HCD0008 - Clarification on applicability of tests 3 and 4 for FDP_DSK_EXT.1 Protection of Data on Disk

Version: 1, Published: 2024-02-05

Impacted Documents

CPP_HCD_V1.0_supporting_doc

References

FDP_DSK_EXT.1 Protection of Data on Disk

Issue Description

Tests 3 and 4 for FDP_DSK_EXT.1 Protection of Data on Disk are only applicable when the ST author claims FPT_WIPE_EXT.1 Data Wiping.

Resolution

Update tests 3 and 4 for FDP_DSK_EXT.1 Protection of Data on Disk to clarify the tests are only applicable when the ST author claims FPT_WIPE_EXT.1 Data Wiping.

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:

3.1.3.4. Tests

The evaluator shall perform the following tests:

Test 1. Write data to Storage device: Perform writing to the storage device with operating TSFI which enforce write process of User documents and Confidential TSF data.

Test 2. Confirm that written data are encrypted: Verify there are no plaintext data present in the encrypted range written by Test 1; and, verify that the data can be decrypted by proper key and key material.

All TSFIs for writing User Document Data and Confidential TSF data should be tested by above Test 1 and Test 2.

Test 3. ~~(If data other than D.USER.DOC and D.TSF.CONF are encrypted,) write~~ [Conditional: If the ST author claims FPT_WIPE_EXT.1 with cryptographic erase, and if data other than D.USER.DOC and D.TSF.CONF are encrypted] Write the data to the storage device with operating TSFI which enforce write process of the data.

Test 4. ~~(If data other than D.USER.DOC and D.TSF.CONF are encrypted,) verify~~ [Conditional: If the ST author claims FPT_WIPE_EXT.1 with cryptographic erase, and if data other than D.USER.DOC and D.TSF.CONF are encrypted] Verify that the data written in Test 3 is not in plaintext form; and verify that the data can be decrypted by proper key and key material.

Tracking

Issue #21