Network Device Interpretation # 202007

Incorrect reference to FCS_TLSC_EXT.2.3

Status: ☐ *Active* ☐ *Inactive*

Date: *15-May-2020*

End of proposed Transition Period (to be updated after TR2TD process): *15-May-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): *NDcPPv2.2*

Affected Section(s): *FIA_X509_EXT.2.2*

Superseded Interpretation(s): *None*

Issue:

Application Note 113 for FIA_X509_EXT.2.2 in NDcPPv2.2 has a reference to FCS_TLSC_EXT.2.3:

"The selection should be consistent with the validation requirements in FCS_IPSEC_EXT.1.14, FCS_TLSC_EXT.1.3 and FCS_TLSC_EXT.2.3".

This seems to be left over from NDcPPv2.1 as TLS requirement have been restructured in NDcPPv2.2. The reference should probably just be changed to: "FCS_IPSEC_EXT.1.14 and FCS_TLSC_EXT.1.3"

The references are confusing, though. FIA_X509_EXT.2.2 is about what to do in the case where a CRL download or OCSP isn't available for certificate validation. The application note talks about validation rules, but IPSEC.1.14 does specify validation rules. In addition, the relation to the SFR remains unclear. Also, FCS_TLSC_EXT.1.3 isn't about validation, it's about override, but this makes more sense in the context of the SFR.

Resolution:

The NIT acknowledges that the references to the single SFR elements of the secure communication protocols is error prone and should therefore be generalized. At the same time a missing reference to DTLS should be added to the first paragraph of the application note. Therefore, the following changes should be performed:

The first sentence of the first paragraph in Application Note 113 shall modified as follows:

<old>

In FIA_X509_EXT.2.1, the ST author's selection includes IPsec, TLS, or HTTPS if these protocols are included in FTP_ITC.1.1 or FPT_ITT.1.

</old>

shall be replaced by

<new>

In FIA_X509_EXT.2.1, the ST author's selection includes IPsec, (D)TLS, or HTTPS if these protocols are included in FTP_ITC.1.1 or FPT_ITT.1.

</new>.

The last sentence of the second paragraph in Application Note 113 shall be modified as follows:

<old>

The selection should be consistent with the validation requirements in FCS_IPSEC_EXT.1.14, FCS_TLSC_EXT.1.3 and FCS_TLSC_EXT.2.3.

</old>

shall be replaced by

<new>

The selection should be consistent with the validation requirements for the secure communication protocols.

</new>

Rationale:

See Issue section.

Further Action:

None

Action by Network iTC:

None