FDE Interpretation # 201806

Status: ☒*Active* □ *Inactive*

Date: 08-10-2018

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

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

Affected Document(s): FDE AA SD V2.0, FDE EE SD v2.0, FDE EE cPP V2.0

Affected Section(s): FCS_CKM_EXT.4(b), FPT_PWR_EXT.1, FPT_PWR_EXT.2, FCS_CKM.1.1(b), C.2 Extended Component Definitions

Superseded Interpretation(s):

Issue:

In both the Full Drive Encryption (FDE) AA and EE cPPs, there are several requirements (FPT_PWR_EXT.1, FPT_PWR_EXT.2, FCS_CKM_EXT.4(b)) where the Assurance Activity states to perform key destruction tests and/or include KMD documentation according to FCS_CKM.4(b). There are a few problems with this Assurance Activity as written:

1) The FDE AA cPP does not have FCS_CKM.4(b) as one of the SFRs, so Assurance Activities referring to it cannot be performed.

2) The FDE EE cPP does have FCS_CKM.4(b), but it is selection-based. In other words, the lab or vendor can CHOOSE not to include FCS_CKM.4(b). In this case, the lab did NOT include FCS_CKM.4(b). Moreover, mandatory requirement FCS_CKM_EXT.4(b) requires a KMD description according to FCS_CKM.4(b), which would defeat the purpose of keeping FCS_CKM.4(b) selection-based. In other words, it would not make sense to perform key destruction according to FCS_CKM.4(b) and not include it in the first place, which is not immediately obvious given the wording in the cPP. The same could apply to other requirements referring to FCS_CKM.4(b) for testing.

3) The Extended Component Definition (ECD) of FCS_CKM_EXT.6 instructs the ST author to select two FCS_CKM.4 iterations through an assignment, even though the ECD was intended for a PP author to instantiate accordingly. However, FCS_CKM_EXT.6 in the FDE EE cPP allows an ST author to include only a single FCS_CKM.4 iteration which, without clarification within the SFR, possibly violates the FCS_CKM_EXT.6 ECD.

Please advise on all of these cPP issues.

Resolution:

The FIT acknowledges the issues described in the 'Issue' section above.

To address issue 1:

The KMD section FCS_CKM_EXT.4(b) in the FDE AA SD v2.0 shall therefore be modified as follows:

The evaluator shall verify the KMD includes a description of the areas where keys and key material reside.

The evaluator shall verify the KMD includes a key lifecycle that includes a description where key material resides, how the key material is used, and how the material is destroyed once it is not needed and that the documentation in the KMD follows FCS_CKM.4(d) for the destruction.

The Test section in FPT_PWR_EXT.1 in the FDE AA SD v2.0 shall therefore be modified as follows:

The evaluator shall confirm that for each listed compliant state all key/key materials are removed from volatile memory by using the test defined in FCS_CKM.4(d).

The Test section in FPT_PWR_EXT.2 in the FDE AA SD v2.0 shall therefore be modified as follows:

The evaluator shall trigger each condition in the list of identified conditions and ensure the TOE ends up in a compliant power saving state by running the test identified in FCS_CKM.4(d).

To address issue 2:
The Application Note section in FCS_CKM.1.1(b) in the FDE EE cPP shall therefore be modified as follows:

The symmetric key generation function may be used to generate keys along the key chain or a DEK. It may also be used to provide inputs for key combining, key encryption, or key wrapping. Therefore, the ST author should select FCS_CKM.1(b), if Symmetric key generation is used.

*Note this removes the final line “FCS_CKM.4(b) Cryptographic Key Destruction (TOE-Controlled Hardware).

The KMD section in FCS_CKM_EXT.4(b) in the FDE EE SD shall therefore be modified as follows:

The evaluator shall verify the KMD includes a description of the areas where keys and key material reside.

The evaluator shall verify the KMD includes a key lifecycle that includes a description where key material resides, how the key material is used, and how the material is destroyed once it is not needed and that the documentation in the KMD follows FCS_CKM_EXT.6 for the destruction

The Test section in FPT_PWR_EXT.1 in the FDE EE SD v2.0 shall therefore be modified as follows:

The evaluator shall confirm that for each listed Compliant state all key/key materials are removed from volatile memory by using the test indicated by the selection in FCS_CKM_EXT.6.

The Test section in FPT_PWR_EXT.2 in the FDE EE SD v2.0 shall therefore be modified as follows:

The evaluator shall trigger each condition in the list of identified conditions and ensure the TOE ends up in a Compliant power saving state by using the test indicated by the selection in FCS_CKM_EXT.6.

To address issue 3:
The FCS_CKM_EXT.6.1 entry in the C.2 Extended Component Definitions section of the FDE EE cPP shall therefore be modified as follows:

The TSF shall use [assignment: one or more iterations of FCS_CKM.4 defined elsewhere in the Security Target] key destruction methods.

The FCS_CKM_EXT.6.1 entry in the C.2 Extended Component Definitions section of the FDE AA cPP shall therefore be removed.

Rationale:
Issue 1 is resolved by updating all reference to FCS_CKM.4(b) to FCS_CKM.4(d). FCS_CKM.4(b) does not exist in the FDE AA cPP v2.0.

Issue 2 is resolved by properly pointing key destruction references to FCS_CKM_EXT.6. Key destruction for an EE is intended to be done in one of three ways, no specific selection should be mandated.

Issue 3 is resolved by correcting the ECD to correctly say one or more iteration, as was the intent of the requirement. The entry is removed in the ECD in the AA as the requirement only exists in the FDE EE cPP.

Further Action:

None.

Action by FDE iTC:

None.