Network Device Interpretation # 202401

Redundant requirements in FPT_TST_EXT.1

Status: ☒ *Active* □ *Inactive*

Date: *17-Apr-2024*

End of proposed Transition Period (to be updated after TR2TD process): *17-May-2024*

Type of Change: □ Immediate application ☒ Minor change □ Major change

Type of Document: ☒ *Technical Decision* ☒ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* ☒ *Network iTC*

Affected Document(s): *NDcPP v3.0e, ND SD v3.0e*

Affected Section(s): *FPT_TST_EXT.1*

Superseded Interpretation(s): *None*

Issue:

Issue:

In the SFR FPT_TST_EXT.1.1 of NDcPP v3.0e

"The TSF shall run a suite of the following self-tests [selection:

- During initial start-up (on power on) to verify the integrity of the TOE firmware and software;
- During start-up (prior to providing any cryptographic services) and [selection: at no other time, on-demand, continuously, [assignment: conditions under which self-tests should occur]] to verify correct operation of cryptographic implementation necessary to fulfil the TSF;
- [selection: no other, start-up, on-demand, continuous, at the conditions [assignment: conditions under which self-tests should occur]] self-tests [assignment: describe self-test objective].

to demonstrate the correct operation of the TSF: [assignment: list of self-tests run by the TSF] and if failure detected [assignment: describe resulting error state]."

all self-tests are being listed in the bulleted points, with the first two covering firmware/software integrity and cryptographic implementation respectively, and the third point giving one the flexibility to list out other self-tests implemented by the TOE, if any. This seems to make the assignment ('list of self-tests run by the TSF') below the bulleted points redundant since all self-tests will already get covered by the bulleted points.

Proposed resolution:

Since all selftests will already get covered by the bulleted points, there seems to be no need of having the subsequent assignment, and could hence be removed.

If keeping the assignment was intentional, the current application note could be updated to clarify the rationale behind having this subsequent assignment.

Resolution:

The NIT has analyzed the SFR for FPT_TST_EXT.1.1 and FPT_TST_EXT.1.2 and came to the conclusion that during the integration of the update proposal for FPT_TST_EXT.1 as provided by the MINT some editorial mistakes have been made which need to be corrected. In particular, the following issues have been identified:

The '[selection:' before the bullet points in FPT_TST_EXT.1.1 was not part of the MINT proposal and needs to be removed. This makes all three bullet points mandatory.

The information how the TOE reacts to failures of self-tests needs to be provided by the ST author. But the corresponding requirement has been added twice to FPT_TST_EXT.1 - on the one hand at the end of FPT_TST_EXT.1.1 (": [assignment: list of self-tests run by the TSF] and if failure detected [assignment: describe resulting error state].") and on the other hand in more detail in FPT_TST_EXT.1.2 (full SFR). To avoid redundancy the less detailed requirement in FPT_TST_EXT.1.1 needs to be removed.

The Application Note for FPT_TST_EXT.1.1 needs to be updated to properly cover the changes applied to the SFR.

An Application Note for FPT_TST_EXT.1.2 needs to be added.

Several inconsistencies related to self-tests need to be corrected.

As a result, the following changes shall be applied:

For FPT_TST_EXT.1.1

{old}

"The TSF shall run a suite of the following self-tests [selection:

- During initial start-up (on power on) to verify the integrity of the TOE firmware and software;
- During start-up (prior to providing any cryptographic services) and [selection: at no other time, on-demand, continuously, [assignment: conditions under which self-tests should occur]] to verify correct operation of cryptographic implementation necessary to fulfil the TSF;
- [selection: no other, start-up, on-demand, continuous, at the conditions [assignment: conditions under which self-tests should occur]] self-tests [assignment: describe self-test objective].

to demonstrate the correct operation of the TSF: [assignment: list of self-tests run by the TSF] and if failure detected [assignment: describe resulting error state]."

