FDE Interpretation # 201702

Status: ☒ *Active* ☐ *Inactive*

Date: 07-05-2017

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 SD V1.0, FDE EE SD V1.0, FDE AA cPP V2.0, FDE EE cPP V2.0, FDE AA SD V2.0, FDE EE SD V2.0

Affected Section(s): FCS_SMV_EXT.1.2, FCS_SMV_EXT.1, FCS_VAL_EXT.1.3, FCS_VAL_EXT.1

Superseded Interpretation(s):

Issue:

Validation attemp threshold config

In FDE v1.0, EE, FCS_SMV_EXT.1.2 requires that the DEK be zeroized after an *administrator configured* number of failed BEV validation attempts, if key zeroization is selected. In FDE v1.0, AA, FCS_VAL_EXT.1.3 echoes the same requirement.

Depending on the FDE device, this configuration ability may not be desirable to the end customer. FDE devices may (and currently do) come with a "hardcoded" threshold of failed BEV validations that cause DEK zeroization.

We would like to ask the TRRT to consider allowing the addition of an assignment this selection of each of the above SFRs. The SFR would allow the zeroization to occur after an administrator-configured number of failed BEV validations *or* ST-defined number of failed BEV validations.

It should be noted that a seperate selection for validation blocking allows for the ST to specify the hard coded failed validation threshold. Since the TOE performs DEK zeroization, and blocking implies the ability to "unblock" at a future time, it is not clear that this selection is intended for this use.

Resolution:

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

FCS_SMV_EXT.1.2 in the FDE EE cPP v1 shall therefore be modified as follows:

The TSF shall [selection: perform a key sanitization of the DEK upon [selection: a configurable number of, [assignment: ST Author specified number of]] consecutive failed validation attempts, institute a delay such that only [assignment: ST Author specified number of attempts] can be made within a 24 hour

period, block validation after a [assignment: ST Author specified number of attempts] of consecutive failed validation attempts]

The operational guidance in FCS_SMV_EXT.1 in the FDE EE SD v1 shall therefore be modified as follows:

[conditional] If configurable, the evaluator shall examine the operational guidance to ensure it describes how to configure the TOE to ensure the limits regarding validation attempts can be established.

[conditional] If ST Author assigned, the evaluator shall examine the operational guidance to ensure it states the values the TOE uses for limits regarding validation attempts.

FCS_VAL_EXT.1.3 in the FDE EE cPP v2 shall therefore be modified as follows:

The TSF shall [selection:

- [perform a key sanitization of the DEK] upon [selection: a configurable number of, [assignment: ST Author specified number of]] consecutive failed validation attempts,
- institute a delay such that only [assignment: ST author specified number of attempts] can be made within a 24 hour period,
- block validation after [assignment: ST author specified number of attempts] of consecutive failed validation attempts,
- require power cycle/reset the TOE after [assignment: ST author specified number of attempts] of consecutive failed validation attempts].

Application Note: “Validation” of the BEV can occur at any point in the key chain, including when the DEK is decrypted. For the purposes of this requirement, validating a key derived from the BEV equates to “validating” the BEV. The purpose of performing secure validation is to not expose any material that might compromise the submask(s).
The TOE validates the BEV prior to allowing the user access to the data stored on the drive. When the key wrap in FCS_COP.1(d) is used, the validation is performed inherently.
The delay must be enforced by the TOE, but this requirement is not intended to address attacks that bypass the product (e.g. attacker obtains hash value or “known” crypto value and mounts attacks outside of the TOE, such as a third party password cracker). The cryptographic functions (i.e., hash, decryption) performed are those specified in FCS_COP.1(b) and FCS_COP.1(f).

FCS_VAL_EXT.1 in the FDE EE SD v2 shall therefore be modified as follows:

[conditional] If the validation functionality is configurable, the evaluator shall examine the operational guidance to ensure it describes how to configure the TOE to ensure the limits regarding validation attempts can be established.

[conditional] If ST Author assigned, the evaluator shall examine the operational guidance to ensure it states the values the TOE uses for limits regarding validation attempts.

The evaluator shall verify that the guidance documentation states which authorization factors are allowed to exit a compliant power saving state.

