FBCA Certificate Policy Change Proposal Number: 2018-01

To: Federal PKI Policy Authority (FPKIPA)

From: FPKI Certificate Policy Working Group (CPWG)

Subject: Proposed modifications to the FBCA Certificate Policy

Date: July 6, 2017

Title: Add requirements for Key Recovery

Version and Date of Certificate Policy Requested to be changed: X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA) Version 2.31 June 29, 2017

Change Advocate's Contact Information: FPKIPA

Organization requesting change: FPKI Policy Authority

Change summary: Update the CP to require conformity to FPKI Key Recovery Policy (KRP) whenever key escrow services are implemented for key management certificates issued by organizations cross certified with the FBCA

Background:

In order to achieve consistency and improved reliability, there is a need to standardize the approach to key recovery within the federal enterprise. This change applies to all cross certified entities that issue key management certificates to subscribers and maintain a key recovery system. The protection of this key recovery system is as critical as the protection of the certification issuance components and processes. To this end, a FPKI Key Recovery Policy (KRP) was published that provides the minimum requirements for maintaining and recovering keys. Any cross certified PKI that offers key recovery services to its members must have a key recovery policy. There are two choices: adopt the FPKI KRP and write a KRPS that implements it *or* write a key recovery policy that is comparable to the FPKI KRP. The FPKI will determine comparability.

Specific Changes:

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

4.12.1 Key Escrow and Recovery Policy and Practices

CA private keys are never escrowed.

Subscriber key management keys may be escrowed to provide key recovery. CAs that support private key escrow for key management keys shall ~~document their key recovery practices~~ do one of the following:

- Adopt the *FPKI Key Recovery Policy* (KRP) and develop a Key Recovery Practice Statement (KRPS) describing the procedures and controls implemented to comply with the FPKI KRP; or
- Develop a KRP that establishes security and authentication requirements comparable to the FPKI KRP. The KRP may be a separate document or combined with the organization's Certificate Policy (CP). Develop a KRPS describing the procedures and controls implemented to comply with the organization's KRP.

In both cases, the KRPS may be a separate document or may be combined with the CPS.

Key Recovery policies and practices shall satisfy privacy and security requirements for CAs issuing and managing digital certificates under the Entity's CP.

Practice Note: Escrowed keys must be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber.

Under no circumstances will a subscriber signature key be held in trust by a third party.

12 Glossary

Key Recovery Policy (KRP)	A key recovery policy is a specialized form of administrative policy tuned to the protection and recovery of key management private keys (i.e. decryption keys) held in escrow. A key recovery policy addresses all aspects associated with the storage and recovery of key management certificates.
Key Recovery Practices Statement (KRPS)	A statement of the practices that a Key Recovery System employs in protecting and recovering key management private keys, in accordance with specific requirements (i.e., requirements specified in the KRP).

Estimated Cost:

Current key recovery systems and documentation must be reviewed/updated to ensure comparability with the FPKI Key Recovery Policy.

Implementation Date:

Organizations with key recovery systems will have one (1) year to achieve comparability with the requirements in the FPKI Key Recovery Policy

Prerequisites for Adoption:

None

Plan to Meet Prerequisites:

Not Applicable

Approval and Coordination Dates:

Date presented to CPWG:	July 18, 2017
Date presented to FPKIPA:	November 14, 2017
Date comment adjudication published:	January 10, 2018