Common Policy Change Proposal Number: 2012-01

To: Federal PKI Policy Authority

From: CPWG

Subject: Proposed modifications to the Common Policy Certificate Policy

Date: March 22, 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 Common Policy Certificate Policy Version 1.17, 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 1.3.1.5, 8.0, 8.1, 8.4, 8.5, 8.6 and the Glossary.

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

1.3.1.5 ~~Agency~~ Policy Management Authority

Each organization that provides PKI services under this policy shall identify an individual or group that is responsible for maintaining the Shared Service Provider's (SSP) CPS and for ensuring that all SSP PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with the SSP CPS and this CP. This body is referred to as the SSP PMA within this CP.

Agencies that ~~operate a CA under this policy, or~~ contract for the services of a CA under this policy, shall establish a management body to manage any agency-operated components (e.g., RAs or repositories) and resolve name space collisions. This body shall be referred to as an Agency Policy Management Authority, or Agency PMA.

An Agency PMA is responsible for ensuring that all Agency operated PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with this CP and the applicable CPS and shall serve as the liaison for that agency to the FPKIPA and the SSP PMA.

8. COMPLIANCE AUDIT & OTHER ASSESSMENTS

CAs operating under this policy shall have a compliance audit mechanism in place to ensure that the requirements of their CPS are being implemented and enforced. The SSP 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.

8.1. **Frequency or Circumstanced of Assessment**

CAs and RAs operating under this policy shall be subject to a periodic compliance audit at least once per year in accordance with the "Compliance Audit Requirements" document~~. 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/.

8.4 Topics Covered by Assessment

The purpose of a compliance audit shall be to verify that a CA ~~and its recognized RAs~~ operated by an SSP and all RAs of that CA compl~~y~~ with all the requirements of the current versions of ~~this~~the FCPCA CP and the ~~CA~~SSP's CPS. All aspects of the CA/RA operation shall be subject to compliance audit inspections. 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.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

…

- The compliance auditor shall notify the responsible party promptly ~~parties identified in section 8.6 of the discrepancy~~; and
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the FPKIPA and appropriate Agency PMA.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the FPKIPA may decide to temporarily halt operation of the CA or RA, to revoke a certificate issued to the CA or RA, or take other actions it deems appropriate. The FPKIPA will develop procedures for

making and implementing such determinations.- In accordance with section 8.1, a compliance audit may be required to confirm the implementation and effectiveness of the remedy.-

8.6 COMMUNICATION OF RESULTS

On an annual basis, an Auditor Letter of Compliance ~~Report~~, prepared in accordance with the "Compliance Audit Requirements" document, on behalf of an Agency PMA shall be provided to the SSP ~~entity responsible for CA operations. The Audit Compliance Report and identification of corrective measures shall be provided to both the FPKIPA and (where applicable) the Agency PMA within 30 days of completion. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.~~

On an annual basis, the SSP PMA shall submit an audit compliance package to the FPKIPA. This package shall be prepared in accordance with the "Compliance Audit Requirements" document and includes an assertion from the SSP PMA that all PKI components have been audited - including any components that may be separately managed and operated. The report shall identify the versions of this 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 (PMA) – Body established to oversee the creation and update of certificate policies, review certificate practice statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. The individual or group that is responsible for maintaining the SSP CPS and for ensuring that all SSP PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with this CP and the SSP CPS.

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 Common Policy CP. Implementation will occur upon the next regularly scheduled audit following incorporation into the FCPCA 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: March 22, 2012

Date Presented to FPKIPA: April 10, 2012
Date of approval by FPKIPA: April 10, 2012