FDE Interpretation # 202210

Status: ☒ *Active* □ *Inactive*

Date: 08-23-2022

Type of Document: ☒ *Technical Decision* □ *Technical Recommendation*

Approved by: □ *FDE iTC Interpretations Team* ☒ *FDE iTC*

Affected Document(s): FDE AA cPP v2.0 + Errata 20190201, FDE EE cPP v2.0 + Errata 20190201

Affected Section(s): FPT_KYP_EXT.1.1

Superseded Interpretation(s): *202204*

Issue:

FPT_KYP_EXT.1 lists various scenarios when plaintext keys may be stored. One input to FMT_SMC_EXT.1 may be plaintext if the other input is derived. The same allowance should be allowed for the final bullet as well. Using a plaintext/known key to unwrap or decrypt a derived key does not provide an attacker to access to the non-volatile memory (i.e. plaintext key) any information about the resulting value.

The proposed changes are highlighted below:

FPT_KYP_EXT.1.1 The TSF shall [selection:

- not store keys in non-volatile memory
- only store keys in non-volatile memory when wrapped, as specified in FCS_COP.1(d), or encrypted, as specified in FCS_COP.1(g) or FCS_COP.1(e)
- only store plaintext keys that meet any one of the following criteria [selection:
  - the plaintext key is not part of the key chain as specified in FCS_KYC_EXT.2,
  - the plaintext key will no longer provide access to the encrypted data after initial provisioning,
  - the plaintext key is a key split that is combined as specified in FCS_SMC_EXT.1, and the other half of the key split is [selection:
    - wrapped as specified in FCS_COP.1(d),
    - encrypted as specified in FCS_COP.1(g) or FCS_COP.1(e),
    - derived and not stored in non-volatile memory],
  - the non-volatile memory the key is stored on is located in an external storage device for use as an authorization factor,
  - the plaintext key is [selection:
    - used to wrap a key as specified in FCS_COP.1(d),
    - used to encrypt a key as specified in FCS_COP.1(g) or FCS_COP.1(e)]

    that is ~~already~~ [selection:
    - already wrapped as specified in FCS_COP.1(d),
    - already encrypted as specified in FCS_COP.1(g) or FCS_COP.1(e),
    - derived and not stored in non-volatile memory]]].

Resolution:

After additional discussions to understand the proposed use case the FIT concurs with the proposed changes.

Rationale:

This method has been included to allow the merging into a key chain where one of the keys is volatile and merged with a plaintext key. The keychain would still be unable to be decrypted without access to the authentication factor with the additional option included.

Further Action:

None.

Action by FDE iTC:

None.