FDE Interpretation # 202002

Status: ☒*Active* □ *Inactive*

Date: 08-20-2020

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

Affected Section(s): FCS_SNI_EXT.1.3, FCS_COP.1(f)

Superseded Interpretation(s):

Issue:

Selections in FCS_SNI_EXT.1.3

Reference

[CPP_FDE_AA_V2.0E] collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, 1 Feb 2019

Background

In [CPP_FDE_AA_V2.0E], FCS_SNI_EXT.1 is a mandatory SFR that covers various factors (e.g., salts must be random, but nonces only have to be unique) and specifies how the Initialization Vector (IV) is to be handled for each encryption mode of AES (i.e., CBC, CCM, XTS, and GCM). In [CPP_FDE_AA_V2.0E], CBC, XTS, and GCM are allowed modes for AES encryption of data and CCM is an allowed mode for key wrapping.

However, none of the SFRs specifying encryption using AES are mandatory in [CPP_FDE_AA_V2.0E]. The relevant SFRs, and the basis for their selection in an ST, are as follows:

· - FCS_COP.1(d)—specifies requirements for key wrapping using AES in one or more of the following modes: KW; KWP; GCM; CCM. This SFR is selected if the ST author chooses to use key wrapping in the key chaining approach specified in FCS_KYC_EXT.1

· - FCS_COP.1(f)—specifies data encryption/decryption using AES in one of the following modes: CBC; GCM; XTS. This SFR is selected if the ST includes the validation requirement (FCS_VAL_EXT.1) and selects the option to decrypt a known value. The Application Note accompanying FCS_COP.1(f) also states it can be selected if the ST chooses to use AES encryption/decryption for protecting keys in the key chaining approach specified in FCS_KYC_EXT.1, but FCS_KYC_EXT.1 does not reference FCS_COP.1(f), and the PP provides FCS_COP.1(g) for that purpose

· - FCS_COP.1(g)—specifies data encryption/decryption using AES in one of the following modes: CBC; GCM. This SFR is selected if the ST chooses to use AES encryption/decryption for protecting keys in the key chaining approach specified in FCS_KYC_EXT.1.

Now, consider a TOE that claims conformance only to [CPP_FDE_AA_V2.0E]. The TOE uses key wrapping as the method for protecting the keychain from the authorization factor to the BEV, and so the ST specifies FCS_KYC_EXT.1.1 as follows:

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [

· intermediate keys originating from one or more submask(s) to the BEV using the following method(s): [

o key derivation as specified in FCS_KDF_EXT.1,

o key wrapping as specified in FCS_COP.1(d)]]

while maintaining an effective strength of [256 bits] for symmetric keys and an effective strength of [not applicable] for asymmetric keys.

For FCS_KDF_EXT.1, the TOE accepts a conditioned password submask and derives an intermediate key using a keyed-hash function as specified in FCS_COP.1(c). For key wrapping (FCS_COP.1(d)), the TOE uses AES in KWP mode. Finally, for FCS_VAL_EXT.1, the TOE validates the submask by hashing it and comparing it to a stored hashed value. The TOE does not use AES encryption in CBC, CCM, XTS, or GCM mode and the ST does not include FCS_COP.1(f) or FCS_COP.1(g).

Issue to be Resolved

Given this scenario, how should the ST complete FCS_SNI_EXT.1.3? None of the available selections is applicable to the TOE, because it does not use AES in any of the specified modes, yet there is no option to select “no IVs” or “none of the above”. Can the ST author leave the selection in FCS_SNI_EXT.1.3 unperformed and provide an Application Note explaining why no selection is made? For comparison, this approach has been accepted for STs conforming to the Network Device cPP and not storing plaintext keys in non-volatile storage (FCS_CKM.4.1).

Resolution:

The FIT acknowledges the issues described in the 'Issue' section above. **Bolding** and ~~strikethrough~~ indicates change.

FCS_SNI_EXT.1.3 The TSF shall **[selection: use no IVs,** create IVs in the following manner [selection:
• CBC: IVs shall be non-repeating and unpredictable;
• CCM: Nonce shall be non-repeating and unpredictable;

- XTS: No IV. Tweak values shall be non-negative integers, assigned consecutively, 28 and starting at an arbitrary non-negative integer;
- GCM: IV shall be non-repeating. The number of invocations of GCM shall not exceed 30 2^32 for a given secret key]**]**.

TSS
If salts are used, t~~T~~he evaluator shall ensure the TSS describes how salts are generated. The evaluator shall confirm that the salt is generating using an RBG described in FCS_RBG_EXT.1 or by the Operational Environment. If external function is used for this purpose, the TSS should include the specific API that is called with inputs. **If IVs or nonces are used, t**~~T~~he evaluator shall ensure the TSS describes how nonces are created uniquely and how IVs and tweaks are handled (based on the AES mode). The evaluator shall confirm that the nonces are unique and the IVs and tweaks meet the stated requirements.

FCS_COP.1(f)
Application Note: The intent of this requirement in the context of this cPP is to provide a SFR that expresses the appropriate symmetric encryption/decryption algorithms suitable for use in the TOE. If the ST author incorporates the validation requirement (FCS_VAL_EXT.1) and chooses to select the option to decrypt a known value and perform a comparison, this is the requirement used to specify the algorithm, modes, and key sizes the ST author can choose from. ~~Or, this requirement is used in the body of the ST if the ST author chooses to use AES encryption/decryption for protecting the keys as part of the key chaining approach that is specified in FCS_KYC_EXT.1.~~

When the XTS mode is selected, a cryptographic key of 256-bit or of 512-bit is allowed as specified in IEEE 1619. XTS-AES key is divided into two AES keys of equal size - for example, AES-128 is used as the underlying algorithm, when 256-bit key and XTS mode are selected. AES-256 is used when a 512-bit key and XTS mode are selected.

Rationale:

The FIT agrees key management of the AA allows for situations where the AA will not use an IV, so a use no IV selection was added. The TSS was altered to support the absence of salts, nonces, and IVs. During review of this item an error in FCS_COP.1(f) was discovered, the data encryption SFR application note references key chaining, so this is also corrected.

Further Action:

None.

Action by FDE iTC:

None.