Network Device Interpretation # 202001

Clarification about digital signature algorithms for FTP_TUD.1

Status: ☒ *Active* ☐ *Inactive*

Date: *24-Feb-2020*

End of proposed Transition Period (to be updated after TR2TD process): *24-Feb-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): *NDcPPv2.1*

Affected Section(s): *FTP_TUD.1*

Superseded Interpretation(s): *None*

Issue:

NDcPP v2.2 includes the following element describing supported trusted update:

"FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a [selection: … digital signature …] prior to installing those updates."

NDcPP v2.2 Application Note 31 includes the following explanation:

"The ST author selects 'digital signature' for all other digital mechanisms (e.g. X.509 certificates that do not meet FIA_X509_EXT.1/Rev, GPG, raw public key). The digital algorithm must be one of the algorithms specified in FCS_COP.1/SigGen."

NDcPPv2.1 Application Note 32 lacks clear "must be" statement. Please confirm whether NDcPPv2.1 also intended to exclude any signed updates implementations that are not based on RSA or ECDSA schemes.

Resolution:

The corresponding statement in NDcPPv2.1 Application Note 32 says " The digital signature mechanism referenced in the selection of FPT_TUD_EXT.1.3 is one of the algorithms specified in FCS_COP.1/SigGen." The NIT regards the statements "is one of the algorithms" (NDcPPv2.1) and "must be one of the algorithms" (NDcPPv2.2) as equivalent. So, also for NDcPPv2.1 the digital algorithm must be one of the algorithms specified in FCS_COP.1/SigGen. This decision does not update NDcPPv2.1/2.2.

Rationale:

Provided in the Resolution section.

Further Action:

None

Action by Network iTC:

None