FBCA Certificate Policy Change Proposal Number: 2024-10

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 Bridge Certification Authority Version 3.5 May 8, 2024

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

Organization requesting change: CPWG

Change summary: Clarify the key storage requirements for recovered key management keys that were originally issued to subscribers on hardware tokens and asserting mediumHardware 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 key recovery requests wherein the requested certificates and keys to be recovered originally asserted the common-hardware OID for PIV users. This scenario can also impact PIV-I or other hardware based KMK that chain through the FBCA. 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 requestors and can be easily be consumed by e-discovery decryption tools. As a result, this change seeks to clarify the approved exceptions to PIV-I or other hardware-based KMK storage in only hardware by extending FIPS 140 level 1 key storage to 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

…

Human Subscriber Certificates

Certificates valid for the following policies are issued to Human Subscribers:

PIV-I Authentication certificate	id-fpki-certpcy-pivi-hardware
Digital Signature certificate with the private key generated on a PIV-I credential	id-fpki-certpcy-mediumHardware
Key Management certificate associated with a PIV-I credential	id-fpki-certpcy-mediumAssurance id-fpki-certpcy-mediumHardware
Practice Note: Asserting id-fpki-certpcy-mediumAssurance for key management certificates is recommended as it provides implementation flexibility for specific use cases such as mobile devices and key recovery.	
All other hardware-based certificates	id-fpki-certpcy-mediumHW-CBP id-fpki-certpcy-mediumHardware id-fpki-certpcy-highAssurance*
All software-based certificates	id-fpki-certpcy-rudimentaryAssurance id-fpki-certpcy-basicAssurance id-fpki-certpcy-medium-CBP id-fpki-certpcy-mediumAssurance

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.

When implemented, key recovery requirements must be documented in a Key Recovery Policy (KRP). The KRP may be a separate document or may be combined with the CP.

Practice Note: When considering allowing recovery of id-fpki-certpcy-mediumHardware 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 CP/KRP or CPS/RPS/KRPS, see Section 6.2.1 for further details.

Key Recovery policies and practices must 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 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.
...

	Rudimentary	**Basic**	**Medium, PIV-I, High**
MISCELLANEOUS			
All records of authentication, authorization, recovery, agreement and delivery of key management keys to a key recovery requestor.	**X**	**X**	**X**

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is [FIPS 140], *Security Requirements for Cryptographic Modules*. A FIPS 140 Level 1 or higher validated cryptographic module must be used for all cryptographic operations.

Cryptographic modules must be minimally validated to the FIPS 140 level identified in this section, with the exception of Hardware Subscriber Key Management Key(s) only for key recovery and when dictated by extenuating circumstances put for by a Third-Party Requestor in alignment with legal or technical requirements. Additionally, the FPKIPA reserves the right to

review technical documentation associated with any cryptographic modules under consideration for use by the FBCA.

Practice Note: The Federal PKI Policy Authority may determine that other comparable validation, certification, or verification standards are sufficient when cross-certifying with non-U.S. government PKIs.

The table below summarizes the minimum FIPS 140 requirements for cryptographic modules; higher levels may be used.

Assurance Level	CA	CMS & CSS	Subscriber	RA
Rudimentary	Level 1	Level 1	N/A	Level 1
Basic	Level 2	Level 2	Level 1	Level 1
Medium	Level 3 (Hardware)	Level 2 (Hardware)	Level 1	Level 2 (Hardware)
PIV-I Card Authentication	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
Medium Hardware	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware) <u>Level 1* (Key Recovery)</u>	Level 2 (Hardware)
High	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
<u>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.</u>				

<u>*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</u>.

PIV-I Cards must 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-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.

For hardware tokens associated with PIV-I, see Appendix A for additional requirements.

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

A CA private key must not exist in plain text outside the cryptographic module.

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

If 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,
- 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.

~~The protection mechanism must include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CP.~~

Practice Note: For [FIPS 140] level 2 and higher modules, the protection mechanism should include 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, as set forth in the respective CP.

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