Network Device Interpretation # 202417b

Addition of FIPS PUB 186-5 for ECDSA

Status: ☒ *Active* ☐ *Inactive*

Date: *3-Mar-2025*

End of proposed Transition Period (to be updated after TR2TD process): *3-May-2025*

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Superseded Interpretation(s): *None*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 ECDSA, see RFI 202417a for RSA. 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:

{old}

- *ECC schemes using 'NIST curves' [selection: P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;*

{/old}

shall be replaced by:

{new}

- ECC schemes using elliptic curves [selection: P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4, or FIPS PUB 186-5, "Digital

Signature Standard (DSS)", Appendix A.2, or ISO/IEC 14888-3, "IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms", Section 6.6.

{/new}.

In NDcPPv3.0e, FCS_COP.1.1/SigGen, the last selection:

{old}

that meet the following: [selection:

- *For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [selection: P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4,*

{/old}

shall be replaced as follows:

{new}

that meet the following: [selection:

- *For ECDSA schemes implementing [selection: P-256, P-384, P-521] curves that meet the following : FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST Recommended" curves; or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 6 and NIST SP 800-186 Section 3.2.1, Implementing Weierstrass curves; or ISO/IEC 14888-3, "IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms", Section 6.6.*

{/new}.

and append Application 14 as follows:

{new}

The Weierstrass or "NIST Recommended" curves P-256, P-384, and P-521 (also referred to as secp256r1, secp384r1, and secp521r1) are elliptic curves $W_{a,b}$ defined over the prime field GF(p) that has order h·n, where h = 1, and n is a prime number. Domain parameters for these curves documented in the NIST SP 800-186, Section 3.2.1.

{/new}

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

{old}

Key Generation for Elliptic Curve Cryptography (ECC)

FIPS 186-4 ECC Key Generation Test

For each supported NIST curve…

{/old}

shall be replaced by:

{new}

Key Generation for ECDSA Schemes

Key pairs for the ECDSA consist of pairs (d, Q), where the private key, d, is an integer, and the public key, Q, is an elliptic curve point.

The evaluator shall verify the implementation of ECC Key Generation by the TOE using the following components tests:

- *ECC Key Pair Generation*
- *ECC Public Key Validation (PKV)*

ECC Key Pair Generation Test

There are four methods by which these pairs may be generated:

- *FIPS 186-4 Section B.4.1 Key Pair Generation Using Extra Random Bits*

Using this method, 64 more bits are requested from the RBG than are needed for d so that bias produced by the mod function is negligible.

- *FIPS 186-4 Section B.4.2 Key Pair Generation by Testing Candidates*

Using this method, a random number is obtained and tested to determine that it will produce a value of d in the correct range. If d is out-of-range, another random number is obtained (i.e., the process is iterated until an acceptable value of d is obtained.

- *FIPS 186-5 Section A.2.1 ECDSA Key Pair Generation using Extra Random Bits*

Using this method, more bits are requested from the DRBG than are needed for d so that the bias produced by the mod function is negligible.

- *FIPS 186-5 Section A2.2 ECDSA Key Pair Generation by Rejection Sampling*

Using this method, a random number is obtained and tested to determine that it will produce a value of d in the correct range. If d is out of range, an ERROR is returned.

The evaluator shall test the ECC Key Pair Generation by having the TSF produce 10 key pairs (d, Q) for each implemented key generation method using each supported curve (i.e., P-256, P-384, and P-521). The steps are the same for each key generation method and curve. The private key, d, shall be generated using the output of an approved DRBG converted to an integer via modular reduction or the discard method. The known private key is then used by the TSF to compute the public key, Q'. To evaluator then validates the correctness by comparing the value Q' computed by the TSF to the public key, Q generated by a known good implementation.

ECC Public Key Validation (PKV) Test

The evaluator shall generate 12 key pairs (d, Q) for each selected curve, with 6 valid public keys, Q, using a known good implementation and 6 modified, Q', and determine whether the TSF can accurately detect these modifications. Q' should be otherwise valid but include at least one of the following errors: a) point X or Y not on the curve, b) point X or Y is too large for the field for the given curve. The evaluator encouraged to make sure that the modification does not inadvertently result in another valid public key (e.g., modifying Y and accidentally hitting a different point on the curve).

{/new}

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

{old}

ECDSA Algorithm Tests

ECDSA FIPS 186-4 Signature Generation Test

…

ECDSA FIPS 186-4 Signature Verification Test

…

{/old}

shall be replaced by:

{new}

ECDSA Signature Algorithm Tests

The evaluator shall verify the implementation of ECDSA Signature generation by the TOE using the Signature Generation Test. This test validates the TSF generation of the (r, s) pair that represent the digital signature. The digital signature shall be verified using the same domain parameters and hash function that were used during signature generation. An approved hash function or an XOF shall be used for this purpose.

Signature Generation Test

The purpose of this test is to verify the ability of the TSF to produce correct signatures.

To test signature generation, the evaluator supplies 10 pseudorandom messages to the TSF and a key pair, (d, Q), generated by a known good implementation. Exercising each applicable curve (i.e., P-256, P-384, or P-521) and hash algorithm or extendable-output function combination, the TSF generates signatures for each supplied message and returns the corresponding signatures. Using a known-good implementation, the evaluator validates the signatures by using the associated public key, Q, to verify the signature.

Signature Verification Test

The purpose of this test is to verify the ability of the TSF to accept valid signatures and reject invalid signatures.

For each curve/hash algorithm or extendable-output function combination supported by the TSF, the evaluator shall use a known good implementation to generate a key pair, (d, Q), and use known good implementation with the private key, d, to sign 15 pseudorandom messages of 1024 bits. The evaluator shall alter some of the messages or signatures so that signature verification should fail.

To test signature verification, the evaluator supplies the public key, Q, and 15 pseudorandom messages, including altered messaged, to the TSF for verification of signatures. The evaluator shall then 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