Network Device Interpretation # 16

Inconsistency between FMT_SMF.1 and FPT_TUD_EXT.1.3

Status: ☒ *Active* ☐ *Inactive*

Date: *6-Jun-2016*

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

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

Affected Document(s): *NDcPP V1.0, FWcPP V1.0*

Affected Section(s): *FMT_SMF.1*

Superseded Interpretation(s): *None.*

Issue:

FPT_TUD_EXT.1.3 and FMT_SMF.1 are inconsistent.

FPT_TUD_EXT.1.3 (trusted update) allows for the selection of a digital signature mechanism and/or a published hash mechanism.

FMT_SMF.1 contains the following mandatory digital signature requirement for updates:

"Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates;"

It would seem that this FMT_SMF.1 requirement should only apply when a digital signature mechanism is selected in FPT_TUD_EXT.1.3.

Resolution:

The omission of published hashes from FMT_SMF.1 was an oversight. Published hashes should be included along with digital signatures as an acceptable option in FMT_SMF.1.

Changes to the cPPs:

Addition to the FMT_SMF.1.1 SFR:

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*

- *Ability to update the TOE, and to verify the updates using [selection: digital signature, hash comparison] capability prior to installing those updates;*
- *[selection:*
    - *Ability to configure audit behavior;*
    - *Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;*
    - *Ability to configure the cryptographic functionality;*
    - *No other capabilities.]*

Rationale:

The iTC intended to allow for digital signatures or published hashes to be used when authenticating updates to the TOE. FPT_TUD_EXT.1.3 currently includes a selection to allow for this choice, but FMT_SMF.1 mistakenly states that updates must be verified only by digital signatures.

Modifying this SFR does not change any functionality permitted by the cPPs as published hashes are already permitted in FPT_TUD_EXT.1.3.

Further Action:

Update the ND cPP V1.0 and FW cPP V1.0 as proposed.

No changes are needed to the ND SD V1.0 or FW SD V1.0 as all evaluation activities associated with FMT_SMF.1 are described in the relevant SFRs for the security functionality (FPT_TUD_EXT.1.3 in this case).

Action by Network iTC:

Update the draft ND cPP V2.0 and draft FW cPP V2.0 as proposed.