FDE Interpretation # 202205

Status: ☒ *Active* □ *Inactive*

Date: 06-08-2022

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_PCC_EXT.1

Superseded Interpretation(s):

Issue:

FCS_PCC_EXT.1 only allows PBKDF with an iteration count equal or greater than 1000; however, there are additional ways a password can be stretched into a key while mitigating a brute force attack.

NIAP has issued TD0366 (https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0366) for the equivalent SFR in PP_MD_V3.1 to read:

> FCS_COP.1.1(5): The TSF shall perform conditioning in accordance with a specified cryptographic algorithm HMAC-[selection: SHA-256, SHA-384, SHA-512]] using a salt, and [selection: PBKDF2 with [assignment: number of iterations] iterations, [assignment: key stretching function], no other functions] and output cryptographic key sizes [selection: 128, 256] that meet the following: NIST [selection: SP 800-132, no standard].

Can this change be made to CPP_FDE_AA_V2.0E?

Resolution:

This replaced the original 202205 a minor error in the correction was missed.

The FIT has determined this be a valid, yet non-standard for software only approach to this problem. The FIT recommends the follow change until the affected FDE cPPs are updated with DSC support:

FCS_PCC_EXT.1.1 A password used by the TSF to generate a password authorization factor shall enable up to [assignment: positive integer of 64 or more] characters in the set of {upper case characters, lower case characters, numbers, and [assignment: other supported special characters]} and shall perform Password-Based Key Derivation Functions in accordance with a specified cryptographic algorithm HMAC-[selection: SHA-256, SHA-384, SHA-512], with[selection: [assignment: positive integer of 1000 or more] iterations, [assignment: positive integer of 1 or more] and [assignment: positive integer of 10000 or more] subsequent rounds of AES operations with a device key and PBKDF2 output per FCS_COP.1(g) or FCS_COP.1(e)], and output cryptographic key sizes [selection: 128 bits, 256 bits] that meet the following: [NIST SP 800-132].

Rationale:

The FIT wants to allow for hardware support in the future, where the PBKDF2 requirement could exist alongside rate-limiting approaches. This supports one such design for an approach and the software work-load for this solution is larger than the work-load associated with a 1000 iteration PBKDF2 solution.

Further Action:

None.

Action by FDE iTC:

Review by FDE iTC for approval of TD.