Network Device Interpretation # RFI201840

Clarification about application of RfI#201726rev2

Status: ☒ *Active* □ *Inactive*

Date: *20-May-2019*

End of proposed Transition Period (to be updated after TR2TD process): *20-Jun-2018*

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): *NDcPPv2.0e, FWcPPv2.0e, NDcPPv2.1*

Affected Section(s): *FIA_X509_EXT.3*

Superseded Interpretation(s): *None*

Issue:

In https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/NITDecisionRfI201726rev2.pdf, the rationale states "If a TOE does not need to present an X.509 certificate to another endpoint via the TSF, there is no need for the TOE to request an X.509 certificate in the first place." The term "endpoint" implies machine-oriented consumption and subsequent validation of the presented certificate. However, in the Resolution section of the decision, it states "…only needs to be able to generate a Certification Request if the TOE needs to present an X.509 certificate to another endpoint via the TSF for authentication (i.e. if at least one of the following SFRs is included in the ST: FCS_DTLSC_EXT.2, FCS_DTLSS_EXT.1, FCS_DTLSS_EXT.2, FCS_IPSEC_EXT.1, FCS_SSHC_EXT.1.5 (applicable only if at least one of the x509v3- ciphers is selected), FCS_SSHS_EXT.1.5 (applicable only if at least one of the x509v3-* ciphers is selected), FCS_TLSC_EXT.2, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2)."*

If FCS_TLSS_EXT.1 is claimed for the purposes of fulfilling a management GUI trusted path to be used directly by a human operator, then it seems odd that FIA_X509_EXT.3 will be required in this case. A human operator is not "an endpoint" and will not be validating the X.509 certificate in a structured, formal way each time.

It appears the FIA_X509_EXT.3 should be optional in the case where a web GUI needs to present an X.509 certificate to a human user.

Resolution:

The use of 'endpoint' and 'external IT entities' terms in RFI201726rev2 were not intended to restrict the statements applicability to machine-to-machine connections. The RfI explicitly refers to the requirements *for TLS Servers. A TLS Server is expected to be capable of authenticating itself to external IT entities using X.509 certificates – independently whether mutual authentication is supported (FCS_TLSS_EXT.2) or not (FCS_TLSS_EXT.1) and independently whether the communication takes place over a trusted channel, a trusted path or Inter-TOE communication (distributed TOEs). Therefore a TLS Server shall also be capable of generating Certificate Requests which implies that FIA_X509_EXT.3 needs to be claimed.*

The following paragraph shall be added to the general text for chapter B3.1.3 (NDcPPv2.0e, FWcPPv2.0e)/B.4.1.3 (NDcPPv2.1)

This element must be included in the ST if X.509 certificates are used as part of FTP_ITC.1, FTP_TRP.1/Admin, or FPT_ITT.1 where the TOE authenticating itself to external IT entities, administrators, or distributed components.

Rationale:

See issue section.

Further Action:

None

Action by Network iTC:

None