



Federal Bridge CA Certificate Policy Change Proposal
Change Number: 2003-02

To: Federal PKI Policy Authority
From: FPKI Certificate Policy Working Group
Subject: Proposed modifications to the FBCA Certificate Policy
Date: 20 September 2004

Title: Clarify FBCA requirements to facilitate cross certification with the State of Illinois

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 as amended by FBCA Change Proposals 2002-01 through 2002-05.

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: CPWG

Change summary:

Background:

The representative party from the FPKI Certificate Policy Working Group (CPWG) met on May 30, 2003, at the National Institute of Technology and Standards facility located in Gaithersburg, Maryland. The CPWG Co-Chair and the State of Illinois representative, Georgia Marsh presented the open issues identified at this CPWG meeting. To facilitate

the mapping of State of Illinois and FBCA certificate policies, the FPKI CPWG has proposed modifications to address this issue.

The FPKI CPWG has requested that the State of Illinois review these proposed modifications to the FBCA CP. If these changes are considered sufficient, the FPKI CPWG will present a corresponding Certificate Policy Change Proposal to the FPKI Policy Authority at its monthly meeting.

The proposed text change appears as *red underlined text*.

Specific Changes:

Policy Mapping MatrixItem 117

Problem: The FBCA CP requires that only a single copy of the CA signature key be made. The FBCA CP did not consider that some organizations desire to have multiple copies of the CA signature key for key recovery, disaster capabilities, redundant sites and geographical logistics.

To ensure that signature keys are controlled and protected, the CPWG proposes to revise FBCA CP, Section 6.2.4.1.

Proposal:

The first paragraph in FBCA CP, Section 6.2.4.1, states “A single copy of the signature key may be stored at the FBCA or CA location, respectively.” (as set forth below):”

Current:

6.2.4.1 Backup of FBCA and Entity CA private signature key

If backed up, the FBCA and Entity CA private signature keys shall be backed up under the same multi-person control as the original signature key. A single copy of the signature key may be stored at the FBCA or CA location, respectively. A second copy may be kept at the FBCA or CA backup location. Procedures for FBCA private signature key backup shall be included in the FBCA CPS.

Proposed Change:

If backed up, the FBCA and Entity CA private signature keys shall be backed up under the same multi-person control as the original signature key. A controlled copy or copies of the CA signature key may be stored at various FBCA or Entity CA locations, as long as all copies of the signature key are controlled, accounted for and protected from unauthorized access. These multiple copies may be kept at the FBCA or CA backup location under the same multiple person access rules and storage requirements that apply to operational and backup signature keys. Procedures for FBCA private signature key backup shall be included in the FBCA CPS.

Estimated Cost:

There is no financial cost associated with implementing these changes.

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:	30 May 2003
Date CPWG recommended approval:	30 August 2004
Date Presented to FPKI PA:	14 September 2004
Date of approval by FPKI PA:	14 September 2004