FBCA Certificate Policy Change Proposal Number: 2017-05

To: Federal PKI Policy Authority (FPKIPA)

From: FPKI Management Authority (FPKIMA)

Subject: Proposed modifications to the FBCA Certificate Policy

Date: April 3, 2017

Title: Limit Affiliate Relationship to a single path

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: FPKIPA

Organization requesting change: FPKI Policy Authority

Change summary: This change will require that CAs cross certified with the FBCA have a single trust path to the FBCA.

Background:

The Federal PKI relies on the use of Policy Mapping and Policy Constraints to ensure that transitive trust is not accidentally introduced into the FPKI due to members being cross-certified with more than one Bridge in the FPKI. However, some relying party applications do not fully support policy processing when doing path validation. This leads to the possibility of those applications accepting unintended paths as valid. To address this issue, the FPKIPA wants to limit the number of connections a single CA can have to the FPKI.

CAs shall not be cross certified or otherwise connected to the Federal PKI at more than one point. Specifically, aside from existing certificate renewals and rekey, not more than one distinct trust path shall be intentionally created from any CA or End Entity to the Federal Common Policy CA. This policy ensures the simplest possible certificate path building and validation by eliminating unnecessary choices and the potential for undesirable loops. This leads to better performance and fewer opportunities for less robust certificate processing software to fail. Additionally, a single connection provides a clear point from which a relationship can be severed if needed, such as in the event of a critical compromise.

Specific Changes:

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

1.3.1.5 Entity Principal Certification Authority (CA)
The Principal CA is a CA within a PKI that has been designated to cross-certify directly with the FBCA (e.g., through the exchange of cross-certificates). The Principal CA issues either end-entity certificates, or CA certificates to other Entity or external party CAs, or both. Where the Entity operates a hierarchical PKI, the Principal CA is typically the Entity Root CA. Where the Entity operates a mesh PKI, the Principal CA may be any CA designated by the Entity for cross-certification with the FBCA.

It should be noted that an Entity may request that the FBCA cross-certify with more than one CA within the Entity; that is, an Entity may have more than one Principal CA. Additionally, this CP may refer to CAs that are "subordinate" to the Principal CA. The use of the term "subordinate CA" shall encompass any CA under the control of the Entity that has a certificate issued to it by the Entity Principal CA or any CA subordinate to the Principal CA, whether or not the Entity employs a hierarchical or other PKI architecture.

The Entity shall ensure that no CA under its PKI shall have more than one trust path to the FBCA (regardless of path validation results).

3.2.6 Criteria for Interoperation
The FPKIPA shall determine the criteria for cross-certification with the FBCA. See also the *Federal Public Key Infrastructure Bridge Application Process Overview* document [BRIDGE PROCESS] and the *Federal Public Key Infrastructure Annual Review Requirements* document. Under no circumstances shall any certificate have more than one intentional trust path to the FBCA, irrespective of extension processing.

Note: Multiple trust paths created as a result of certificate renewal or CA rekey do not violate the single trust path requirement above.

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 upon issuance of new inter-organizational CA cross-certificates. The notification shall assert that the new CA cross-certification does not introduce multiple paths to a CA already participating in the FPKI.

Estimated Cost:

The cost associated with this change would be the administrative cost to ensure that any new members of a Bridge do not already have a trust path to the FBCA for the CAs which they hope to cross-certify with that Bridge.

Implementation Date:

This change will be effective six (6) months following approval by the FPKIPA and incorporation into the Federal Bridge 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 9, 2017