Network Device Interpretation # 30

Optional use of X.509 certificates for digital signatures

Status: ☒ *Active* ☐ *Inactive*

Date: *27-Jun-2016*

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

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

Affected Document(s): *ND cPP V1.0, FW cPP V1.0*

Affected Section(s): *FPT_TUD_EXT.1; FPT_TUD_EXT.2*

Superseded Interpretation(s): *None*

Issue:

The NDcPP_SIP_EP does not seem to be consistent with the NDcPP on the use of X.509 certificates in TOE updates.

The NDcPP allows a developer to use digital signatures, when performing software and firmware updates, without using X.509 certificates. This can be seen in application notes 33, 35 and 36.

The NDcPP_SIP_EP in Section 4.2.1.5 indicates that the use of digital signatures, in TOE updates, mandates the use of X.509 certificates. "This also triggers the inclusion of the NDcPP's selection-based SFR FPT_TUD_EXT.2 as specified in the NDcPP."

Please clarify if X.509 certificates are required when a digital signature is employed for TOE updates in order to comply with the NDcPP.

Please clarify if X.509 certificates are required when a digital signature is employed for TOE updates in order to comply with the NDcPP_SIP_EP.

Resolution:

The use of X.509 certificates is not mandated when a digital signature is employed for TOE updates in order to comply with the FPT_TUD_EXT.1 requirements.

PP_NDCPP_SIP_EP_V2.0 is beyond the scope of the NIT. NIAP has published a clarification at https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=80

Rationale:

Signing a binary does not imply a certificate has to be used. Application notes 20, 35, 36 and 92 all imply the author intended that signatures could be used without requiring X.509 certificates.

Further Action:

None

Action by Network iTC:

None