{/old}

shall be replaced by

{new}

"The TSF shall run a suite of the following self-tests:

- During initial start-up (on power on) to verify the integrity of the TOE firmware and software;
- Prior to providing any cryptographic service and [selection: at no other time, on-demand, continuously, [assignment: conditions under which self-tests should occur]] to verify correct operation of cryptographic implementation necessary to fulfil the TSF;
- [selection: no other, start-up, on-demand, continuous, at the conditions [assignment: conditions under which self-tests should occur]] self-tests [assignment: 'list an identifier for each self-test that is additional to those identified in the first two bullet points'].

to demonstrate the correct operation of the TSF."

{/new}

The Application Note for FPT_TST_EXT.1.1 shall be updated as follows:

{old}

It is expected that self-tests are carried out during initial start-up of the TOE (physical or virtual power on). Other options should only be used if the developer can justify why they are not carried out during initial start-up. It is expected that at least self-tests for verification of the integrity of the TOE firmware and software as well as for the correct operation of cryptographic functions necessary to fulfil the SFRs will be performed. If not, all self-tests are performed during start-up multiple iterations of this SFR are used with the appropriate options selected. In future versions of this cPP the suite of self-tests will be required to contain at least mechanisms for measured boot including self-tests of the components which perform the measurement.

Non-distributed TOEs may internally consist of several components that contribute to enforcing SFRs. Self-testing shall cover all components that contribute to enforcing SFRs and verification of integrity shall cover all software that contributes to enforcing SFRs on all components.

For distributed TOEs all TOE components have to perform self-tests. This does not necessarily mean that each TOE component has to carry out the same self-tests: the ST describes the applicability of the selection (i.e. when self-tests are run) and the final assignment (i.e. which self-tests are carried out) to each TOE component.

{/old}

shall be replaced by

{new}

For the third bullet point the following restriction applies: If, and only if 'no other' is selected in the selection, 'none' may be used in the second assignment.

Non-distributed TOEs may internally consist of several components that contribute to enforcing SFRs. Self-testing shall cover all components that contribute to enforcing SFRs and verification of integrity shall cover all software that contributes to enforcing SFRs on all components.

For distributed TOEs all TOE components have to perform self-tests. This does not necessarily mean that each TOE component has to carry out the same self-tests.

{/new}

For FPT_TST_EXT.1.2 the following Application Note shall be added.

{new}

For all failed self-tests related to enforcing SFRs as defined in FPT_TST_EXT1.1 the reaction of the TOE to the failure needs to be specified. On the one hand, FPT_TST_EXT.1.2 allows to model TOEs that react to all failures of self-tests related to enforcing SFRs the same way be selecting 'all failures' in the first selection and selection of the corresponding reaction of the two in the second selection. On the other hand, it allows to model TOEs that react differently to different failures of self-tests to enforcing SFRs by specifying the list of failures in the first selection and the corresponding reaction of the TOE in the second selection. In the latter case, it shall be clear which failure of a self-test causes which behavior of the TOE.

{/new}

The description in section 4.1.5 should have been updated together with the update of the SFR to match the updated SFR. This seems to be an oversight. The description in section 4.1.5 shall be updated as follows.

{old}

Security mechanisms of the Network Device generally build up from roots of trust to more complex sets of mechanisms. Failures could result in a compromise to the security functionality of the device. A Network Device self-testing its security critical components at both start-up and during run-time ensures the reliability of the device’s security functionality.

{/old}

shall be replaced by

{new}

Security mechanisms of the Network Device generally build up from roots of trust to more complex sets of mechanisms. Failures could result in a compromise to the security functionality of the device. A Network Device self-testing its security critical components ensures the reliability of the device’s security functionality.

{/new}

As a result to the changes to the SFR in NDcPPv3.0e, the following changes shall be applied to ND SD v3.0e.

The first sentence of section 2.5.3.1, item 187 shall be changed as follows.

{old}

The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used).

{/old}

shall be replaced by

{new}

The evaluator shall examine the TSS to ensure that it details each of the self-tests that are identified by the SFR; this description shall include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used).

{/new}

Section 2.5.3.3, item 193 shall be updated as follows.

{old}

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.

{/old}

shall be replaced by

{new}

The evaluator shall verify that the self-tests described above are carried out according to the SFR and in agreement with the descriptions in the TSS.

{/new}

Rationale:

see Resolution section

Further Action:

None

Action by Network iTC:

None