FBCA Certificate Policy Change Proposal Number: <2016-03>

To: Federal PKI Policy Authority (FPKIPA)
From: FPKI Certificate Policy Working Group (CPWG)
Subject: Proposed modifications to the FBCA Certificate Policy
Date: 12 September 2016

Title: Allow alternate FBCA key change procedures

Version and Date of Certificate Policy Requested to be changed: X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) Version 2.29, May 20, 2016

Change Advocate's Contact Information:

Name: Darlene Gore
Organization: GSA
Telephone number: 703-306-6109
E-mail address: Darlene.Gore@gsa.gov

Organization requesting change: FPKI Certificate Policy Working Group

Change summary: Update the FBCA CP to allow the FBCA to use a new superior certificate rather than key rollover certificates in conjunction with a Directory Name change.

Background:

During the 2005 timeframe, when the FBCA was operated using an Entrust CA product, the FBCA Certificate Policy was amended to state that the FBCA will create key rollover certificates when it does a key change. This was fully supported by the Entrust CA product which fully supports a CA Rekey by generating a new public/private key pair, creates rollover certificates between the new and old keys and then generates CRLs signed by both the old and new keys until the old self-signed certificate expires. However, the FBCA as currently operated performs a rekey in a similar fashion to some of the FPKI Affiliate CAs by establishing a new instantiation of the FBCA using a variation of the Directory Name. Creating rollover certificates between the old and new FBCA instantiations creates the possibility of two different paths to the Federal Common Policy CA which is the trust anchor for the federal government and therefore the superior CA to the FBCA.

This change proposal allows the FPKIMA to perform a key change for the FBCA in a similar fashion as allowed by the FBCA CP for other CAs which are not meant to be used as a trust anchor.

Specific Changes:

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

5.6 KEY CHANGEOVER

…
For the FBCA, key changeover procedures will either

1) 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, or

2) if the DN is changed at the same time as the key, new cross certificates shall be established with the Federal Common Policy CA.

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 to implement this change.

Implementation Date:

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

Prerequisites for Adoption:

N/A

Plan to Meet Prerequisites:

N/A.

Approval and Coordination Dates:

Date presented to CPWG:	9/16/16
Date presented to FPKIPA:	9/28/16

Date of approval by FPKIPA: 10/5/16