COMMON Certificate Policy Change Proposal Number: 2024-08

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Private Key Recovery Storage and Activation Clarifications
Date: October 10, 2024

Title: Clarifications on Private Key Recovery Storage and Private Key Activation

X.509 Certificate Policy For The Federal PKI Common Policy Framework Version 2.8 May 31, 2024

Change Advocate's Contact Information: fpki@gsa.gov

Organization requesting change: CPWG

Change summary: Clarify the key storage requirements for Third-Party recovery of PIV key management keys that were originally issued to subscribers asserting common-hardware policies.

Additionally, clarify requirements for securely recording private key activation data.

Background:

The FPKIPA support team was recently made aware of potential policy constraints associated with legitimate Third-Party key recovery requests wherein the requested certificates and keys to be recovered originally asserted the common-hardware OID. Currently, Section 6.2.1 of policy indicates that these keys can only be stored in FIPS 140 level 2 hardware with no cited exceptions or associated stipulations.

The FPKIPA has always understood that recovery of keys to software (e.g., PKCS12 or PFX files) is a feature of most KEDs and allows for generally easier acceptance and usage by legitimate Third-Party requestors and can easily be consumed by e-discovery decryption tools. As a result, this change seeks to clarify the approved exceptions to PIV KMK for storage in only hardware by extending FIPS 140 level 1 key storage to legitimate third-party key recovery

scenarios, provided all other security requirements for key recovery in Section 4.12 and 6.2.6 are met.

Additionally, independent Auditors informed the CPWG that they have observed different technical tools (e.g., password managers) that CA trusted roles use to record PINs/Passphrases that are needed to activate the CA private keys (or split keys). This proposed change seeks to provide clarity on the allowability of these tools to securely store memorized secrets.

Specific Changes:

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

1.2 Document Name and Identification

…

Additional Human Subscriber Certificates

Digital signature certificate with the private key on a PIV credential	id-fpki-common-hardware or id-fpkicommon-high
Digital signature certificate with the private key not on a PIV credential	id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-high
Key Management certificate, whether or not on a PIV credential	id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-high
Practice Note – Asserting id-fpki-common-policy for key management certificates is recommended as it provides implementation flexibility for specific use cases such as mobile devices and key recovery.	
Common PIV-I Authentication certificate with the private key on a federally-issued PIV-I credential	id-fpki-common-pivi-authentication
Other authentication certificate	id-fpki-common-policy, id-fpki-commonhardware, or id-fpki-common-high

4.12.1. Key Escrow and Recovery Policy and Practices

CA private keys are never escrowed.

Human Subscriber key management keys must be escrowed to provide key recovery. Escrowed keys must be maintained within an online KED for a minimum of one year after the expiration of

the associated public key certificate.

Practice Note: When considering allowing Third-Party recovery of id-fpki-common-hardware key management keys to software, Entities should carefully consider the risk of unauthorized decryption of data encrypted by the recovered keys and should define which scenarios this risk is acceptable in their CPS, RPS, or KRPS, see Section 6.2.1 for further details.

Subscriber signature keys are never escrowed.

5.4.1. Types of Events Recorded

...
The CA and KRS must record all events identified in the list below, where applicable to the application, environment, or both. Where these events cannot be electronically logged, electronic audit logs must be supplemented with physical logs as necessary.
...

- **MISCELLANEOUS:**
  - All records of authentication, authorization, recovery, agreement and delivery of key management keys to a key recovery requestor.

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is Security Requirements for Cryptographic Modules [FIPS 140]. A FIPS 140 Level 1 or higher validated cryptographic module must be used for all cryptographic operations. Cryptographic modules must be minimally validated to a FIPS 140 level identified in this section, with the exception of Hardware Subscriber Key Management Key(s) only for recovery and when dictated by extenuating circumstances put for by a Third-Party Requestor in alignment with legal or technical requirements.

Private Key	FIPS 140 Level
CA, KED, and DDS ● all applicable policies	3
CSS ● all applicable policies	2
PIV and Common PIV-I Content Signing ● id-fpki-common-piv-contentSigning ● id-fpki-common-pivi-contentSigning	2
Hardware Signature and Authentication ● id-fpki-common-authentication ● id-fpki-common-derived-pivAuth-hardware ● id-fpki-common-cardAuth	2

• id-fpki-common-hardware • id-fpki-common-high • id-fpki-common-pivi-authentication • id-fpki-common-pivi-cardAuth	
Hardware Subscriber Key Management • id-fpki-common-hardware	2 or 1*
Hardware Device • id-fpki-common-devicesHardware	2
Software Signature and Authentication • id-fpki-common-policy • id-fpki-common-derived-pivAuth	1
Software Subscriber Key Management • id-fpki-common-policy	1
Software Device • id-fpki-common-devices	1
Practice Note – All instances of recovered keys should be destroyed as early as practicable in consultation with the Third-Party Recovery Requestor (e.g., after required data has been decrypted). See Sections 4.12 and 6.2.6 for additional key recovery requirements to include secure transport.	

*When necessary for completing an authenticated and authorized Third-Party key recovery request (e.g., in support of an investigation) Hardware Subscriber key management keys can only be recovered into a Level 1 module or an encrypted file (.p12 or .pfx) provided there is organizational approval based on the acceptance of risk to data encrypted with the associated public keys.

RAs must use a FIPS 140 Level 2 or higher validated hardware cryptographic module when authenticating to systems to fulfill their duties.

PIV or Common PIV-I cards must only be issued using card stock that has been tested and approved by the FIPS 201 Evaluation Program and listed on the GSA Approved Products List (APL). Card stock that has been removed from the APL may continue to be issued for no more than one year after GSA approved replacement card stock is available. PIV or Common PIV-I cards issued using the deprecated card stock may continue to be used until the current Subscriber certificates expire, unless otherwise notified by the FPKIPA/FPKIMA.

Any pseudo-random numbers used for key generation material must be generated using a FIPS-validated cryptographic module.

6.2.6 Key Transfer into or from a Cryptographic Module

At no time shall the CA private key exist in plaintext outside the cryptographic module boundary.

CA, CSS and PIV Content Signing private signature keys may be exported from the cryptographic module only to perform key backup procedures as described in Section 6.2.4.

In the event that any private key is transported from one cryptographic module to another, to include key recovery operations, the private key must be protected using a FIPS approved algorithm and at a bit strength commensurate with the key being transported. Private keys must never exist in plaintext form outside the cryptographic module boundary.

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

6.4.2 Activation Data Protection

Data used to unlock private keys must be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data must be:

- memorized,
- biometric in nature; or
- contained within an organizationally approved device or software tool (e.g., password manager) that leverages encryption commensurate with the bit-strength of the key it activates, or
- physically recorded and secured at the level of assurance associated with the activation of the cryptographic module, and must not be stored separately from with the cryptographic module.

> Practice Note: Level 2 in For [FIPS 140] Level 2 and higher modules, requires that the protection mechanism should includes a facilityan an ability to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts to protect against repeated guessing attacks.

Estimated Cost: None

Implementation Date: Immediate upon publication

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:

Date presented to CPWG:	May 28, 2024
Date change released for comment:	June 12, 2024
Date comment adjudication published:	September 27, 2024