Network Device Interpretation # 45

Typo in reference to RSASSA-PKCS1v1_5

Status: ☒ *Active* ☐ *Inactive*

Date: *27-Sep-2016*

Type of Document: ☒ *Technical Decision* ☐ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* ☐ *Network iTC*

Affected Document(s): *ND cPP V1.0, FW cPP V1.0*

Affected Section(s): *FCS_COP.1.1(2)*

Superseded Interpretation(s): *None*

Issue:

In NDcPP v1.0 FCS_COP.1(2) reads:

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 RSASSAPKCS2v1_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" P-256, P-384, and [selection: P- 521, no other curves]; ISO/IEC 14888-3, Section 6.4].

<u>A vendor has pointed out that the statement:</u>

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 RSASSAPKCS2v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,

Contains a flaw; specifically, the standard RSASSA-PKCS2v1_5 does not exist. This should be corrected to RSASSA-PKCS1v1_5, as referenced in RFC 3447. Is it permissible to make this correction to the language of the SFR?

Resolution:

The NIT confirms that this is a typo in the reference to the PKCS#1 standard. The reference 'RSASSA-PKCS2v1_5' shall be replaced by ' RSASSA-PKCS1v1_5' when writing a Security Target based on NDcPP v1.0 or FWcPP v1.0.

Rationale:

None

Further Action:

None

Action by Network iTC:

Revise FCS_COP.1.1(2) in future versions of NDcPP and FWcPP and correct the typo as described above.