Network Device Interpretation # 202408

FCS_CKM.2 - Key Establishment Assurance Activities

Status: ☒ *Active* ☐ *Inactive*

Date: *22-Jul-2024*

End of proposed Transition Period (to be updated after TR2TD process): *31-Oct-2022*

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 v3.0e

Affected Section(s): FCS_CKM.2

Superseded Interpretation(s): *None*

Issue:

NDcPPv3.0e, Section 6.4.1.2, FCS_CKM.2.1 as part of selection options allows the following cryptographic key establishment methods:

- *[Option A]* FFC Schemes using "FIPS 186-Type" parameter-size sets that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";

- *[Option B]* 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].

ND SD v3.0e, Section 2.2.2.3 specifies two sets of assurance activities:

- [Option A] ECC and FIPS 186-type FFC SP800-56A Key Establishment Schemes;

- [Option B] FFC Schemes using "safe-prime" groups;

Option A requires functional tests of the key agreement schemes with test vectors, DKM and KDF calculation testing, validation of another party's key agreement results, etc. Option B only specifies interoperability testing using a known good implementation.

NIST SP 800-56Arev3, Appendix D refers to FIPS 186-4 finite field cryptography groups as safe-prime groups. Please clarify Application Note 11 to provide instructions when to select “FIPS 186-Type” over “safe-prime” as that would determine which assurance activities are applied.

Proposed Resolution: Consider combining or removing one of the redundant options. Also see RFI 202027.

Requirements in question:

FCS_CKM.2 Cryptographic Key Establishment
FCS_CKM.2.1 The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [selection:

- *…*
- *FFC Schemes using “FIPS 186-Type” parameter-size sets that meet the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”;*
- *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].*

] ~~that meets the following: [assignment: list of standards].~~

Application Note 11

This is a refinement of the SFR FCS_CKM.2 to deal with key establishment rather than key distribution.

…

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.

Assurance Activities:

ECC and FIPS 186-type FFC SP800-56A Key Establishment Schemes

73. The evaluator shall verify a TOE’s implementation of SP800-56A key agreement schemes using the following Function and Validity tests for ECC and FIPS186- type. These validation tests for each key agreement scheme verify that a TOE has implemented the components of the key agreement scheme according to the specifications in the Recommendation.

…

FFC Schemes using “safe-prime” groups

83. The evaluator shall verify the correctness of the TSF's implementation of safeprime groups 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 safeprime groups. This test must be performed for each safe-prime group that each protocol uses.

Resolution:

The FCS_CKM selections are not redundant. The following changes are implemented to clarify applicability and align with current testing capabilities.

NDcPPv3.0e, Section 6.4.1.2, FCS_CKM.2 Cryptographic Key Generation, shall be modified as follows:

{old}
Application Note 10
The ST author selects all key generation schemes used for key establishment (including generation of ephemeral keys) and device authentication. When key generation is used for key establishment, the schemes in FCS_CKM.2.1 and selected cryptographic protocols must match the selection. When key generation is used for device authentication, other than non-X.509 SSH authentication algorithm, the public key is expected to be associated with an X.509v3 certificate.
{/old}

{new}
Application Note 10
The ST author selects all key generation schemes used for key establishment (including generation of ephemeral keys) and device authentication. When key generation is used for key establishment, the schemes in FCS_CKM.2.1 and selected cryptographic protocols must match the selection. Finite Field Diffie-Hellman used in TLS ffdhe named groups, SSH, and IPsec utilize 'safe-primes.' Specific guidance on the appropriate selection for TLS DHE cannot be provided, because the DHE parameters are implementation dependent. When key generation is used for device authentication, other than non-X.509 SSH authentication algorithm, the public key is expected to be associated with an X.509v3 certificate.
{/new}

NDcPPv3.0e, Section 6.4.1.2, FCS_CKM.2 Cryptographic Key Establishment, shall be modified as follows:

{old}
Application Note 11

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_DTLSC_EXT.1.4, FCS_DTLSS_EXT.1.4, FCS_TLSS_EXT.1.3 or FCS_TLSC_EXT.1.4.

{/old}

{new}
Application Note 11

The option "Finite Field Cryptography (FFC) using safe-prime groups listed in [selection: RFC 3526, RFC 7919] for use with key-agreement schemes according to NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"" 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 the finite-field based Diffie-Hellman Ephemeral (DHE) key exchange mechanism with diffie-hellman-group14 (aka MODP-2048) in (D)TLS is specified in FCS_(D)TLSC_EXT.1.4, FCS_(D)TLSS_EXT.1.4). Finite Field Diffie-Hellman used in TLS ffdhe named groups, SSH, and IPsec utilize 'safe-prime groups' Specific guidance on the appropriate selection for TLS DHE cannot be provided, because the DHE parameters are implementation dependent.

