FDE Interpretation # 201902

Status: ☒ *Active* □ *Inactive*

Date: 07-16-2019

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

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

Affected Document(s): FDE AA cPP v2.0E, FDE EE cPP v2.0E

Affected Section(s): FPT_KYP_EXT.1

Superseded Interpretation(s):

Issue:

The TSS requirement in the Supporting Document section 2.3.1.1 paragraph number 102 of the FDE AA, and section 2.4.1.1 paragraph number 88 of the FDE EE is as follows:

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

This TSS requirement appears out of place. This requirement is listed under FPT_KYP_EXT.1 SFR; however, FPT_KYP_EXT.1 pertains to secure key storage and the methods used to protect keys stored in non-volatile memory, rather than to 'submask combining'.

Given that this is the only TSS assurance activity provided for FPT_KYP_EXT.1, the CCTL suggests that applicable TSS assurance requirements be generated for this SFR and that this non-applicable assurance requirement is removed or relocated to an applicable SFR.

Resolution:

The FIT acknowledges the issues described in the 'Issue' section above. The EA for FPT_KYP_EXT.1 shall now read: (Bold indicates changed/added language, strikethrough indicates removed language)

TSS

The evaluator shall examine the TSS and verify it identifies the methods used to protect keys stored in non-volatile memory.

Operational Guidance

There are no AGD evaluation activities for this SFR.

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.

Test

There are no test evaluation activities for this SFR.

Rationale:

This was an editorial error. In changing we also were more specific with the corrected language.

Further Action:

None.

Action by FDE iTC:

None.