Network Device Interpretation # 202415

FCS_COP.1.1/SigGen needs assignment added

Status: ☒ *Active* ☐ *Inactive*

Date: *1-Oct-2024*

End of proposed Transition Period (to be updated after TR2TD process): *1-Nov-2024*

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): *NDcPP v3.0e*

Affected Section(s): *FCS_COP.1.1/SigGen*

Superseded Interpretation(s): *None*

Issue:

Issue: NDcPPv3.0e Section 6.4.2.1 FCS_COP.1 Cryptographic Operation

The NDcPPv2.2e included an assignment operation in FCS_COP.1/SigGen allowing the ST author to specify RSA and ECDSA key sizes. In the NDcPPv3.0e, the assignment operations were removed.

Proposed resolution:

Add assignments in the first two bullets for RSA (2048 bits or greater) and ECDSA (256 bits or greater).

Resolution:

The structure of the SFR has been updated in NDcPPV3.0e to be in agreement with the SFR definition as specified in CCv3.1R5 Part 2. The NIT agrees, though, that the definition of FCS_COP.1/SigGen could be improved. Therefore, the selection of cryptographic key sizes in the SFR shall be updated as follows:

{old}

and cryptographic key sizes [selection:

- *For RSA: modulus 2048 bits or greater,*
- *For ECDSA: 256 bits or greater*

]

{/old}

shall be replaced by

{new}

and cryptographic key sizes [selection:

• *For RSA: [assignment: modulus 2048 bits or greater],*

• *For ECDSA: [assignment: 256 bits or greater]*

]

{/new}.

Rationale:

see Issue and Resolution sections

Further Action:

None

Action by Network iTC:

None