Network Device Interpretation # 202511

CTR_DRBG in FCS_RBG_EXT.1.2

Status: ☒ *Active* ☐ *Inactive*

Date: *9-Feb-2026*

End of proposed Transition Period (to be updated after TR2TD process): *1-Jan-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, NDSD v3.0e*

Affected Section(s): *FCS_RBG_EXT.1*

Superseded Interpretation(s): *None*

Issue:

Issue:

The selection in FCS_RBG_EXT.1.2 should include an option for 384 bits for when CTR_DRBG is selected in FCS_RBG_EXT.1.1 and there is no derivation function.

Resolution:

The NIT acknowledges the issue raised above. The following changes shall be applied to FCS_RBG_EXT.1.2

{old}

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: [assignment: number of software-based sources] software-based noise source, [assignment: number of platform-based sources] platform-based noise source] with a minimum of [selection: 128 bits, 192 bits, 256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

Application Note 17

For the first selection in FCS_RBG_EXT.1.2, the ST author selects at least one of the types of noise sources. If the TOE contains multiple noise sources of the same type, the ST author fills the assignment with the appropriate number for each type of source (e.g., 2 software-based noise sources, 1 platform-

based noise source). The documentation and tests required in the Evaluation Activity for this element should be repeated to cover each source indicated in the ST. Platform-based means the hardware-based or within the VS resources.

ISO/IEC 18031:2011 contains three different methods of generating random numbers; each of these, in turn, depends on underlying cryptographic primitives (hash functions/ciphers). The ST author will select the function used and include the specific underlying cryptographic primitives used in the requirement.

If the key length for the AES implementation used here is different than that used to encrypt the user data, then FCS_COP.1 may have to be adjusted or iterated to reflect the different key length. For the selection in FCS_RBG_EXT.1.2, the ST author selects the minimum number of bits of entropy that is used to seed the RBG, which must be equal or greater than the security strength of any key generated by the TOE.

{/old}

{new}

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: [*assignment: number of software-based sources*] software-based noise source, [*assignment: number of platform-based sources*] platform-based noise source] with a minimum of [selection: *128 bits, 192 bits, 256 bits, 320 bits, 384 bits*] of entropy at least equal to [selection:

- *the greatest security strength according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions",*
- *the greatest security strength according to ISO/IEC 18031:2011 Table C.2 — "Security strengths, Entropy and Seed length requirements for the AES-128, 192 and 256 Block Cipher",*
- *the seed length according to ISO/IEC 18031:2011 Table C.2 — "Security strengths, Entropy and Seed length requirements for the AES-128, 192 and 256 Block Cipher"*

].

Application Note 17

For the first selection in FCS_RBG_EXT.1.2, the ST author selects at least one of the types of noise sources. If the TOE contains multiple noise sources of the same type, the ST author fills the assignment with the appropriate number for each type of source (e.g., 2 software-based noise sources, 1 platform-based noise source). The documentation and tests required in the Evaluation Activity for this element should be repeated to cover each source indicated in the ST. Platform-based means the hardware-based or within the VS resources.

ISO/IEC 18031:2011 contains three different methods of generating random numbers; each of these, in turn, depends on underlying cryptographic primitives (hash functions/ciphers). For the second selection in FCS_RBG_EXT.1.2, the ST author selects the minimum number of bits of entropy used to seed the RBG which, in the third selection, must be equal or greater than the security strength or seed length listed in Table C.1 or Table C.2 of ISO/IEC 18031:2011.

The following table provides the ST author with available options for completing the allowed minimum number of bits of entropy and the security strength/seed length selections:

Selection	*Allowed minimum bits of entropy*	*DRBG Selected in FCS_RBG_EXT.1.1*
the greatest security strength according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions"	*128, 192, 256*	*Hash_DRBG or HMAC_DRBG*
the greatest security strength according to ISO/IEC 18031:2011 Table C.2 — "Security strengths, Entropy and Seed length requirements for the AES-128, 192 and 256 Block Cipher"	*128, 192, 256*	*CTR_DRBG (AES)*
the seed length according to ISO/IEC 18031:2011 Table C.2 — "Security strengths, Entropy and Seed length requirements for the AES-128, 192 and 256 Block Cipher"	*256, 320, 384*	*CTR_DRBG (AES)*

The second selection, "the greatest security strength according to ISO/IEC 18031:2011 Table C.2 — "Security strengths, Entropy and Seed length requirements for the AES-128, 192 and 256 Block Cipher"", shall be selected only if a derivation function is used.

The third selection, "the seed length according to ISO/IEC 18031:2011 Table C.2 — "Security strengths, Entropy and Seed length requirements for the AES-128, 192 and 256 Block Cipher"", shall be selected only if a derivation function is not used.

If the key length for the AES implementation used here is different than that used to encrypt the user data, then FCS_COP.1 may have to be adjusted or iterated to reflect the different key length.

{/new}

Rationale:

see Issue section

Further Action:

Note: This Technical Decision does not apply to NDcPPv 4.0.

Action by Network iTC:

None