FPKIPA
Federal Public Key Infrastructure Policy Authority

COMMON Certificate Policy Change Proposal Number: 2023-02

To: Federal PKI Policy Authority (FPKIPA)
From: Federal PKI Certificate Policy Working Group (CPWG)
Subject: Proposed modifications to the Federal PKI Common Policy Framework Certificate Policy
Date: March 14, 2023

Title: Updates Common Policy based on general comments received by the CPWG

Version and Date of Certificate Policy Requested to be changed:

- *X.509 Certificate Policy for the Federal PKI Common Policy Framework Version 2.3, September 9, 2022*

Change Advocate's Contact Information:
Organization: FPKI Certificate Policy Working Group
E-mail address: fpki@gsa.gov

Organization requesting change: FPKI Certificate Policy Working Group

Change summary: This proposal incorporates changes to multiple sections of Common Policy based on the comments received during voting period of the most recent rewrite of the FBCA CP (change proposal 2022-04). The changes lend specificity to the following topics:

- Certificate suspension requirements to include reason codes in CRLs supporting certificate suspension
- 3rd party key recovery request handling
- Multi party control of Data Decryption Servers (DDS)
- The definition of a "remote workstation" as it relates to CA administration
- Public key parameters and quality checking, and
- Key generation using FIPS approved methods

The aim of this change is to reduce confusion or misinterpretation of impacted policy requirements.

Background: This update consolidates CPWG policy recommendations based on comments received from FPKIPA members during the vote for change 2022-04.

Specific Changes:
Insertions are underlined; deletions are in ~~strikethrough~~.

4.9.14 Who Can Request Suspension

~~No stipulation for Subscriber certificates.~~

For CAs that support suspension, those authorized to request suspension of a certificate must be identified.

4.9.15 Procedure for Suspension Request

~~No stipulation for Subscriber certificates.~~

For CAs that support suspension, all suspended certificate serial numbers must be populated on a full CRL within a timeframe specified in Section 4.9.7. The reason code CRL entry extension shall be populated with “certificateHold.”

For CAs that support suspension, a request to suspend a certificate must include:

- authentication of the requestor,
- identification of the certificate to be suspended, and
- explanation of the reason for suspension~~,~~

4.9.16 Limits on Suspension Period

~~No stipulation for Subscriber certificates.~~

For CAs that support suspension, the maximum time period a certificate may be suspended must be specified. The CPS must describe in detail how this maximum suspension period is enforced. If the subscriber has not removed the certificate from hold (suspension) within that period, the certificate must be revoked. Certificates must not be published on a CRL with a reason code of “certificateHold” beyond the expiration date of the certificate.

> Practice Note: In order to mitigate the threat of unauthorized person removing the certificate from hold, the identity of the RA or authorized individual removing the suspension should be authenticated using a mechanism equivalent or higher than the assurance level of the certificate being unsuspended.

4.12.1.2. Key Recovery Process and Responsibilities

…

~~Internal~~ Third-Party Requestors may use electronic or manual means to request the Subscribers’ escrowed keys. The Requestor must submit the request to the KRA or KRO. If the request is made electronically, the

Requestor must digitally sign the request using a~~n~~ trusted authentication or signature certificate, as determined by the recovering organization, with an assurance level equal to or greater than that of the escrowed key. Manual requests ~~must be made in person, and~~ must include proper identity verification by the KRA in accordance with Section 3.2.3.1.

~~External Third-Party Requestors must use manual means to request the Subscribers' escrowed keys. The Requestor must submit the request to the KRA or KRO. Manual requests must be made in person, and must include proper identity verification by the KRA in accordance with Section 3.2.3.1.~~

…

4.12.1.6. Key Recovery by Data Decryption Server

…

In order to prevent any individual KRA, KRO or another trusted role from accessing subscriber encryption keys, a combination of physical, procedural, and technical security controls must be used to enforce continuous two-person control on the DDSs. The DDSs must be designed to maximize the ability to enforce two-person control technically.

~~Practice Note: The DDS is considered under two-person control when any human action performed on the DDS requires two persons.~~

5.1. PHYSICAL CONTROLS

...

~~Practice Note: The phrase "remote workstations used to administer the CAs," refers to dedicated systems solely used for accessing either the system hosting the CA or the CA itself through external networks for maintenance and administration. It does not refer to administration workstations or consoles within the CA's security perimeter or to Registration Authority workstations used by RAs to support certificate management and Subscribers.~~

[The following definition will be migrated to the Glossary]

APPENDIX F: GLOSSARY

…

- Remote Workstation	In the context of FPKI, "remote workstation" refers to a ~~dedicated~~ system used ~~solely~~ to ~~for~~ access ~~accessing~~ either the system hosting the CA or the CA itself through external networks for maintenance and administration.

	Note: Reference Section 6.6.1 for additional technical controls required of remote workstations. This term does not refer to consoles within the CA’s security perimeter or to Registration Authority workstations.

6.1.1. Key Pair Generation

Key generation must be performed using a FIPS approved method or equivalent international standard. Key generation events should use the configuration that was the basis of the FIPS or other approved standard (e.g., FIPS mode). If the required keys cannot be generated while in an approved configuration, the specific configuration and reason for use of a different method should be documented by the CA.

6.1.6. Public Key Parameters Generation and Quality Checking

~~Elliptic curve public key parameters must always be selected from the set specified in Section 7.1.3.~~

For RSA, the CA shall perform partial public key validation as specified in NIST SP 800-89 (Section 5.3.3).

For ECC, public keys must fall within curves defined in Section 7.1.3. Additionally, the CA should confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine as specified in NIST SP 800-56A (Sections 5.6.2.3.3, or 5.6.2.3.4).

Change Impacts:

- For those that have chosen to support certificate suspensions, the new suspension requirements:
  - May require updates to CA configurations to leverage CRL reason codes specifically for suspension (e.g., certificateHold); CAs that do not support suspension will remain unaffected
  - May require RAs to collect and archive suspension request artifacts, RAs that do not support suspension will remain unaffected
- Removes ambiguous practice notes or requirements, and clarifies others
- Allows organizations to accept digital signatures in support of external 3rd party key recovery requests
- Ensures key pair generation is done using a FIPS approved method; otherwise, it clarifies specific audit and archive documentation (e.g., 4096 bit key generation)

- Clarifies public key parameters for generation and quality checking by separating references by cryptographic type and provides specific sub-section references in their associated standards

Estimated Cost: Unknown

Implementation Date: September 1, 2023 (aligns with FBCA CP v3.0 implementation date)

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:
Date presented to CPWG: October 25, 2022
Date change released for comment: December 12, 2022
Date comment adjudication published: February 28, 2023