



C4CP Change Proposal Number: 2008-01

To: Federal PKI Policy Authority

From: Certificate Policy Working Group

Subject: Proposed modifications to the Citizen and Commerce Class Common Certificate Policy

Date: February 7, 2008

Title: Aligning records archival requirements with NIST SP 800-63

Version and Date of Certificate Policy Requested to be changed:

Citizen and Commerce Class Common Certificate Policy Version 2.0, December 4, 2007.

Change Advocate's Contact Information:

Name: David Cooper

Organization: NIST

Telephone number: 301-975-3194

E-mail address: david.cooper@nist.gov

Organization requesting change: Federal PKI Policy Authority

Change summary: This change proposal imposes the archiving requirements that appear in NIST Special Publication 800-63 for E-Authentication Level 2.

Background: The C4CP was intended to satisfy the requirements for E-Authentication Level 2 as specified in NIST Special Publication 800-63, *Electronic Authentication Guideline*. A review of the C4CP by one of the authors of SP 800-63 has determined that the C4CP satisfies all of the requirements for E-Authentication Level 2 except for the records retention requirements. This change proposal imposes the records retention requirements on Entity CAs that are mandated by SP 800-63 for E-Authentication Level 2. Section 7.2.2, Records Retention Requirements, of SP 800-63 states:

A record of the facts of registration (including revocation) shall be maintained by the CSP or its representative. The minimum record retention period for registration data for Level 2 credentials is seven years and six months beyond the expiration or revocation (whichever is later) of the credential. CSPs operated by or on behalf of executive branch agencies must also follow either the General Records Schedule established by the National Archives and Records Administration or an agency-specific schedule as applicable. All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities. A minimum record retention period for registration data is:

- For Levels 2, and 3, seven years and six months beyond the expiration, and

- For Level 4, ten years and six months beyond the expiration.

Specific Changes: Specific changes are made to the following section: 5.5

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

5.5 Records Archival

Entity CAs shall maintain a record of the facts of registration (including revocation) for a minimum of seven years and six months beyond the expiration or revocation (whichever is later) of the certificate. Entities shall also comply with their respective records retention policies in accordance with whatever laws apply to those Entities.

Estimated Cost:

No cost to the C4CA.

Risk/Impact:

This change proposal reduces risk by ensuring that information necessary to verify that a certificate was properly issued has been archived.

Implementation Date:

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

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG: February 7, 2008

Date Presented to FPKI PA: March 11, 2008

Date of approval by FPKI PA: March 11, 2008