Network Device Interpretation # 202027

Clarification about use of DH14 in NDcPPv2.2e

Status: ☒ *Active* □ *Inactive*

Date: *23-Feb-2021*

End of proposed Transition Period (to be updated after TR2TD process): *23-Mar-2021*

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): *NDcPPv2.2e, NDSDv2.2*

Affected Section(s): *FCS_CKM.1.1, FCS_CKM.2.1*

Superseded Interpretation(s): *None*

Issue:

The FCS_CKM.2.1 wording "The TSF shall perform cryptographic key establishment in accordance with... FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, ... " might be misunderstood as 'the TOE's key establishment meets all aspects of SP800-56Ar3 that are related to the chosen safe-prime groups and FFC schemes' which would prohibit the use of DH group 14 for TLS. Those words shall be interpreted as 'implementations of the key agreement methods and groups need to satisfy SP800-56Ar3, but the use of those methods and groups is not restricted as specified in SP800-56Ar3', though. This should be clarified in an application note.

Resolution:

To address the issue described above, the last option in FCS_CKM.2.1 shall be modified as follows:

<old>

FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [selection: *RFC 3526, RFC 7919]*

</old>

shall be replaced by

<new>

FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [selection: *groups listed in RFC 3526, groups listed in RFC 7919]*

</new>

The following paragraph shall be added to Application Note 10 for FCS_CKM.2.1:

<new>

The option "FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [selection: groups listed in RFC 3526, groups listed in RFC 7919]." shall be read as 'the TOE performs Key Agreement as specified in SP800-56Ar3', but not necessarily adhering to the protocol restrictions for these groups, as indicated in Appendix D, tables 25 and 26. Instead, the use of those methods for particular protocols is in accordance with the SFR for the specific protocols. E.g. the use of DH group 14 for (D)TLS is specified in FCS_(D)TLSS_EXT.1.4.

</new>

The following parts defined in NDSDv2.2 for FCS_CKM.2 shall be removed:

From the TSS section:

<remove>[1]

If Diffie-Hellman group 14 is selected from FCS_CKM.2.1, the TSS shall claim the TOE meets RFC 3526 Section 3.

</remove>

<remove>

row 'Diffie-Hellman (Group 14)' from the table

</remove>

From the Test section:

<remove>

Diffie-Hellman Group 14

The evaluator shall verify the correctness of the TSF’s implementation of Diffie-Hellman group 14 by using a known good implementation for each protocol selected in FTP_TRP.1/Admin, FTP_TRP.1/Join, FTP_ITC.1 and FPT_ITT.1 that uses Diffie-Hellman group 14.

</remove>

For FCS_CKM.1 the last two paragraphs from Application Note 9 shall be removed as follows:

<remove>[2]

If the TOE acts as a receiver in the key establishment schemes and is not configured to support mutual authentication, the TOE does not need to implement key generation.

In a distributed TOE, if the TOE component acts as a receiver in the key establishment scheme, the TOE does not need to implement key generation.

</remove>

The test section defined in NDSDv2.2 for FCS_CKM.1 shall be modified as follows:

<old>

Diffie-Hellman Group 14 and FFC Schemes using “safe-prime” groups

Testing for FFC Schemes using Diffie-Hellman group 14 and/or safe-prime groups is done as part of testing in CKM.2.1.

</old>

shall be replaced by

<new>

FFC Schemes using “safe-prime” groups

Testing for FFC Schemes using safe-prime groups is done as part of testing in CKM.2.1.

</new>

Rationale:

See Issue section.

Footnotes:

[1] *There has been an additional RfI (#202103) that suggested a replacement of the current wording. As this sentence is removed now, also RfI#202103 is regarded as resolved.*

[2] *This part has been removed to enhance clarity upon scheme request. As this should have been done earlier it has been decided to remove this part as an exception to the rule as it is not directly related to the RfI.*

Further Action:

None

Action by Network iTC:

None