Network Device Interpretation # 202417a

Addition of FIPS PUB 186-5 for RSA

Status: □ *Active* ☒ *Inactive*

Date: *25-Oct-2024*

End of proposed Transition Period (to be updated after TR2TD process): *25-Dec-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, ND SD v3.0e*

Affected Section(s): *FCS_CKM.1, FCS_COP.1.1/SigGen*

Superseded Interpretation(s): *None*

Issue:

Issue:

For FIPS 140-3, it is required to be compliant to FIPS 186-5 for RSA / ECDSA. However, the NDcPPv3.0e states compliance to FIPS 186-4 for RSA / ECDSA. Developers of some products have moved to FIPS 186-5.

Resolution:

This resolution focuses on RSA, see RFI 202417b for ECDSA. To overcome the issue outlined in the 'Issue' section, the following changes shall be applied:

In NDcPPv3.0e, FCS_CKM.1.1, the selection operation shall be replaced as follows:

{old}

• RSA schemes using cryptographic key sizes of [assignment: 2048 bits or greater] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;

{/old}

by

{new}

• RSA schemes using cryptographic key sizes of [assignment: 2048 bits or greater] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3 or FIPS PUB 186-5, “Digital Signature Standard (DSS)”, A.1;

{/new}.

In NDcPPv3.0e, FCS_COP.1.1/SigGen, the last selection shall be replaced as follows.

{old}

• For RSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,

{/old}

by

{new}

• For RSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5 using PKCS #1 v2.1 or FIPS PUB 186-5, “Digital Signature Standard (DSS)”, Section 5.4, using PKCS #1 v2.2 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,

{/new}.

In ND SD v3.0e, FCS_CKM.1, Section 2.2.1.3 the following paragraph shall be replaced:

{old}

Key Generation for FIPS PUB 186-4 RSA Schemes

The evaluator shall verify the implementation of RSA Key Generation by

…

from a known good implementation.

{/old}

by

{new}

Key Generation for FIPS PUB 186-4 or FIPS PUB 186-5 RSA Schemes

The evaluator shall verify the implementation of RSA Key Generation by the TOE using the Key Generation test. This test verifies the ability of the TSF to correctly produce values for the key components including the public verification exponent e, the private prime factors p and q, the public modulus n and the calculation of the private signature exponent d. This test must be repeated for each supported RSA modulo and generation method.

Key Pair generation specifies 5 ways (or methods) to generate the primes p and q. These include:

a. Random Provable primes (p and q shall be provable primes)
b. Random Probable primes (p and q shall be probable primes)
c. Provable primes with Conditions (p1, p2, q1, q2, p and q shall all be provable primes)
d. Provable/probable primes with Conditions (p1, p2, q1, and q2 shall be provable primes and p and q shall be probable primes)
e. Probable primes with Conditions (p1, p2, q1, q2, p and q shall all be probable primes)

The Random Provable primes, and all the Primes with Conditions can be tested in the same manner because each of these begin with a starting random number and calculate the p and q values from this value. The test instructs the TSF to generate intermediate values and the p, q, n, and d values. The evaluator then validates the correctness of the values generated by the TSF.

To test the key generation method for the Random Provable primes or Primes with Conditions methods, the evaluator must seed the TSF key generation routine with sufficient data to deterministically generate the RSA key pair. This includes the random seed(s), the public exponent of the RSA key, and the desired key length. If the TSF provides the input to the key generation function, such input must be recorded and verified. For each RSA key length (modulo) claimed, the evaluator shall generate 25 key pairs. The evaluator shall verify the correctness of the TSF's implementation by comparing Key Pair values generated by the TSF with those generated using the same set of input values using a known good implementation.

The Random Probable primes must be tested in a different way because this test generates different random numbers, not related to each other, until the number satisfies the "probably prime" requirements. This validation method requires two tests for Random Probable primes. These include the Known Answer Test and the Miller-Rabin probabilistic primality test.

To test the key generation method for the Random Probable primes, the known answer test must be used. The evaluator shall compare the results of a known good implementation with the TSF results for a set (of a corresponding size depending on modulus) of supplied values containing private prime factor p, private prime factor q and confirm all public keys, e, match. Then the evaluator shall use the TSF to generate prime p, q pairs for each modulus size and perform the Miller-Rabin tests.

{/new}

In ND SD v3.0e, FCS_COP.1/SigGen, Section 2.2.5.3:

{old}

RSA Signature Algorithm Tests

…

detects the errors introduced in the altered messages.

{/old}

shall be replaced by:

{new}

RSA Signature Algorithm Tests

Signature Generation Test
The evaluator shall verify the implementation of RSA Signature generation by the TOE using the Signature Generation Test. This test verifies the ability of the TSF to produce correct signatures.

There are 2 different RSA Signature algorithms that can be implemented. These include:

a. RSASSA-PKCS1-v1.5
b. RSASSA-PSS

To test signature generation, the evaluator generates or obtains 10 messages for each modulus size/hash or extendable-output function combination supported by the TOE. Using a key generated by a known good implementation, the TSF generates and returns the corresponding signatures to a known-good implementation that validates the signatures by using the associated public key to verify the signature.

Signature Verification Test
The evaluator shall verify the implementation of RSA Signature verification by the TOE using the Signature Verification Test. This test verifies the ability of the TSF to recognize valid and invalid signatures.

There are 2 different RSA Signature algorithms that can be implemented. These include:

a. RSASSA-PKCS1-v1.5
b. RSASSA-PSS

For each modulus size/hash or extendable-output function combination supported by the TOE, the evaluator shall use a known good implementation to generate a modulus and three associated key pairs, (d, e). Each private key d is used to sign six pseudorandom messages each of 1024 bits. Some of the public keys, e, messages, IR format, or signatures must be altered so that signature verification should fail. The modifications must cover distinct "key modified", "message modified", "signature modified", "IR moved", and "trailer moved" tests. The modulus, hash or extendable-output algorithm, public key e values, messages, and signatures are forwarded to the TSF. The TSF then attempts to verify the signatures and returns the results. The evaluator then compares the received results with the stored results from a known good implementation.

The evaluator shall verify that the TSF validates correct signatures on the original messages and flags or rejects the altered messages.
{/new}.

Rationale:

To avoid issues during transition between FIPS PUB 186-4 to FIPS PUB 186-5, the NIT decided to allow FIPS PUB 186-5 concurrently instead of replacing the existing FIPS186-4. At the time of issuing of this RFI conformance to either or both are acceptable.

Further Action:

None

Action by Network iTC:

None