Network Device Interpretation # 201925

Use of seeds with higher entropy

Status: ☒ *Active* ☐ *Inactive*

Date: *10-Dec-2019*

End of proposed Transition Period (to be updated after TR2TD process): *10-Dec-2019*

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): *NDcPPv2.1*

Affected Section(s): *FCS_RGB_EXT.1.2*

Superseded Interpretation(s): Click here to enter text.

Issue:

In NDcPP v2.1, FCS_RBG_EXT.1.2 allows for selections of a "minimum of [selection: 128 bits, 192 bits, 256 bits] of entropy". Our vendor is providing 384 bits of entropy to the DRBG. Is it acceptable to select 256 bits from the selection and clarify in the TSS that 384 bits are actually provided by the TOE? This value would still meet "a minimum of 256 bits of entropy"?

Request that future versions of the cPP include a selection for 384 bits.

Resolution:

The NIT agrees that all minimum entropy values provided by the TOE that are higher than the ones selected in FCS_RBG_EXT.1.2 are suitable to fulfill the SFR. The actual minimum entropy value provided by the TOE can be provided in the TSS.

Rationale:

Provided in the Issue section.

Further Action:

None

Action by Network iTC:

For future versions of the NDcPP the Network iTC should consider whether this SFR needs to be revised to explicitly cover higher values for minimum entropy.