Network Device Interpretation # 201611rev2

Using secp521r1 for TLS communication

Status: ☒ *Active* ☐ *Inactive*

Date: *10-Apr-2017*

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): *FCS_TLSS_EXT.1.3, FCS_TLSS_EXT.2.3*

Superseded Interpretation(s): *RfI#201611, Feb 15 2016*

Issue:

NDcPP V1.0: Regarding Eliptic curve cryptography (ECC) and TLS, was secp521r1 intentionally left out of FCS_TLSS_EXT.1.3 and FCS_TLSS_EXT.2.3 or can an ST author add secp521r1 to these elements?

Resolution:

The NIT acknowledges the problem specified in the Issue section. FCS_TLSS_EXT.1.3 and FCS_TLSS_EXT.2.3 shall therefore be modified as follows:

"The TSF shall generate key establishment parameters using RSA with key size 2048 bits and [selection: *3072 bits, 4096 bits, no other size*] and *[selection: over NIST curves [selection: secp256r1, secp384r1, secp521r1] and no other curves; Diffie-Hellman parameters of size 2048 bits and [selection: 3072 bits, no other size]; no other]*."

Rationale:

N/A

Further Action:

None.

Action by Network iTC: