Proposal for FPT_KYP_EXT.1 from JBMIA

Issue #173
FPT_KYP_EXT.1 should be modified based on the proper intention of ITSCC

2021.Apr.13

JBMIA

Outline of our proposal : FPT_KYP_EXT should be modified

ESR and SPD require the "protection" of initial data of key.

ESR v0.7

To support encryption, the HCD shall maintain key chains in such a way that keys and key materials are protected. Note that the initial data of the key chain stored on the nonvolatile storage device without protection do not meet the requirement.

SPD (HCD-SPD-DRAFT_v0.2_2021-03-15.pdf)

2.3 Organizational Security Policies
4. Storage Encryption
Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on any nonvolatile storage device without protection [P.KEY_MATERIAL].

However, Current FPT_KEY_EXT.1 has no selection how to protect the keys.

B.1. Confidential Data on Field-Replaceable Nonvolatile Storage Devices
B.1.1. FPT_KYP_EXT.1 Extended: Protection of Key and Key Material
(for O.KEY_MATERIAL)

FPT_KYP_EXT.1.1 Refinement: The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in any Field-Replaceable Nonvolatile Storage Device.

<u>Our proposal</u>
FPT_KYP_EXT should be modified so that it requires "protection" of initial data of key chain rather than prohibit of storing plaintext keys. In this presentation, we propose a new SFR description.

Referred to FPT_KYP_EXT.1 in FDE AA/EE cPP v2.0

FPT_KYP_EXT.1 in FDE AA/EE cPP v2.0 has three major classification to store plaintext keys.
In FDE cPP, the plaintext key storage in non-volatile memory is allowed.
For HCD cPP, modify the 3rd selection of FPT_KYP_EXT.1 and define the criteria how to store protected keys instead of plaintext keys.

FPT_KYP_EXT.1 Protection of Key and Key Material
FPT_KYP_EXT.1.1 The TSF shall [selection:

- 1. not store keys in non-volatile memory
- 2. 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)
- 3. only store plaintext keys that meet any one of the following criteria [selection:
  - 3-1. the plaintext key is not part of the key chain as specified in FCS_KYC_EXT.1,
  - 3-2. the plaintext key will no longer provide access to the encrypted data after initial provisioning,
  - 3-3. 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:
    - 3-3-a. wrapped as specified in FCS_COP.1(d),
    - 3-3-b. encrypted as specified in FCS_COP.1(g) or FCS_COP.1(e),
    - 3-3-c. derived and not stored in non-volatile memory],
  - 3-4. the non-volatile memory the key is stored on is located in an external storage device for use as an authorization factor,
  - 3-5. the plaintext key is [selection:
    - 3-5-a-1. used to wrap a key as specified in FCS_COP.1(d),
    - 3-5-a-2. used to encrypt a key as specified in FCS_COP.1(g) or FCS_COP.1(e)]

    that is already [selection:
    - 3-5-b-1. wrapped as specified in FCS_COP.1(d),
    - 3-5-b-2. encrypted as specified in FCS_COP.1(g) or FCS_COP.1(e)]]].

Heading numbers in red are added for reference

Our proposal to modify FPT_KYP_EXT.1

FPT_KYP_EXT.1 Protection of Key and Key Material

FPT_KYP_EXT.1.1 The TSF shall [selection:

- 1. not store keys in non-volatile memory
- 2. only store keys in non-volatile memory when wrapped, as specified in ~~FCS_COP.1(d)~~FCS_COP.1(e), or encrypted, as specified in ~~FCS_COP.1(g)~~FCS_COP.1(f) or ~~FCS_COP.1(e)~~FCS_COP.1(i)
- 3. only store ~~plaintext~~protected keys that meet any one of the following criteria [selection:
  - 3-1. the plaintext key is not part of the key chain as specified in FCS_KYC_EXT.1,
  - 3-2. the plaintext key will no longer provide access to the encrypted data after initial provisioning,
  - 3-3. 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:
    - 3-3-a. wrapped as specified in ~~FCS_COP.1(d)~~FCS_COP.1(e),
    - 3-3-b. encrypted as specified in ~~FCS_COP.1(g)~~FCS_COP.1(f) or ~~FCS_COP.1(e)~~FCS_COP.1(i),
    - 3-3-c. derived and not stored in non-volatile memory],
  - 3-4. ~~the non-volatile memory the key is stored on is located in an external storage device for use as an authorization factor, a secure storage device,~~
  - 3-5. the plaintext key is [selection:
    - 3-5-a-1. used to wrap a key as specified in ~~FCS_COP.1(d)~~FCS_COP.1(e),
    - 3-5-a-2. used to encrypt a key as specified in ~~FCS_COP.1(g)~~FCS_COP.1(f) or ~~FCS_COP.1(e)~~FCS_COP.1(i)]

