FCPF Certificate Policy Change Proposal Number: 2018-08

To: Federal PKI Policy Authority (FPKIPA)

From: FPKI Certificate Policy Working Group (CPWG)

Subject: Proposed modifications to the FCPF Certificate Policy

Date: November 2, 2018

Title: Change Requirement for Destruction of Private Signing Key(s) following CA Termination

Version and Date of Certificate Policy Requested to be changed:

- *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (FCPF) Version 1.28 April 4, 2018*

Change Advocate's Contact Information: FPKIPA

Organization requesting change: FPKI Policy Authority

Change summary: Update the FCPF CP to add specificity regarding the treatment of CA private keys and escrowed private keys following CA termination. Specifically, due to technical constraints and a desire to archive all artifacts, permit CA private keys to be retained in lieu of zeroization, so long as they are protected in a manner comparable to their protection while active.

Background:

The FCPF CP currently requires that when any CA operating under that policy terminates operation, once the last CRL has been issued, the private signing key(s) of the CA to be terminated, unless said CAs terminate before all certificates issued have expired, in which case the CA signing keys shall be surrendered to the FPKIPA.

It was recently brought to the attention of the CPWG that some Federal agencies and FPKI affiliates are using PKI products where escrowed end entity keys or multiple CA private signing keys are collocated within the same Hardware Security Module (HSM) as the CA private signing keys of a CA to be terminated. In some instances there is either:

a) an inability to destroy the CA private signing key of the CA to be terminated without

also destroying the CA private signing keys of the collocated CAs, or the escrowed end entity keys; and/or

b) an inability to provide adequate assurance that all copies of the CA private signing key of the CA to be terminated, such as those in Disaster Recovery facilities, are destroyed without also destroying the CA private signing keys

In these instances, it is necessary to preserve the CA private signing key of the CA to be terminated in order to preserve the CA private signing keys of the collocated CAs and/or the escrowed end entity keys, even after termination (i.e. expiration or revocation) of the CA.

Additionally, some Federal agencies and FPKI affiliates indicated a need to preserve CA private signing keys for forensic purposes, or as a means for reconstituting a PKI for the purposes of recovering escrowed end entity keys after the CA has been terminated or escrow system taken offline.

Specific Changes:

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

X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (FCPF) Version 1.28 April 4, 2018

5.8 CA OR RA TERMINATION

Whenever possible, the FPKIPA shall be notified at least two weeks prior to the termination of a CA operating under this policy. For emergency termination, CAs shall follow the notification procedures in Section 5.7.

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).

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 or taken offline, designated as "not in use", and protected as stipulated in 5.1.2.1.

Prior to CA termination, the CA shall provide archived data to an archive facility as specified in the CPS. As soon as possible, the CA will advise all other organizations to which it has issued certificates of its termination, using an agreed-upon method of communication specified in the CPS.

Estimated Cost:

TBD

Implementation Date:

TBD

Prerequisites for Adoption:

None

Plan to Meet Prerequisites:

Not Applicable

Approval and Coordination Dates:

Date presented to CPWG:	July 24, 2018
Date change released for comment:	July 26, 2018; September 7, 2018; September 18, 2018
Date approved by PA:	Dec 11, 2018