Network Device Interpretation # 202005

Update Verification Inconsistency

Status: ☒ *Active* ☐ *Inactive*

Date: *7-Apr-2020*

End of proposed Transition Period (to be updated after TR2TD process): *7-Apr-2020*

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): *ND SDv2.1, ND SDv2.2*

Affected Section(s): *AGD_OPE.1*

Superseded Interpretation(s): *None*

Issue:

ISSUE:

The Evaluator Activity for AGD_OPE.1 (Supporting Document Section 5.3.1.5) makes a statement that suggests that only update verification using a digital signature is allowed; however, FPT_TUD_EXT.1.3 allows for the selection of digital signature or published hash for validation of updates.

DETAILS:

The SD, Section 5.3.1.5.b (AGD_OPE.1) seems to mandate digital signatures with the following statement in the evaluator activity:

"b) The documentation must describe the process for verifying updates to the TOE by verifying a digital signature."

The literal interpretation is that digital signature validation must be described in the AGD. The intent of the requirement appears to be that procedures regarding how to verify updates using either digital signature or hash validation are provided in the guidance documentation as indicated in the SD Section 5.3.1.5.b.2.

RECOMMENDATION:

Modify the following wording in the SD, Section 5.3.1.5.b from:

 "b) The documentation must describe the process for verifying updates to the TOE by verifying a digital signature. The evaluator shall verify that this process includes the following steps:" ; to:

"b) The documentation must describe the process for verifying updates to the TOE for each method selected for FPT_TUD_EXT.1.3 in the Security Target. The evaluator shall verify that this process includes the following steps:"

Resolution:

To address the issue raised above, the following changes shall be applied to ND SDv2.1/v2.2, section 5.3.1.5 b. The paragraph

<old>

The documentation must describe the process for verifying updates to the TOE by verifying a digital signature. The evaluator shall verify that this process includes the following steps:

</old>

shall be replaced by

<new>

The documentation must describe the process for verifying updates to the TOE for each method selected for FPT_TUD_EXT.1.3 in the Security Target. The evaluator shall verify that this process includes the following steps:

</new>

Rationale:

See Issue section

Further Action:

None

Action by Network iTC:

None