HCD0001 - Clarification is needed about algorithm verification of Root of Trust in the Test Assurance activities for the Secure Boot SFR

Version: 1, Published: 2024-01-12

Impacted Documents

CPP_HCD_V1.0_supporting_doc

References

FCS_COP.1/Hash Cryptographic operation (Hash Algorithm)

FCS_COP.1/SigGen Cryptographic Operation (for signature generation/verification)

FCS_COP.1/KeyedHash Cryptographic Operation (for keyed-hash message authentication)

FCS_COP.1/DataEncryption Cryptographic Operation (Symmetric encryption/decryption)

FCS_COP.1/StorageEncryption Cryptographic operation (Data Encryption/Decryption)

FCS_COP.1/CMAC Cryptographic Operation (for keyed-hash message authentication)

Issue Description

The Root of Trust (FPT_SBT_EXT.1.1) shall be implemented in immutable code or be protected by a HW-based protection mechanism. As a result, it would be difficult to perform cryptographic algorithm validation testing of the cryptographic algorithm(s) implemented in the Root of Trust, and therefore, should be avoided.

Resolution

In cPP_HCD_V1.0, the following SFRs are listed as dependencies for FPT_SBT_EXT.1:

- FCS_COP.1/Hash Cryptographic operation (Hash Algorithm)
- FCS_COP.1/SigGen Cryptographic Operation (for signature generation/verification)
- FCS_COP.1/KeyedHash Cryptographic Operation (for keyed-hash message authentication)
- FCS_COP.1/DataEncryption Cryptographic Operation (Symmetric encryption/decryption)

- FCS_COP.1/StorageEncryption Cryptographic operation (Data Encryption/Decryption)
- FCS_COP.1/CMAC Cryptographic Operation (for keyed-hash message authentication)

In CPP_HCD_V1.0_supporting_doc, add the following note in the Test section for each FCS_COP.1 SFR above:

Note: The tests detailed below are not required to be performed for cryptographic functions implemented in the Root of Trust for Secure Boot (FPT_SBT_EXT.1).

CPP_HCD_V1.0_supporting_doc

The SD is updated as follows (yellow highlights for additions, strikethrough for deletions) per section that is being updated:

2.2.5.3 Tests

Note: The tests detailed below are not required to be performed for cryptographic functions implemented in the Root of Trust for Secure Boot (FPT_SBT_EXT.1).

2.2.6.3. Tests

The evaluator shall include test cases of FCS_COP.1/SigGen to the test subset. Note that FCS_COP.1/SigGen may be not mapped to the specific interface(s) after evaluator's analysis during ADV_FSP.1.

The evaluator shall produce test documentation for test cases of FCS_COP.1/SigGen. If there is no explicit external interface(s) mapped to FCS_COP.1/SigGen, the evaluator shall employ an alternative test approach (refer to CEM, section 15.2.2.).

Each section below contains tests the evaluators shall perform for each selected digital signature scheme. Based on the assignments and selections in the requirement, the evaluators choose the specific activities that correspond to those selections.

Note: The tests detailed below are not required to be performed for cryptographic functions implemented in the Root of Trust for Secure Boot (FPT_SBT_EXT.1).

2.2.7.3. Tests

The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit-oriented mode. In this mode the TSF hashes messages of arbitrary length. As there are different tests for each mode, an indication is given in the following sections for the bit-oriented vs. the byte-oriented test mode.

The evaluator shall perform all of the following tests for each hash algorithm implemented by the TSF and used to satisfy the requirements of this cPP.

Note: The tests detailed below are not required to be performed for cryptographic functions implemented in the Root of Trust for Secure Boot (FPT_SBT_EXT.1).

5.1.1.3. Tests

The following tests are conditional based upon the selections made in the SFR.

Note: The tests detailed below are not required to be performed for cryptographic functions implemented in the Root of Trust for Secure Boot (FPT_SBT_EXT.1).

5.2.9.3. Tests

Note: The tests detailed below are not required to be performed for cryptographic functions implemented in the Root of Trust for Secure Boot (FPT_SBT_EXT.1).

5.3.3.4. Tests

Note: The tests detailed below are not required to be performed for cryptographic functions implemented in the Root of Trust for Secure Boot (FPT_SBT_EXT.1).

Tracking

Issue #2