Federal Bridge CA Certificate Policy Change Proposal

Change Number: *2005-03*

To: Federal PKI Policy Authority
From: FPKI Certificate Policy Working Group
Subject: Proposed modifications to the FPKI Audit Cycle
Date: 13 December 2005

Title: Changes to the FBCA CP to modify audit cycle for consistency with Government certification and accreditation process

Version and Date of Certificate Policy Requested to be changed:
X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA) dated 13 September 2005.

Change Advocates Contact Information:
Dave Hanko, DoD
(410) 854-4096
dhanko@missi.ncsc.mil

Cheryl Jenkins, FPKI OA
Cheryl.Jenkins@gsa.gov

Tim Polk, NIST
(301) 975-3348
tim.polk@nist.gov

Organization requesting change: CPWG

Background: The FBCA CP requires a full compliance audit annually, even where significant changes to the PKI have not occurred. This is inconsistent with established OMB policy (A-130) and NIST practices (NIST SP 800-37) for ensuring the trustworthiness of government computing systems. This change proposal eliminates unnecessary audits without compromising trustworthiness of the PKI.

Change summary:
This change proposal modifies the FBCA CP as follows:

1) A three year cycle for compliance audits is established. Beginning with a "full compliance audit."
2) Alternative annual review mechanisms are established within the overall cycle for entity PKIs operated by agencies, or under federal contracts. These PKIs fall under FISMA regulation, so federal C&A requirements may also be considered.

Specific Changes:
The following changes are to be made to the FBCA CP: *insertions* are shown in italics.

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

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.

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.

[no changes in 8.2 or 8.3]

8.4 TOPICS COVERED BY ASSESSMENT

The compliance audit of the FBCA shall verify that the FPKI Operational 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 Operational 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:
There is no financial cost associated with implementing this change. Substantial savings may be achieved by PKIs when little or no changes occur in years following a full compliance audit.

Implementation Date:
This change will be implemented immediately upon approval by the FPKIPA and incorporation into the FBCA CP.

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:
There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG:	18 November 2005
Date CPWG recommended approval:	9 December 2005
Date Presented to FPKI PA:	13 December 2005
Date of approval by FPKI PA:	13 December 2005