



FBCA CP Change Proposal Number: 2010-08

To: Federal PKI Policy Authority
From: FPKI Certificate Policy Working Group
Subject: Proposed modifications to the FBCA Certificate Policy
Date: October 20, 2010
Title: Change to FBCA CP to clarify requirement to support CA Key Rollover

Version and Date of Certificate Policy Requested to be changed: X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) Version 2.19, October 15, 2010.

Change Advocate's Contact Information:

Name: Cheryl Jenkins
Organization: GSA
Telephone number: 202-577-1441
E-mail address: cheryl.jenkins@gsa.gov

Organization requesting change: FPKI Management Authority

Change summary: This change proposal requires Affiliate PKIs cross certified with the FBCA to continue to interoperate with the FBCA after the FBCA performs a key rollover.

Background:

October 15, 2007, the Federal PKI Management Authority performed a key rollover for the Common Policy CA. Following the key rollover, one of the SSPs could not interoperate with the new Common Policy CA certificate because the certificate violated the SSP's definition of Name Uniqueness. The SSP's definition of Name Uniqueness does not allow different certificate with the same DN and different keys, even in the case of a CA key rollover or certificate renewal.

The SSP vendor involved is now cross certified with the FBCA. When the Management Authority performs future key rollovers, clarification is required to the FBCA CP to ensure PKIs cross certified with the FBCA continue to interoperate after a key rollover is performed.

Specific Changes:

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

3.1.5 Uniqueness of Names

Name uniqueness must be enforced by the FBCA and Entity CAs.

The Federal PKI Policy Authority is responsible for ensuring name uniqueness in certificates issued by the FBCA. Entity CAs shall identify the authority that is responsible for ensuring name uniqueness in certificates issued by the entity CA. Name uniqueness is not violated when multiple certificates are issued to the same entity.

4.7 CERTIFICATE RE-KEY

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. Re-key of a certificate does not require a change to the subjectName and does not violate the requirement for name uniqueness.

5.6 KEY CHANGEOVER

To minimize risk from compromise of a CA's private signing key, that key may be changed often; from that time on, only the new key will be used for certificate signing purposes. The older, but still valid, public key will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs that cover certificates signed with that key, then the old key must be retained and protected.

For the FBCA, key changeover procedures will establish key rollover certificates where a certificate containing the old public key will be signed by the new private key, and a certificate containing the new public key will be signed by the old private key.

Entity CAs cross certified with the FBCA must be able to continue to interoperate with the FBCA after the FBCA performs a key rollover, whether or not the FBCA DN is changed.

Entity CAs either must establish key rollover certificates as described above or must obtain a new CA certificate for the new public key from the issuers of their current certificates.

Practice Note: For example, a CA in a hierarchical PKI may obtain a new CA certificate from its superior CA rather than establish key rollover certificates.
--

Estimated Cost:

There is no cost expected for Federal Agencies.

Implementation Date:

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

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

Not Applicable.

Approval and Coordination Dates:

Date presented to CPWG:	October 26, 2010
Date presented to FPKIPA:	November 9, 2010
Date of approval by FPKIPA:	December 14, 2010