Network Device Interpretation # 201835rev2

RSA-based FCS_CKM.2 Selection

Status: ☒ *Active* ☐ *Inactive*

Date: *1-Jul-2019*

End of proposed Transition Period (to be updated after TR2TD process): *1-Jul-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): *NDcPP V2.0e, NDcPP V2.1, FWcPP V2.0e, NDSD V2.0e, NDSD V2.1*

Affected Section(s): *FCS_CKM.2*

Superseded Interpretation(s): *RfI#201835(rev1)*

Issue:

Background:

FCS_CKM.2 specifies the following key establishment methods:

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

- RSA-based key establishment schemes that meet the following: NIST Special Publication 800-56B Revision 1, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography”;
- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”;
- Finite field-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”;
- Key establishment scheme using Diffie-Hellman group 14 that meets the following: RFC 3526, Section 3;

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

Application Note 9 specifically references Section 9 of SP 800-56B Revision 1 for RSA-based key establishment schemes.

NIST SP 800-56B Revision 1 specifies the following schemes:

- Section 8 – Key Agreement Schemes
  - KAS1

- KAS2
- Section 9 – Key Transport Schemes
  - KTS-OAEP Key-Transport Scheme
  - KTS-KEM-KWS Key-Transport Scheme

Note: SP 800-131Ar2 (DRAFT), July 2018 addresses the widespread use of TLS by extending the transition date for PKCS#1 v1.5 (non-56B complaint key transport). It is now deprecated and will be disallowed after 2023. Technically SP 800-131Ar1 disallows all non-56B RSA key transport after 2017.

Section 7.4.7.1 of RFC 5246 (TLSv1.2) specifies the use of the RSAES-PKCS1-v1_5 scheme for use with RSA key transport ciphersuites for encrypting the pre-master secret.

The following is included for completeness of research; however, we do not believe any RSA-key establishment selection need is needed in FCS_CKM.2:

Section 5.2 of RFC 2409 (IKEv1) describes the use of RSA encryption for authentication according to the PKCS#1 format. This RFC references RSA Laboratories, "PKCS #1: RSA Encryption Standard", November 1993. KTS-OAEP was added to PKCS #1 in PKCS #1; RSA Cryptography Specifications in Version 2.0 in October 1998, so IKEv1 does not specify the use of KTS-OAEP. This encryption is performed in addition to Diffie-Hellman key establishment.

Issue

FCS_CKM.2 does not provide an appropriate selection for the key establishment schemes used in TLS with RSA key transport and IKEv1 with Public Key Encryption. The “RSA-based key establishment schemes…” selection is not used by any of the allowed protocol configurations.

Resolution:

The NIT acknowledges the issue described in the Issue section. Therefore the following changes shall be applied:

In FCS_CKM.2 the selection option for RSA

<old>”RSA-based key establishment schemes that meet the following: NIST Special Publication 800-56B Revision 1, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography ”“</old>

Shall be replaced by

<new>”RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1””</new>

The test requirements in the Supporting Document for FCS_CKM.2, SP800-56B Key Establishment Schemes

<old>" If the TOE acts as a sender, the following assurance activity shall be performed to ensure the proper operation of every TOE supported combination of RSA-based key establishment scheme:

a) To conduct this test the evaluator shall generate or obtain test vectors from a known good implementation of the TOE supported schemes. For each combination of supported key establishment scheme and its options (with or without key confirmation if supported, for each supported key confirmation MAC function if key confirmation is supported, and for each supported mask generation function if KTS-OAEP is supported), the tester shall generate 10 sets of test vectors. Each test vector shall include the RSA public key, the plaintext keying material, any additional input parameters if applicable, the MacKey and MacTag if key confirmation is incorporated, and the outputted ciphertext. For each test vector, the evaluator shall perform a key establishment encryption operation on the TOE with the same inputs (in cases where key confirmation is incorporated, the test shall use the MacKey from the test vector instead of the randomly generated MacKey used in normal operation) and ensure that the outputted ciphertext is equivalent to the ciphertext in the test vector.

If the TOE acts as a receiver, the following assurance activities shall be performed to ensure the proper operation of every TOE supported combination of RSA-based key establishment scheme:

a) To conduct this test the evaluator shall generate or obtain test vectors from a known good implementation of the TOE supported schemes. For each combination of supported key establishment scheme and its options (with our without key confirmation if supported, for each supported key confirmation MAC function if key confirmation is supported, and for each supported mask generation function if KTS-OAEP is supported), the tester shall generate 10 sets of test vectors. Each test vector shall include the RSA private key, the plaintext keying material (KeyData), any additional input parameters if applicable, the MacTag in cases where key confirmation is incorporated, and the outputted ciphertext. For each test vector, the evaluator shall perform the key establishment decryption operation on the TOE and ensure that the outputted plaintext keying material (KeyData) is equivalent to the plaintext keying material in the test vector. In cases where key confirmation is incorporated, the evaluator shall perform the key confirmation steps and ensure that the outputted MacTag is equivalent to the MacTag in the test vector.

The evaluator shall ensure that the TSS describes how the TOE handles decryption errors. In accordance with NIST Special Publication 800-56B, the TOE must not reveal the particular error that occurred, either through the contents of any outputted or logged error message or through timing variations. If KTS-OAEP is supported, the evaluator shall create separate contrived ciphertext values that trigger each of the three decryption error checks described in NIST Special Publication 800-56B section 7.2.2.3, ensure that each decryption attempt results in an error, and ensure that any outputted or logged error message is identical for each. If KTS-KEM-KWS is supported, the evaluator shall create separate contrived

ciphertext values that trigger each of the three decryption error checks described in NIST Special Publication 800-56B section 7.2.3.3, ensure that each decryption attempt results in an error, and ensure that any outputted or logged error message is identical for each."</old>

Shall be replaced by

<new>"The evaluator shall verify the correctness of the TSF's implementation of RSAES-PKCS1-v1_5 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 RSAES-PKCS1-v1_5."</new>

Rationale:

The original resolution Rfl#201835rev1 contained the wrong reference to RFC8017 instead of RFC3447. This has been corrected.

Further Action:

None.

Action by Network iTC:

None.