FBCA Certificate Policy Change Proposal Number: 2017-03

To: Federal PKI Policy Authority (FPKIPA)
From: Chi Hickey, Co-Chair, FPKIPA
Subject: Proposed modifications to the Federal Bridge Certificate Policy
Date: April 3, 2017

Title: CA Infrastructure Change Notification

Version and Date of Certificate Policy Requested to be changed: X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) Version 2.30, October 5, 2016

Change Advocate's Contact Information: chi.hickey@gsa.gov

Organization requesting change: FPKI Policy Authority

Change summary: Implementation of this change proposal will require CAs cross certified with the FBCA to notify the FPKIPA whenever a change is made to their infrastructures.

Background:

On several occasions, Federal Agencies have been adversely affected due to changes to member infrastructures that were not communicated to the FPKI beforehand. In some cases, there has been potential for introducing security vulnerabilities to the FPKI trust infrastructure.
This change will make communication with the FPKIPA mandatory at least two (2) weeks prior to a planned change taking place, and within 24 hours following the change to share new objects (certificates, etc.), where applicable. Changes include any modification to the infrastructure that may affect the FPKI community and any time a new CA is implemented. By providing this notification, the FPKIPA can ensure the larger trust community is informed by posting the information and/or distributing the information through the listserv *FPKI-Operations-Customers*, thereby providing the tools needed to maintain the security posture of the FPKI and ensure continuing interoperability.

Specific Changes

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

1.3.1.6 Entity PKI Policy Management Authority

Entity PKIs (including other Bridges) that are cross certified with the Federal Bridge shall identify an individual or group that is responsible for maintaining the entity PKI CP and for ensuring that all Entity PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with the entity PKI CP. This body is referred to as Entity PKI Policy Management Authority (PMA) within this CP.

The Entity PKI PMA shall be responsible for notifying the FPKIPA of any change to the infrastructure that has the potential to affect the FPKI operational environment at least two weeks prior to implementation; all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change shall be provided to the FPKIPA within 24 hours following implementation.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities.

For the FBCA, notification of certificate issuance will be provided to all cross-certified entities.

For Entity CAs, the FPKIPA shall be notified at least two weeks prior to the issuance of a new CA certificate ~~upon~~ or issuance of new inter-organizational CA cross-certificates. In addition, all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the CA certificate issuance shall be provided to the FPKIPA within 24 hours following issuance.

4.9 Certificate Revocation & Suspension

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

For High, Medium Hardware, Medium, and Basic Assurance, all CAs shall publish CRLs.

For Entity CAs, the FPKIPA shall be notified at least two weeks prior to the revocation of a CA certificate, whenever possible. For emergency revocation, CAs shall follow the notification procedures in Section 5.7.

5.8 CA or 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.

Whenever possible, the FPKIPA shall be notified at least two weeks prior to the termination of any CA operated by an Entity cross certified with the FBCA. For emergency termination, CAs shall follow the notification procedures in Section 5.7.

9.11 Individual Notices and Communications with Participants

The Federal PKI PA shall establish appropriate procedures for communications with Entity CAs via contracts or memoranda of agreement as applicable.

For Entity CAs, any planned change to the infrastructure that has the potential to affect the FPKI operational environment shall be communicated to the FPKIPA at least two weeks prior to implementation, and all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change must be provided to the FPKIPA within 24 hours following implementation.

For all other communications, no stipulation.

Estimated Cost:

There may be a cost to PKI operators for revising documentation and implementing the notification process.

Implementation Date:

This change will be effective immediately upon approval by the FPKIPA and incorporation into the FBCA Certificate Policy.

Prerequisites for Adoption:

None

Plan to Meet Prerequisites:

N/A.

Approval and Coordination Dates:

Date presented to CPWG:	April 3, 2017
Date change released for comment:	May 17, 2017
Date comment adjudication published:	June 1, 2017