    that is already [selection:
    - 3-5-b-1. wrapped as specified in ~~FCS_COP.1(d)~~FCS_COP.1(e),
    - 3-5-b-2. encrypted as specified in ~~FCS_COP.1(g)~~FCS_COP.1(f) or ~~FCS_COP.1(e)~~FCS_COP.1(i)]
  - 3-6. the non-volatile memory the key is stored on is located in a protected storage device]].

Text in red are modified from FDE AA cPP v2.0. Sub-number in FCS_COP.1 is defer between FDE cPP and HCD cPP.
3) Declare a selection for protected keys instead of plaintext keys.
3-4) Delete a selection with external authorization factor since the factor is not defined in HCD cPP.
3-6) Instead of 3-4, add a new criteria that uses a protected storage device (e.g. TPM and others in application note.).

Our proposal to modify application note in FPT_KYP_EXT.1

In current FPT_KYP_EXT.1 in HCD cPP has no application note. We propose a new application note with reference to FDE AA cPP v2.0. The red text is a difference between FDE cPP and HCD cPP.

Application Note: *~~The plaintext key storage in non-volatile memory is allowed for several reasons.~~ The keys must be protected from unauthorized access and must not be stored on any non-volatile storage device without protection. If the keys exist within protected memory that is not user accessible on the TOE or OE, the only methods that allow it to play a security relevant role for protecting the BEV or the DEK are if it is a key split or protection key is not part of the key chain or providing additional layers of wrapping or encryption on keys that have already been protected. Examples of a protected storage device that could claim conformance to this SFR include Secure Elements (SE), Trusted Platform Modules (TPM), Hardware Security Modules (HSM), Trusted Execution Environments (TEE), and Secure Enclave Processors (SEP).*

Three modifications in application note.

- According to ESR, modify the first sentence.
- Add a description for the selection 3-1.
- Add examples of a protected storage device. This sentence is according to DSC cPP.

Our proposal to modify HCD Supporting Document

3.1.1. FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

current

3.1.1.1. KMD

The evaluator shall examine the Key Management Description (KMD) for a description of the methods used to protect keys stored in nonvolatile memory.

The evaluator shall verify the KMD to ensure it describes the storage location of all keys and the protection of all keys stored in nonvolatile memory.

Proposal

2.3.1 Key and Key Material Protection (FPT_KYP_EXT)

2.3.1.1 FPT_KYP_EXT.1 Protection of Key and Key Material

2.3.1.1.1 TSS

The evaluator shall examine the TSS to verify that it describes the method by which intermediate keys are generated using submask combining.

2.3.1.1.2 Operational Guidance

There are no AGD evaluation activities for this SFR.

Copy the description of FDE AA cPP v2.0.

2.3.1.1.3 KMD

The evaluator shall examine the KMD for a description of the methods used to protect keys stored in non-volatile memory. The evaluator shall verify the KMD to ensure it describes the storage location of all keys and the protection of all keys stored in non-volatile memory. The description of the key chain shall be reviewed to ensure the selected method is followed for the storage of wrapped or encrypted keys in non-volatile memory and plaintext keys in non-volatile memory meet one of the criteria for storage.

2.3.1.1.4 Test

There are no test evaluation activities for this SFR.

Appendix: Our proposal to modify FPT_KYP_EXT.1 without heading numbers

FPT_KYP_EXT.1 Protection of Key and Key Material

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(e), or encrypted, as specified in FCS_COP.1(f) or FCS_COP.1(i)
- only store protected 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.1,
  - 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(e),
    - encrypted as specified in FCS_COP.1(f) or FCS_COP.1(i),
    - derived and not stored in non-volatile memory],
  - the plaintext key is [selection:
    - used to wrap a key as specified in FCS_COP.1(e),
    - used to encrypt a key as specified in FCS_COP.1(f) orFCS_COP.1(i)]

    that is already [selection:
    - wrapped as specified in FCS_COP.1(e),
    - encrypted as specified in FCS_COP.1(f) or FCS_COP.1(i)]
  - the non-volatile memory the key is stored on is located in a protected storage device]].