Federal Bridge 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 BRIDGE Policy
Date: August 17, 2017

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

X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)
Version 2.32 4 April 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 Federal BRIDGE CP to specify requirements for revoking or verifying certificates that were issued with a compromised RA credential or under otherwise unauthorized circumstances.

Background:

Neither the BRIDGE CP nor the COMMON CP addresses a revocation use case in which some certificates may 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 and revoke the certificates that were derived from the compromised key (e.g., rekey). If some were issued properly, but some improperly, only the improperly issued certificates must be revoked.

Specific Changes:

Insertions are <u>underlined</u>, deletions are in ~~strikethrough~~:

4.9.3 Procedure for Revocation Request

….

For PIV-I and in all other cases not identified above, revocation of the certificates is mandatory. Even where all the above conditions have been met, revocation of the associated certificates is recommended.

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 from the date the change is incorporated into FBCA 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