FPKIPA
Federal Public Key Infrastructure Policy Authority

Common Policy Framework Certificate Policy Change Proposal Number: 2017-03

To: Federal PKI Policy Authority (FPKIPA)

From: Chi Hickey, Co-chair, FPKIPA

Subject: Proposed modifications to the Common Policy Framework 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 U.S. Federal PKI Common Policy Framework, Version 1.25, September 22, 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 issuing under the COMMON Policy Framework to notify the FPKIPA whenever a change is made to their infrastructures.

Background:

On several occasions, the Federal Agencies has been adversely affected due to changes to member infrastructures that were not communicated to the FPKIPA 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~~:

1.3.1.5 Policy Management Authority

Each organization that provides PKI services under this policy shall identify an individual or group that is responsible for maintaining the Shared Service Provider's (SSP) CPS and for ensuring that all SSP PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with the SSP CPS and this CP. This body is referred to as the SSP PMA within this CP.

Agencies that contract for the services of a CA under this policy, shall establish a management body to manage any agency-operated components (e.g., RAs or repositories) and resolve name space collisions. This body shall be referred to as an Agency Policy Management Authority, or Agency PMA.

An SSP PMA shall be responsible for notifying its customer Agency PMAs and 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.

An Agency PMA is responsible for ensuring that all Agency operated PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with this CP and the applicable CPS and shall serve as the liaison for that agency to the FPKIPA and the SSP PMA.

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

~~The FPKIPA must be notified~~ Whenever a CA operating under this policy issues a CA certificate, the FPKIPA shall be notified at least two weeks prior to issuance. In addition, all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the event shall be provided to the FPKIPA within 24 hours following issuance.

4.9 Certificate Revocation and Suspension

CAs operating under this policy shall issue CRLs covering all unexpired certificates issued under this policy except for OCSP responder certificates that include the id-pkix-ocsp-nocheck extension.

CAs operating under this policy shall make public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to subscribers during certificate request or issuance, and shall be readily available to any potential relying party.

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**.**

Certificate suspension for CA certificates is not allowed by this policy. However, the use of certificate suspension for end entity certificates is allowed.

For CAs operating under this policy, 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

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.

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.

9.11 Individual Notices and Communications with Participants

The FPKIPA shall establish appropriate procedures for communications with CAs operating under this policy via contracts or memoranda of agreement as applicable.

For CAs operating under this policy, any planned changes 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 the date of approval by the FPKIPA and incorporation into the Federal Common Policy Framework Certificate Policy.

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not Applicable

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