Network Device Interpretation # 201903

Documenting Diffie-Hellman 14 groups

Status: ☒ *Active* ☐ *Inactive*

Date: *4-Jun-2019*

End of proposed Transition Period (to be updated after TR2TD process): *4-Jun-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): *ND SD V2.0e, ND SD V2.1*

Affected Section(s): FCS_CKM.2

Superseded Interpretation(s): *None*

Issue:

ND Supporting Document, FCS_CKM.2 Cryptographic Key Establishment, Section 2.2.2.1 TSS states:

"If Diffie-Hellman group 14 is selected from FCS_CKM.2.1, the TSS shall describe how the implementation meets RFC 3526 Section 3."

Please clarify the scope of documentation effort sufficient to describe specifics of diffie-hellman group implementation to satisfy "how" or rewrite the requirement to only require affirmation.

Suggested rewrite:

"If the TOE claims finite field cryptography (i.e., non-EC Diffie-Hellman), the TSS shall list all supported predefined Diffie-Hellman groups (e.g., ffdhe2048 as specified in RFC 7919 or 2048-bit MODP Group 14 as specified in RFC 3526)."

Resolution:

The NIT does not support the suggested rewrite since it does not clarify the issue. The term 'how' shall be understood in a way that the TSS should describe which DH14 groups according to RFC 3526 Section 3 are supported by the TOE. There is no need to provide implementation details of the crypto algorithms to prove the compliance. The sentence referenced in the issue section shall therefore be rephrased as follows:

<old> If Diffie-Hellman group 14 is selected from FCS_CKM.2.1, the TSS shall describe how the implementation meets RFC 3526 Section 3. </old>
Shall be replaced by

<new>If Diffie-Hellman group 14 is selected from FCS_CKM.2.1, the TSS shall affirm that the TOE implements RFC 3526 Section 3.</new>

Rationale:

See resolution section.

Further Action:

None.

Action by Network iTC:

None.