FCS_VAL_EXT.1.3 in the FDE AA cPP v1 shall therefore be modified as follows:

The TSF shall [selection: issue a key sanitization of the DEK to the EE upon [selection: a configurable number of, [assignment: ST Author specified number of]] consecutive failed validation attempts, institute a delay such that only [assignment: ST Author specified number of attempts] can be made within a 24 hour period, block validation after a [assignment: ST Author specified number of attempts] of consecutive failed validation attempts].

Application Note: The purpose of performing secure validation is to not expose any material that might compromise the submask(s). For the selections in FCS_VAL_EXT.1.1, the ST author must clarify in the KMD which specific entities are referred to in this SFR if multiple entities of a type exist.
The TOE validates the submask(s) (e.g., authorization factor(s)) prior to presenting the BEV to the EE. When a password is used as an authorization factor, it is conditioned before any attempts to validate. In cases where validation of the authorization factor(s) fails, the product will not forward a BEV to EE. When the key wrap in FCS_COP.1(d) is used, the validation is performed inherently.
The delay must be enforced by the TOE, but this requirement is not intended to address attacks that bypass the product (e.g. attacker obtains hash value or “known” crypto value and mounts attacks outside of the TOE, such as a third party password crackers). The cryptographic functions (i.e., hash, decryption) performed are those specified in FCS_COP.1(b), FCS_COP.1(c), and FCS_COP.1(f).
The ST Author may need to iterate this requirement if multiple authentication factors are used, and either different methods are used to validate, or in some cases one or more authentication factors may be validated, and one or more are not validated.

FCS_VAL_EXT.1 in the FDE AA SD v1 shall therefore be modified as follows:

[conditional] The evaluator shall examine the operational guidance to ensure it describes how to configure the TOE to ensure the limits regarding validation attempts can be established.

[conditional] If ST Author assigned, the evaluator shall examine the operational guidance to ensure it states the assignments the TOE uses for limits regarding validation attempts.

FCS_VAL_EXT.1.3 in the FDE AA cPP v2 shall therefore be modified as follows:

The TSF shall [selection:

- issue a key sanitization of the DEK to the EE upon [selection: a configurable number of, [assignment: ST Author specified number of]] consecutive failed validation attempts,
- institute a delay such that only [assignment: ST author specified number of attempts] can be made within a 24 hour period,
- block validation after [assignment: ST author specified number of attempts] of consecutive failed validation attempts,
- require power cycle/reset the TOE after [assignment: ST author specified number of attempts] of consecutive failed validation attempts].

Application Note: The purpose of performing secure validation is to not expose any material that might compromise the submask(s). For the selections in FCS_VAL_EXT.1.1, the ST author must clarify in the KMD which specific entities are referred to in this SFR if multiple entities of a type exist.
The TOE validates the submask(s) (e.g., authorization factor(s)) prior to presenting the BEV to the EE. When a password is used as an authorization factor, it is conditioned before any attempts to validate. In cases where validation of the authorization factor(s) fails, the product will not forward a BEV to EE. When the key wrap in FCS_COP.1(d) is used, the validation is performed inherently.
The delay must be enforced by the TOE, but this requirement is not intended to address attacks that bypass the product (e.g. attacker obtains hash value or "known" crypto value and mounts attacks outside of the TOE, such as a third party password crackers). The cryptographic functions (i.e., hash, decryption) performed are those specified in FCS_COP.1(b), FCS_COP.1(c), and FCS_COP.1(f).

The ST author may need to iterate this requirement if multiple authentication factors are used, and either different methods are used to validate, or in some cases one or more authentication factors may be validated, and one or more are not validated.

FCS_VAL_EXT.1 in the FDE AA SD v2 shall therefore be modified as follows:

[conditional] If the validation functionality is configurable, the evaluator shall examine the operational guidance to ensure it describes how to configure the TOE to ensure the limits regarding validation attempts can be established.

[conditional] If ST Author assigned, the evaluator shall examine the operational guidance to ensure it states the assignments the TOE uses for limits regarding validation attempts.

Rationale:

This is in reference to FCS_SMV_EXT.1.2 in the EE and FCS_VAL_EXT.1.3 in the AA. Version 1.

Initially discussed having minimum value, but we allow other selections to be assigned by the ST author.

Noted that the possibility of denial of service is a real threat. This is the reason we do not want just ST author assignment as the only option.

Agreed upon making a selection of ST author assignment or admin configurable.

The operational guidance in the supporting document needs to be updated as well.

Further Action:

None

Action by FDE iTC:

This was sent out the FDE iTC and no additional comments were received.