

HCD0009 - Clarification on Tests assurance activity for FPT_TST_EXT.1 TSF testing

Version: 1, Published: 2024-02-05

Impacted Documents

CPP_HCD_V1.0_supporting_doc

References

FPT_TST_EXT.1 TSF testing

Issue Description

The Tests assurance activity for FPT_TST_EXT.1 TSF testing lacks clarification and context to avoid overlap with the Tests assurance activity for FPT_SBT_EXT.1 Secure Boot and limit the scope to verifying the execution of self-tests.

Resolution

Update Tests assurance activity for FPT_TST_EXT.1 TSF testing to avoid overlap with the Tests assurance activity for FPT_SBT_EXT.1 Secure Boot and limit the scope to verifying the execution of self-tests.

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:

2.6.4.3. Tests

~~The evaluator with assistance from the vendor (if needed) shall confirm that when an error in the self-test results is induced into the TOE, the TOE no longer enters into operational mode. For example, DRGB self-test is a self-test function.~~

Although formal compliance is not mandated, the self-tests performed should aim for a level of confidence comparable to:

- [FIPS 140-2], chap. 4.9.1, Cryptographic algorithm test for the verification of the correct

operation of cryptographic functions. Alternatively, national requirements of any CCRA member state for the security evaluation of cryptographic functions should be considered as appropriate.

The evaluator shall either verify that the self-tests described above are carried out during initial start-up or that the developer has justified any deviation from this.

Tracking

Issue #22