FBCA Certificate Policy Change Proposal Number: <2016-02>

To: Federal PKI Policy Authority (FPKIPA)
From: FPKI Certificate Policy Working Group (CPWG)
Subject: Proposed modifications to the FBCA Certificate Policy
Date: 1 August 2016

Title: Allow for Long-Term CRL for retired CA key

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 a long term CRL when a CA retires a key after performing a key changeover to align with the FPKI CPS.

Background:

During the annual audit, the FPKI Auditor found a disparity between the FBCA CP and the FPKI CPS. The FBCA CP does not specify the activities of the CA when a CA key is retired. This change proposal will specify two approved activities 1) continue to issue a CRL until all entries in the CRL have expired or 2) issue a long-term CRL.

Specific Changes:

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

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.

After a CA performs a Key Changeover, the CA may continue to issue CRLs with the old key until all certificates signed with that key have expired. As an alternative, after all certificates signed with that old key have been revoked, the CA may issue a final long-term CRL using the old key, with a nextUpdate time past the validity period of all issued certificates. This final CRL shall be available for all relying parties until the validity period of all issued certificates has past. Once the last CRL has been issued, the old private signing key of the CA may be destroyed.

5.8 CA & RA TERMINATION

In the event of termination of the FBCA operation, certificates signed by the FBCA shall be revoked and the FPKIPA shall advise entities that have entered into MOAs with the FPKIPA that FBCA operation has terminated so they may revoke certificates they have issued to the FBCA. Prior to FBCA termination, the FPKIMA shall provide all archived data to an archival facility. Any issued certificates that have not expired, shall be revoked and a final long term CRL with a nextUpdate time past the validity period of all issued certificates shall be generated. This final CRL shall be available for all relying parties until the validity period of all issued certificates has past. Once the last CRL has been issued, the private signing key(s) of the FBCA will be destroyed.

Entities will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought in the event the FBCA is terminated.

In the event that an Entity CA terminates operation, the Entity shall provide notice to the FBCA prior to termination.

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:

CAs may need to update their CPS to allow for these two methods.

Plan to Meet Prerequisites:

N/A.

Approval and Coordination Dates:

Date presented to CPWG:	8/16/2016
Date presented to FPKIPA:	9/15/16
Date of approval by FPKIPA:	9/23/16