FDE Interpretation # 201804

Status: ☒*Active* □ *Inactive*

Date: 3/14/18

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

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

Affected Document(s): FDE AA cPP V1.0, FDE EE cPP V1.0, FDE AA cPP V2.0, FDE EE cPP V2.0

Affected Section(s): FPT_KYP_EXT.1.1

Superseded Interpretation(s): RFI201708

Issue:

In the FDEEEcPP20, the FPT_KYP_EXT.1.1 SFR states:

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)] unless the key meets any one of 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 plaintext key is stored on 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), encrypted as specified in FCS_COP.1(g) or FCS_COP.1(e)] that is already [selection: wrapped as specified in FCS_COP.1(d), encrypted as specified in FCS_COP.1(g) or FCS_COP.1(e)].]

In the (Vendor) firmware product case, the ST has the following selections:

The TSF shall [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)], unless the key meets any one of following criteria [none].

Question: The PP does not offer the selection of none but in the Curtiss-Wright firmware product, the TOE always stores keys wrapped or encrypted in non-volatile memory. There are no exceptions. Is this an acceptable operation for the SFR?

NIAP Response

The TRRT agrees that None should be a valid selection.

However, the TRRT may only provide an interpretation to clarify cPP Security Functional Requirements (SFRs) and Evaluation Activities (EAs) in the context of a specific product evaluation and specifically its ability to meet the cPP requirements. An FDE Interpretations Team (FIT) has been established by the iTC to address issues which may result in modifications to the cPP. Your question will be forwarded to the FDE iTC shortly. We highly recommend your participation in the iTC to ensure this issue is follow up on and brought to closure.

Resolution:

The FIT acknowledges a clarity issue that needs to be addressed.

The FPT_KYP_EXT.1.1 in the FDE EE cPP requirement shall be modified as follows:

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:
    - wrapped as specified in FCS_COP.1(d),
    - encrypted as specified in FCS_COP.1(g) or FCS_COP.1(e)]]].

The FPT_KYP_EXT.1.1 in the FDE AA cPP requirement shall be modified as follows:

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.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(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:
        - wrapped as specified in FCS_COP.1(d),
        - encrypted as specified in FCS_COP.1(g) or FCS_COP.1(e)]]].

Rationale:

Additional clarity on selections.

Further Action:

None.

Action by FDE iTC:

None