVERED BY ASSESSMENT**

*Modify section 8.4 as follows:*

The compliance audit of the FBCA shall verify that the FPKI Management Authority is implementing all provisions of a CPS approved by the FPKI Policy Authority consistent with this CP. The audit shall also verify that the FPKI Management Authority is implementing the relevant provisions of the MOAs between the FPKI Policy Authority and each Entity PKI.

The purpose of a compliance audit of an Entity PKI shall be to verify that an entity subject to the requirements of an Entity CP is complying with the requirements of those documents, as well as any MOAs between the Entity PKI and any other PKI.

A full compliance audit for the FBCA or an Entity PKI covers all aspects within the scope identified above.

~~Where permitted by section 8.1, the FBCA or Entity PKI may perform a delta compliance audit in lieu of the full compliance audit. A delta compliance audit covers all changes to policies, procedures, or operations that have occurred during the previous year. The following topics must be addressed in a delta compliance audit even if no changes have occurred since the last full compliance audit:~~

- ~~(1) Personnel controls;~~
- ~~(2) Separation of Duties;~~
- ~~(3) Audit review frequency and scope;~~
- ~~(4) Types of events recorded in physical and electronic audit logs;~~
- ~~(5) Protection of physical and electronic audit data;~~
- ~~(6) Physical security controls; and~~
- ~~(7) Backup and Archive generation and storage.~~

**Estimated Cost:**

No additional cost to the Federal Bridge CA.

**Risk/Impact:**

None identified.

**Implementation Date:**

This change will be implemented immediately upon approval by the FPKIPA and incorporation into the Federal Bridge CA Certificate Policy. Currently cross-certified entities have two years from the date of approval to effect this change.

**Prerequisites for Adoption:**

There are no prerequisites.

**Plan to Meet Prerequisites:**

There are no prerequisites.

**Approval and Coordination Dates:**

Date presented to CPWG: January 7, 2010  
Date presented to FPKIPA April 6, 2010  
Date of approval by FPKIPA: April 6, 2010