



Federal Common Policy Change Proposal Number: 2010-02

To: Federal PKI Policy Authority

From: Certificate Policy Working Group

Subject: Proposed modifications to the Federal Common Policy Framework Certificate Policy

Date: December 3, 2009

Title: Remote Administration of Certification Authorities

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the Federal PKI Common Policy Framework Version 3647-1.7, April 15, 2009

Change Advocate's Contact Information:

Name: Charles R. Froehlich

Organization: FPKI Certificate Policy Working Group / U.S. Department of State

Telephone number: 202-203-5069

E-mail address: FroehlichCR@state.gov / Charles.Froehlich@ManTech.com

Organization requesting change: Federal PKI Certificate Policy Working Group (FPKI CPWG) and U.S. Department of State

Background: Currently, the FCPF CP is silent on the subject of remote administration of the CAs. Changes in networking, physical location, staffing, and CA operations necessitate outlining general guidelines for the FCPF and subordinate CAs to implement remote administration without degrading the operational and security requirements imposed by the overall FCPF CP. These guidelines are intended to reinforce those requirements without being overly specific to allow for varying implementations by individual entities.

Change summary: This change will permit the remote administration of Certification Authorities and associated repositories by the appropriate Trusted Role personnel, such that the operational and security requirements of the FCPF CP are maintained.

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

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

2.1 REPOSITORIES

All CAs that issue certificates under this policy are obligated to post all CA certificates issued by or to the CA and CRLs issued by the CA in a directory that is publicly accessible through the Lightweight Directory Access Protocol (LDAP) and Hypertext Transport Protocol (HTTP). Specific requirements are found in Shared Service Provider Repository Service Requirements [SSP REP]. CAs may optionally post subscriber certificates in this directory in accordance with agency policy, except as noted in section 9.4.3. To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanisms to prevent unauthorized modification or deletion of information.

2.4 ACCESS CONTROLS ON REPOSITORIES

The CA shall protect information not intended for public dissemination or modification. CA certificates and CRLs in the repository shall be publicly available through the Internet. Direct and/or remote access Access to other information in the CA repositories shall be determined by agencies pursuant to their authorizing and controlling statutes. The CPS shall detail what information in the repository shall be exempt from automatic availability and to whom, and under which conditions, the restricted information may be made available.

5.1 PHYSICAL CONTROLS

[Text omitted for expedience]

All the physical control requirements specified below apply equally to the FCPF and subordinate CAs, and any remote workstations used to administer the CAs except where specifically noted.

5.1.1 Site Location & Construction

The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CAs, shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.

5.1.2.1 Physical Access for CA Equipment

At a minimum, the physical access controls for CA equipment, as well as remote workstations used to administer the CAs, shall—

- *[Text omitted for expedience]*
- Require two person physical access control to both the cryptographic module and computer systems.

When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA equipment shall be placed in secure containers. Activation data shall be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be

stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA.

A security check of the facility housing the CA equipment or remote workstations used to administer the CAs shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

5.4.4 Protection of Audit Logs

The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing. CA system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data. Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access). Security audit data shall be moved to a safe, secure storage location separate from the ~~CA equipment~~ location where the data was generated.

6.5.1 Specific Computer Security Technical Requirements

[Text omitted for expedience]

For remote workstations used to administer the CAs, the computer security functions listed below are required:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see section 5.4)
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

All communications between any PKI trusted role and the CA shall be authenticated and protected from modification

6.7 Network Security Controls

[Text omitted for expedience]

Directories, ~~and~~ certificate status servers, and remote workstations used to administer the CAs shall employ appropriate network security controls. Any network software present shall be necessary to the functioning of the equipment.

The CA shall establish connection with a remote workstation used to administer the CA only after successful authentication of the remote workstation at a level of assurance commensurate with that of the CA.

Estimated Cost:

No cost to the Federal Common Policy Framework apart from internal implementation.

Risk/Impact:

Since this is a new option, there is no impact to other CAs who would otherwise not allow or conduct remote administration of CAs.

Implementation Date:

This change will be implemented immediately upon approval by the FPKIPA and incorporation into the Federal Common Policy Framework 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: December 3, 2009

Date Presented to FPKI PA: January 12, 2010

Date of approval by FPKI PA: January 12, 2010