FCPCA 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 FCPCA 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 U.S. Federal PKI Common Policy Framework Version 1.24, May 7, 2015

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 FCPCA 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 FCPCA CP and the FPKI CPS. The FCPCA 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 to sign CA and subscriber certificates. If the old private key is used to sign OCSP responder certificates or CRLs that cover certificates signed with that key, 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 As an alternative, after all certificates signed with that old key have been revoked, the CA may issue a final long-term CRL using the old key, with a nextUpdate time past the validity period of all issued certificates.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 OR RA TERMINATION

When a CA operating under this policy terminates operations before all certificates have expired, the CA signing keys shall be surrendered to the FPKIPA.

This section does not apply to CAs that have ceased issuing new certificates but are continuing to issue CRLs until all certificates have expired. Such CAs are required to continue to conform with all relevant aspects of this policy (e.g., audit logging and archives).

~~This section does not apply to CAs that have ceased issuing new certificates but are continuing to issue CRLs until all certificates have expired. Such CAs are required to continue to conform with all relevant aspects of this policy (e.g., audit logging and archives).~~

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 CA to be terminated will be destroyed.

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 FCPCA 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