Network Device Interpretation # 201610

Handling of X.509 certificates when ssh-rsa is used for all remote communication

Status: ☒ *Active* □ *Inactive*

Date: *15-Feb-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): *FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3*

Superseded Interpretation(s): *None.*

Issue:

NDcPP V1.0 requires several SFRs related to digital certificates including, FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3. However, it is possible for a product to only select cryptographic services that do not rely upon digital certificates. Specifically, if all remote communication (both with remote servers and remote administrators) use SSH with "ssh-rsa" and the TOE does not use digital certificates for trusted updates then the FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3 requirements are not applicable to any required services provided by the TOE. In this scenario, it does not make sense for the FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3 requirements to be mandatory.

Resolution:

NIT recommends to move the FIA_X509_EXT SFRs to Annex B and make them selection-based requirements. This RfI requires input by the overall Network iTC to gather enough information about the different use cases and selection scenarios.

Rationale:

N/A

Further Action:

- Hand over to Network iTC.

Action by Network iTC: