FPKIPA
Federal Public Key Infrastructure Policy Authority

COMMON Certificate Policy Change Proposal Number: 2018-04

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Identify certificate revocation requirements for Transitive Closure under the COMMON Policy
Date: July 17, 2017

Title: Certificate revocation requirements for Transitive Closure under the COMMON Policy

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

Change Advocate's Contact Information:
Name: Matt King, Vice President, Global Policy
Organization: SAFE-BioPharma Association
Telephone number: 410.271.5624 (m)
E-mail address: MKing@SAFE-BioPharma.org

Organization requesting change: N/A

Change summary: Update the COMMON CP to specify requirements for revoking or verifying certificates that were issued with a compromised RA credential or under otherwise unauthorized circumstances.

Background:

The COMMON CP does not address a revocation use case in which most certificates have been issued properly, but some may have been issued improperly, such as with a compromised key.

When such an event occurs, the OA should investigate the compromise, identify the certificates that were issued with the compromised key, and revoke the certificates that were improperly issued from the compromised key. If some certificates were issued properly during the suspected period of compromise, but some improperly, only the improperly issued certificates must be revoked.

Specific Changes:

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

4.9.1 Circumstances for Revocation

…..

…. Whenever any of the above circumstances are reported, the appropriate authority shall review the circumstances and make a revocation decision. The revocation decision shall be made based on appropriate criteria, to include:

- The nature of the alleged problem;
- The number of Certificate Problem Reports received about a particular Certificate or Subscriber; and
- Relevant legislation.

If it is determined that a private key used to authorize the issuance of one or more certificates may have been compromised, all certificates directly or indirectly authorized by that private key since the date of actual or suspected compromise shall be revoked or shall be verified as appropriately issued.

If it is determined that revocation is required, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

Estimated Cost: The change would incur the cost associated with determining if certificates issued since the date of an actual or suspected compromise have been issued properly or improperly.

Implementation Date: 90 days following publication in the Federal Common Policy CP.

Prerequisites for Adoption: none

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:

Date presented to CPWG: September 20, 2017
Date presented to FPKIPA: November 14, 2017
Date published: May 8, 2018