FPKIPA
Federal Public Key Infrastructure Policy Authority

COMMON Certificate Policy Change Proposal Number: 2018-01

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Require Key Recovery for key management certificates issued under the COMMON Policy
Date: July 5, 2017

Title: Require Key Recovery for key management certificates issued under the COMMON Policy

X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework Version 1.27, June 29, 2017

Change Advocate's Contact Information:
Name: Chi Hickey
Organization: FPKI Policy Authority
Telephone number:
E-mail address: chi.hickey@gsa.gov

Organization requesting change: N/A

Change summary: Update the CP to require key escrow services for key management certificates issued under COMMON and include reference to the newly approved Key Recovery Policy

Background:

In order to achieve consistency and improved reliability, there is a need to standardize the approach to key recovery within the federal enterprise. In order to preserve key management certificates for key history purposes, issuers must maintain an escrow capability. The protection of this escrow is as critical as the protection of the certification issuance components and processes. To this end, a FPKI Key Recovery Policy was published that provides the minimum requirements for maintaining a key escrow. This Key Recovery Policy cites the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework as its source document and makes the escrow of PIV key management keys mandatory. This requirement is extended to all key management certificates issued by a CA that is subordinated to COMMON.

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.

Human subscriber key management keys ~~may~~ shall be escrowed to provide key recovery. CAs ~~that support private key escrow for key management keys~~ shall develop a Key Recovery Practice Statement (KRPS) describing the procedures and controls implemented to comply with the *FPKI Key Recovery Policy*. The KRPS may be a separate document or may be combined with the appropriate Certification Practice Statement and/or Registration Practice Statement. The Federal PKI Policy Authority (FPKIPA) will determine the KRPS compliance with the KRP and this CP. ~~Escrowed keys shall be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber.~~

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

6.2.3 Private Key Escrow

CA private keys are never escrowed.

Human subscriber key management keys ~~may~~ shall be escrowed to provide key recovery as described in section 4.12.1. If a device has a separate key management key certificate, the key management private key may be escrowed.

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: For organizations not already doing so, a key recovery system must be implemented. Current key recovery systems and documentation must be reviewed/updated to comply with the FPKI Key Recovery Policy.

Implementation Date: Organizations will have one (1) year to implement this change and 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