Network Device Interpretation # 201602rev2

Make elliptic curves P-256 and P-384 optional for signature generation and signature verification

Status: ☒ *Active* ☐ *Inactive*

Date: *21-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_COP.1(2) (to be renamed to FCS_COP.1/SigGen in NDcPP V2.0)*

Superseded Interpretation(s): *RfI#(2016)02, 15-Feb-2016*

Issue:

NDcPP V1.0 FCS_COP.1.1(2) requires signature generation and signature verification of NIST curves P-256 and P-384, yet all of the other elliptic curve SFRs (e.g., FCS_CKM.1, FCS_SSHC_EXT.1, FCS_SSHS_EXT.1, FCS_TLSC_EXT.1, FCS_TLSC_EXT.2) in this cPP allow P-256 and P-384 to be optional and, thus, possibly never selected. Was it intended for P-256 and P-384 to be required by FCS_COP.1.1(2) even though no other SFRs require it or should P-256 and P-384 be selectable in FCS_COP.1.1(2) in the way that P-521 is selectable?

Resolution:

The NIT acknowledges the issue described in the 'Issue' section above. FCS_COP.1.1(2) shall therefore be modified as follows:

FCS_COP.1.1(2) The TSF shall perform *cryptographic signature services (generation and verification)* in accordance with a specified cryptographic algorithm [selection:

- *RSA Digital Signature Algorithm and cryptographic key sizes **(modulus)** [assignment: 2048 bits or greater]*,
- *Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [assignment: 256 bits or greater]*

]

that meet the following: [selection:

- *For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,*

- *For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [selection: P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4*

].

The application note for FCS_COP.1.1(2) shall be replaced by the following:

The ST Author chooses the algorithm(s) implemented to perform digital signatures. For the algorithm(s) chosen, the ST author makes the appropriate assignments/selections to specify the parameters that are implemented for that algorithm. The ST author ensures that the assignments and selections for this SFR include all the parameter values necessary for the cipher suites selected for the protocol SFRs (see Appendix B.2.1) that are included in the ST. The ST Author checks for consistency of selections with other FCS requirements, especially when supporting elliptic curves.

Rationale:

N/A

Further Action:

None.

Action by Network iTC: