Network Device Interpretation # 4

Using CTR_DRBG for random bit generation

Status: ☒ *Active* ☐ *Inactive*

Date: *15-Feb-2016*

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(1) (to be renamed to FCS_COP.1/DataEncryption in NDcPP V2.0)*

Superseded Interpretation(s): *None.*

Issue:

NDcPP V1.0 FCS_RBG_EXT.1 defines CTR_DRBG (using AES) as a selectable method of random bit generation. However, the AES requirements only reference CBC and GCM as supported modes. Is it acceptable for a conformant ST to claim support for CTR_DRBG without a corresponding claim for AES-CTR mode, or should the AES SFR be amended in a future revision to include CTR as a selectable option?

Resolution:

Explicit claim of AES in CTR mode is not required to satisfy DRBG requirements as long as ST includes at least one AES claim of the same key size.

Rationale:

AES in CTR mode is not included as allowed option in any of the protocol ciphersuites in the NDcPP V1.0. Consequently, introducing it as a selectable option in FCS_COP.1(1) would only increase potential for misunderstandings.

Further Action:

None.

Action by Network iTC:

None.