{/new}

NDcPPv3.0e, Section B.3.1.3, FCS_IPSEC_EXT.1 IPsec Protocol, shall be modified as follows:

{old}
FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH Group(s) [selection:

- [selection: 14 *(2048-bit MODP), 15 (3072-bit MODP), 16 (4096-bit MODP), 17 (6144-bit MODP), 18 (8192-bit MODP)] according to RFC 3526,*
- [selection: *19 (256-bit Random ECP), 20 (384-bit Random ECP), 21 (521-bit Random ECP), 24 (2048-bit MODP with 256-bit POS)] according to RFC 5114.*

].

{/old}

{new}
FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH Group(s) [selection:

- [selection: *14 (2048-bit MODP), 15 (3072-bit MODP), 16 (4096-bit MODP), 17 (6144-bit MODP), 18 (8192-bit MODP)] according to RFC 3526,*
- [selection: *19 (256-bit Random ECP), 20 (384-bit Random ECP), 21 (521-bit Random ECP)] according to RFC 5114.*

].

{/new}

NDcPPv3.0e, Section C.2.2.4, FCS_IPSEC_EXT.1 IPsec Protocol, shall be modified as follows:

{old}
FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH Group(s) [selection:

- [selection: 14 *(2048-bit MODP), 15 (3072-bit MODP), 16 (4096-bit MODP), 17 (6144-bit MODP), 18 (8192-bit MODP)] according to RFC 3526,*
- [selection: *19 (256-bit Random ECP), 20 (384-bit Random ECP), 21 (521-bit Random ECP), 24 (2048-bit MODP with 256-bit POS)] according to RFC 5114.*

].

{/old}

{new}
FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH Group(s) [selection:

- [selection: *14 (2048-bit MODP), 15 (3072-bit MODP), 16 (4096-bit MODP), 17 (6144-bit MODP), 18 (8192-bit MODP)] according to RFC 3526,*
- [selection: *19 (256-bit Random ECP), 20 (384-bit Random ECP), 21 (521-bit Random ECP)] according to RFC 5114.*

].

{/new}

ND SDv3.0e, Section 2.2.2.3 Tests, shall be modified as follows:

{old} ***ECC and FIPS 186-type FFC SP800-56A Key Establishment Schemes***

…

{/old}

{new} ***Elliptic Curve Cryptography (ECC) and Finite Field Cryptography (FFC) SP800-56A Key Establishment Schemes***

…

{/new}

{remove} ***FFC Schemes using "safe-prime" groups***

83. The evaluator shall verify the correctness of the TSF's implementation of safe-prime groups 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 safe-prime groups. This test must be performed for each safe-prime group that each protocol uses. {/remove}

Rationale:

NIST Special Publication 800-56A Revision 3, Appendix D: Approved ECC Curves and FFC Safe-prime Groups states*: "Finite Field Cryptography Groups for Key Establishment: The following safe-prime groups are defined in RFC 3526 and RFC 7919 for use with key-agreement schemes that employ either the FFC DH or FFC MQV primitives."* **Therefore, according to NIST SP 800-56Ar3, both MODP and ffdhe groups are both considered safe-primes.**

Table 25 lists the following approved IKE groups for FFC key agreement*: MODP-2048 (ID=14), MODP-3072 (ID=15), MODP-4096 (ID=16), MODP-6144 (ID=17), MODP-8192 (ID=18).*

These correspond to FCS_IPSEC_EXT.1.11: "*[selection: 14 (2048-bit MODP), 15 (3072-bit MODP), 16 (4096-bit MODP), 17 (6144-bit MODP), 18 (8192-bit MODP)] according to RFC 3526*".

IPsec Group 24 uses FIPS 186-type parameters (compliant p and q relationship); however, the parameters are statically specified in RFC 5114. Current testing methodologies for FIPS 186-type key agreement require the parameters to be dynamically generated.

Table 26 lists the following approved TLS groups for FFC key agreement*: ffdhe2048 (ID = 256), ffdhe3072 (ID = 257), ffdhe4096 (ID = 258), ffdhe6144 (ID = 259), ffdhe8192 (ID = 260).*

The default configuration of most TLS 1.2 implementations perform key agreement using diffie-hellman-group14; however, this is not specified or required by any standard. TLS 1.2 DHE may use any Diffie-Hellman parameters, safe-prime or FIPS 186-type. Optionally, TLS uses Supported Groups Extension to signal support for all groups listed in the NIST SP 800-56Ar3 Table 25 and Table 26. The issue of conformance to the NIST SP 800-56A with the older versions of TLS is moot, as these are no longer supported in NDcPPv3.0e.

Functional Package for Secure Shell (SSH), FCS_SSH_EXT.1.6 include the following groups: *"diffie-hellman-group14-sha256 (RFC 8268), diffie-hellman-group15-sha512 (RFC 8268), diffie-hellman-group16-sha512 (RFC 8268), diffie-hellman-group17-sha512 (RFC 8268), diffie-hellman-group18-sha512 (RFC 8268)".* These identical to 'safe prime' MODP groups listed in the NIST SP 800-56Ar3 Table 25.

Further Action:

None

Action by Network iTC:

None