FBCA Policy Change Proposal Number: 2007-03

To:	**Federal PKI Policy Authority**
From:	Certificate Policy Working Group
Subject:	Proposed modifications to the Federal Bridge Certificate Policy
Date:	May 10, 2007
Title:	SAFE Harmonization Policy Change Recommendations

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the Federal Bridge Certificate Policy Version 2.4, June 13, 2007.

Change Advocate's Contact Information:

Name: Dave Cooper
Organization: NIST
Telephone number: 301-975-3194
E-mail address: david.cooper@nist.gov

Organization requesting change: Federal PKI Policy Authority

Change summary: On March 15, 2007, the CPWG hosted a meeting with the SAFE Bridge policy management team to discuss the SAFE reverse mapping and policy harmonization with the FBCA CP. At this meeting a good number of the issues were resolved. The CPWG agreed to take the residual issues under consideration for resolution. A meeting for this purpose was held on April 24, 2007 and the following policy changes are recommended.

Background: A line-by-line comparison was conducted between the FBCA Policy and the SAFE Certificate Policy. From this comparison several areas for improvement were identified in the Federal Bridge Policy. The recommended changes add clarity to the FBCA Certificate Policy and the CPWG believes these changes are not substantive and will not affect the FBCA cross-certified Entities.

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

2.4 5.7.3 6.2.1 6.2.4.4 6.7

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

2.4 Access Controls on Repositories

The FPKI Operational Authority and Entity CAs shall protect any repository information not intended for public dissemination or modification.

[…]

5.7.3 Entity (CA) Private Key Compromise Procedures

Section 5.7.3
If the FBCA or Entity CA signature keys are compromised or lost (such that compromise is possible even though not certain):

- The Federal PKI Policy Authority and all of its member entities shall be notified so that entities may issue CRLs revoking any cross-certificates issued to the compromised CA;
- A new FBCA or Entity CA key pair shall be generated by the FBCA or Entity CA in accordance with procedures set forth in the FBCA or Entity CPS; and
- New FBCA or Entity CA certificates shall be issued to Entities also in accordance with the FBCA or Entity CPS.

If the CA distributes its key in a self-signed certificate, the new self-signed certificate shall be distributed as specified in Section 6.1.4.

The FPKI Operational Authority or Entity CA governing body shall also investigate and report to the Federal PKI Policy Authority what caused the compromise or loss, and what measures have been taken to preclude recurrence.

6.2.1 Cryptographic Module Standards & Controls

[…]

Assurance Level	**CA & CSS**	**Subscriber**	**RA**

[…]

6.2.4.4 Backup of CSS Private Key

CSS private keys may be backed up. If backed up, all copies shall be accounted for and protected in the same manner as the original.

6.7 Network Security Controls

[…]

Entity CAs, RAs, directories, 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.

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: 15 May 2007
Date Presented to FPKI PA: 10 July 2007
Date of approval by FPKI PA: 10 July 2007