



Common Policy Change Proposal Number: 2008-01

To: Federal PKI Policy Authority
From: Certificate Policy Working Group
Subject: Proposed modifications to the Common Policy
Date: April 3, 2008
Title: § 8.3 Assessor's Relationship to Assessed Entity

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 1.3, December 12, 2007.

Change Advocate's Contact Information:

Name: John Cornell
Organization: FPKI-CPWG
Telephone number: 202-501-1598
E-mail address: john.cornell@gsa.gov

Organization requesting change: CPWG

Change summary: Clarification on what constitutes auditor independence.

Background: In reviewing a compliance audit, the CPWG encountered an instance in which the same firm that was conducting the compliance audit had also (through an acquired company) also written significant portions of the entity's CP and CPS. The CPWG was of the opinion that this would have the compliance auditor standing in judgment of their own work in drafting the CP and CPS, which called objectivity into question.

Specific Changes: Specific changes are made to the following section:

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

Common Policy CP

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor either shall be a private firm, that is independent from the entities (CA and RAs) being audited, or it shall be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation. An example of the latter situation may be an Agency inspector general. To insure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's CA Facility or certificate practices statement. The Federal PKI Policy Authority shall determine whether a compliance auditor meets this requirement.

The agency PMA is responsible for identifying and engaging a qualified auditor of agency operations implementing aspects of this CP.

Estimated Cost:

No cost to the Federal Bridge CA.

Risk/Impact: Low risk – impact will improve integrity of audit function.

Implementation Date:

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

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG: 3 April 2008

Date presented to FPKI PA: 8 April 2008

Date of approval by FPKI PA: 25 July 2008