



FBCA Certificate Policy Change Proposal Number: 2010-01

To: Federal PKI Policy Authority

From: Certificate Policy Working Group

Subject: Proposed modifications to the Federal Bridge 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 Bridge Certification Authority (FBCA CP)

Version 2.12, February 11, 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 FBCA 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 FBCA and cross certified CAs to implement remote administration without degrading the operational and security requirements imposed by the overall FBCA 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 FBCA CP are maintained.

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

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

2.1.1 FBCA Repository Obligations

The FPKI Management Authority may use a variety of mechanisms for posting information into a repository as required by this CP. These mechanisms at a minimum shall include:

- [Text omitted for expedience], and
- Access control and communication mechanisms when needed to protect repository information as described in later sections.

2.4 ACCESS CONTROLS ON REPOSITORIES

The FPKI Management Authority and Entity CAs shall protect any repository information not intended for public dissemination or modification. Certificates and certificate status information in the FBCA repository shall be publicly available through the Internet.

Direct and/or remote access Access to information in Entity CA repositories shall be determined by the Entity pursuant to the rules and statutes that apply to that entity. Certificates and certificate status information in the Entity repository should be publicly available through the Internet wherever reasonable. At a minimum, the Entity repositories shall make CA certificates and CRLs issued by the Entity PKI and CA certificates issued to the Entity PKI available to Federal Relying Parties.

5.1 PHYSICAL CONTROLS

All CA equipment including CA cryptographic modules shall be protected from unauthorized access at all times.

All the physical control requirements specified below apply equally to the FBCA and Entity 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 FBCA and Entity 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 FBCA and Entity CA equipment and records.

5.1.2.1 Physical Access for CA Equipment

The FBCA and Entity CA equipment, to include remote workstations used to administer the CAs, shall always be protected from unauthorized access. The security mechanisms shall be commensurate with the level of threat in the equipment environment. Since the FBCA must plan to issue certificates at all levels of assurance, it shall be operated and controlled on the presumption that it will be issuing at least one High Assurance certificate.

[Text omitted for expedience]

In addition to those requirements, the following requirements shall apply to CAs that issue Medium, Medium Hardware, or High Assurance certificates:

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

Removable cryptographic modules, activation information used to access or enable cryptographic modules, and other sensitive CA equipment shall be placed in secure containers when not in use. Activation data shall either be 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 FBCA or Entity CA equipment or remote workstations used to administer the CAs (operating at the Basic Assurance level or higher) shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- [Text omitted for expedience]

5.4.4 Protection of Audit Logs

The off-site storage location for audit logs shall be a safe, secure 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]

Entity CAs, RAs, directories, remote workstations used to administer the CAs, and certificate status servers shall employ appropriate network security controls. Networking equipment shall turn off unused network ports and services. 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 Bridge CA apart from internal implementation.

Risk/Impact:

Since this is a new option, there is no impact to other cross-certified CAs or Bridges 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 Bridge 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