**FBCA Certificate Policy Change Proposal Number: 2007-02**

| | |
|---|---|
| **To:** | **Federal PKI Policy Authority** |
| **From:** | Certificate Policy Working Group |
| **Subject:** | Proposed modifications to the Federal Bridge Certificate Policy |
| **Date:** | May 03, 2007 |
| **Title:** | Clarification on multiparty physical access control in Physical Access for CA Equipment |

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

X.509 Certificate Policy for the Federal Bridge Certificate Policy Version 2.3, March 14, 2007.

**Change Advocate's Contact Information:**

Name: Sally Caldwell
Organization: Department of State
Telephone number: 202-203-7808
E-mail address: caldwellsx@state.gov

**Organization requesting change**: Federal PKI Policy Authority

**Background**: Federal agencies are experiencing severe resource shortfalls in funding, staffing, and equipment. The pace of operations is increasing, resulting in the need to identify unique ways of accomplishing the mission without sacrificing capabilities or security. In such cases, policies and procedures must eliminate confusion.

**Change summary**: paragraph 5.1.2.1 "Physical Access for CA Equipment" and Paragraph 5.2.2, "Number of Persons Required per Task," need further clarification for the multiparty physical access to the CA computer system and cryptographic module so as to address situations where the CA operational site does not segregate CA specific equipment from other equipment needed for a Certification Practice.

The Auditor trusted role is presumably subject to the same standards of trustworthiness as Administrators, Officers, and Operators. It is proposed to add language in paragraph 5.1.2.1 by including a practice note that explains that multiparty physical access control is attained by any combination of two or more trusted roles, as long as tasks being conducted are segregated in accordance with the policy requirements specified for each trusted role.

It is further proposed to add language in paragraph 5.2.2 to specifically indicate that the other stated requirements of that paragraph do not apply to physical access controls.

**Specific Changes:** Specific changes are made to the following sections; insertions are underlined, deletions are in ~~strikethrough~~:

*5.1.2.1 Physical Access for CA Equipment*

[…]

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

- Ensure manual or electronic monitoring for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Require two person physical access control to both the cryptographic module and computer system

Practice Note: Multiparty physical access control to CA equipment can be achieved by any combination of two or more trusted roles (see Section 5.2.2) as long as the tasks being conducted are segregated in accordance with the requirements and duties defined for each trusted role. As an example, an Auditor and an Operator might access the site housing the CA equipment to perform a tape backup, but only the Operator may perform the tape backup.

[…]

**5.2.2 Number of Persons Required per Task**

[…]

Where multiparty control for logical access is required, at least one of the participants shall be an Administrator. All participants must serve in a trusted role as defined in Section 5.2.1. Multiparty control for logical access shall not be achieved using personnel that serve in the Auditor Trusted Role.

Physical access to the CAs does not constitute a task as defined in this section. Therefore, two-person physical access control may be attained as required in Section 5.1.2.1.

[…]

**Estimated Cost:**

No cost to the FBCA or FBCA cross-certified entities.

**Implementation Date:**

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

**Prerequisites for Adoption:**

There are no prerequisites.

**Plan to Meet Prerequisites:**

There are no prerequisites.

**Approval and Coordination Dates:**

Date presented to CPWG: May 3, 2007

Date Presented to FPKI PA:  June 12, 2007
Date of approval by FPKI PA:  June 12, 2007