



Federal Bridge CA Certificate Policy Change Proposal

Change Number: 2004-01

To: Federal PKI Policy Authority
From: FPKI Certificate Policy Working Group
Subject: Proposed modifications to the FBCA CP
Date: 08 June 2004

Title: Clarify FBCA requirements for online FBCA internal and border directories

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), dated 10 September 2002.

Change Advocates Contact Information:

Name: Tim Polk

Organization: NIST

Telephone number: (301) 975-3348

E-mail address: tim.polk@nist.gov

Name: John Cornell

Organization: GSA

Telephone number: (202) 501-1598

E-mail address: john.cornell@gsa.gov

Organization requesting change: FBCA Operational Authority (OA)

Change summary:

The FBCA CPWG recommends the following changes to address the current configuration and automatic publication of CRLs to the FBCA Border directory.

Background: The Federal PKI Policy Authority (FPKIPA) met on 8 June 2004 and the FBCA OA informed the CPWG and the FPKIPA members that the current wording of the FBCA CP, dated 10 September 2002, would make the current operations of the directories supporting the FBCA non-compliant. Therefore, the FBCA OA suggested that the changes suggested in the change proposal be made immediately to the FBCA CP.

Specific Changes:

Replace section 6.7, paragraph 1...

The FBCA and FBCA Internal Directory shall be connected within the Bridge membrane. They will not be connected to any network external to the Bridge membrane. The FBCA Border Directory shall be connected to the Internet and provide continuous service (except, when necessary, for brief periods of maintenance or backup). Information will be transported from the

Internal Directory to the Border directory using manual mechanisms, and all such information will be digitally signed (certificates and CARLs). The FBCA Border Directory shall be protected by a network guard, firewall or filtering router to guard against denial of service and intrusion attacks.

...with the following text:

The FBCA and FBCA Internal Directory shall be connected within the Bridge membrane. The Bridge membrane will be connected with the FBCA Border directory through a firewall. The FBCA Border Directory shall be connected to the Internet and provide continuous service (except, when necessary, for brief periods of maintenance or backup). Information will be transported from the Internal Directory to the Border directory using automatic mechanisms, and all such information will be digitally signed (certificates and CARLs). The firewall will restrict connections to those initiated by the Internal directory to the Border directory. The FBCA Border Directory shall be protected from Internet systems by a network guard, firewall or filtering router to guard against denial of service and intrusion attacks.

Estimated Cost:

There is no financial cost associated with implementing this change.

Implementation Date:

This change will be implemented immediately.

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG: 8 June 2004

Date CPWG recommended approval: 8 June 2004

Date Presented to FPKI PA: 8 June 2004

Date of approval by FPKI PA: 8 June 2004