FBCA Policy Change Proposal Number: 2012-01

To: Federal PKI Policy Authority

From: CPWG

Subject: Proposed modifications to the Federal Bridge Certificate Policy

Date: March 1, 2012

Title: Updates to Certificate Policy to RA & CMS Audit Requirements

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the Federal Bridge Certificate Policy Version 2.25, December 9, 2011

Submitter's Contact Information:

Certificate Policy Working Group

Change summary: This change adds clarification about audit requirements for Registration Authorities (RA), Card Management Systems (CMS), and other PKI system components that may be managed by organizations other than the CA Owner.

Background: Due to recent incidents where RAs violated certificate policy and RA procedures, there were questions raised about which organization has responsibility for auditing the RA function when an agency uses an SSP, but performs some of the RA functions within the agency. Therefore, it was agreed that changes were needed in the Common and FBCA certificate policies to provide clarification about audit responsibilities concerning PKI system components that may be managed by organizations other than the CA Owner.

Issue

In order to ensure all PKI system components are compliant with certificate policy, clarification is needed in the certificate policy to ensure all components of a PKI are audited regardless of who manages the functionality of that component.

Specific Changes:

Specific changes are made to sections 1.3.1.6, 8.0, 8.4 and 8.6.

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

Inserting a new section that needs to go after the current section 1.3.1.5 in the CP

1.3.1.6 Entity PKI Policy Management Authority

Entity PKIs (including other Bridges) that are cross certified with the Federal Bridge shall identify an individual or group that is responsible for maintaining the entity PKI CP and for ensuring that all Entity PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with the entity PKI CP. This body is referred to as Entity PKI Policy Management Authority (PMA) within this CP.

8. COMPLIANCE AUDIT & OTHER ASSESSMENTS

Replace second paragraph in 8.0 with:

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.

~~Entity CAs shall have a compliance audit mechanism in place to ensure that the requirements of their CP/CPS are being implemented and enforced.~~

8.4 Topics Covered by Assessment

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. Components other than CAs may be audited fully or by using a representative sample. If the auditor uses statistical sampling, all PKI components, PKI component managers and operators shall be considered in the sample. The samples shall vary on an annual basis.

8.6 COMMUNICATION OF RESULTS

~~Upon completion, an Audit Compliance Report letter shall be provided to the Federal PKI Policy Authority.~~ On an annual basis, the Entity PKI PMA shall submit an audit compliance package to the Federal PKI Policy Authority. This package shall be prepared in accordance with the "Compliance Audit 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 ~~report~~ 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.

Glossary

Policy Management Authority – The individual or group that is responsible for maintaining the entity PKI CP and for ensuring that all Entity PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with the entity PKI CP

Estimated Cost:
This change adds detail to audit expectations and may have a cost associated with updating audit procedures to comply.

Implementation Date:
This change will be effective immediately upon approval by the FPKIPA and incorporation into the FBCA CP. Implementation will occur upon the next regularly scheduled audit following incorporation into the FBCA CP.

Prerequisites for Adoption:
Combine the *Triennial Compliance Audit Requirements* and *FPKI Auditor Letter of Compliance* template into a single *Compliance Audit Requirements* document.

Plan to Meet Prerequisites:
CPWG will propose a new *Compliance Audit Requirements* document.

Approval and Coordination Dates:
Date presented to CPWG: December 1 and 20, 2011; March 1, 2012
Date Presented to FPKIPA: April 10, 2012
Date of approval by FPKIPA: April 10, 2012