



**Common Policy CP Change Proposal Number: 2010-04**

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

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

X.509 Certificate Policy for the U. S. Federal PKI Common Policy Framework Version 3647 – 1.7, April 15, 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 ~~strikethrough~~ text:

**8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT**

*Modify Section 8.1 as follows:*

CAs and RAs operating under this policy shall be subject to a periodic compliance audit at least once per year. 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/>

~~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.

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.

Further, the Federal PKI Policy Authority has the right to require aperiodic compliance audits of CAs operating under this policy. 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 purpose of a compliance audit shall be to verify that a CA and its recognized RAs comply with all the requirements of the current versions of this CP and the CA's CPS. All aspects of the CA/RA operation shall be subject to compliance audit inspections.

Where permitted by section 8.1, CAs operating under this policy 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 Common Policy CA.

### **Risk/Impact:**

None identified.

### **Implementation Date:**

This change will be implemented immediately upon approval by the FPKIPA and incorporation into the Common Policy CP.

**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