Request for Network Device Interpretation

The NIT is responsible for providing responses to requests for interpretations on NDcPP for the CC community. The NDcPP iTC is responsible for developing and maintaining NDcPP. These requests for information (RFIs) should focus on interpretations of existing requirements and not changes you would like to see to the requirements within NDcPP. If you would like to request a change to a requirement, please post a message for the iTC at Network iTC (CCUF Forum) (free registration required to access CCUF Forum).

Requestor Name and Organization: Kristy Knowles, Cisco Systems, Inc.

Status: ☐ *On-going certification* ☒ *Preparatory/Other*

If your issue arises from a currently active CC evaluation then please tick the 'On-going certification' box, submit the completed request through your Certification/Validation Body (CB), and update the 'Certification deadline dates' field. Otherwise please tick the 'Preparatory/Other' box and send your request directly to the NIT. In either case, enter the current date into the Submittal date field.

Submittal date: <15-01-2026>

Certification deadline dates:

If your product is in an on-going CC effort, please include any scheme deadlines above.

SFR or Section of cPP in question: FCS_CKM.1/AKG, FCS_COP.1/SigGen, FCS_COP.1/SigVer

Supporting document testing in question: FCS_CKM.1/AKG, FCS_COP.1/SigGen, FCS_COP.1/SigVer

Issue:

NDcPP v4.0 and the ND Supporting Document v4.0 currently reference FIPS PUB 186-5 as the Digital Signature Standard (DSS) for RSA and ECDSA key generation, signature generation, and signature verification. In NDcPP v3.0e, these algorithms explicitly referenced FIPS PUB 186-4. In addition, TD0918/TD0921 allowed for compliance with FIPS 186-5 if desired. The removal of FIPS PUB 186-4 in v4.0 creates ambiguity and transition friction for products and Security Targets migrating from NDcPP v3.0e to NDcPP v4.0.

In practice, differences between the two standards primarily involve the removal of certain algorithms and algorithm modes and the addition of extra algorithm modes. The differences in the algorithm details for RSA and ECDSA are very minor between FIPS 186-4 and 186-5 and are limited to RSA KeyGen. As a result, implementations compliant with FIPS PUB 186-4 do not represent weaker cryptography, and prior NIT decisions (e.g., TD0921) provide precedent for continuity-based handling during such transitions.

Proposed resolution:

Update NDcPP v4.0 and the ND Supporting Document v4.0 to reference either FIPS PUB 186-4 or FIPS PUB 186-5. Update the cryptographic algorithm parameters, relevant list of standards, and assurance activities where appropriate for key generation and signature-related algorithms such the ST author can select either FIPS PUB 186-4 or FIPS PUB 186-5. This clarification preserves continuity during transition and avoids unintended restriction of acceptable implementations.

Resolution:

The following changes shall be applied:

NDcPP v4.0

Update FCS_CKM.1/AKG, Table 3

{old}

Identifier	**Cryptographic Key Generation Algorithm**	**Cryptographic Algorithm Parameters**	**List of Standards**
RSA	RSA	Modulus of size [selection: *2048, 3072, 4096, 6144, 8192*] bits	NIST FIPS PUB 186-5 (Section A.1.1)
ECC-ERB	ECC-ERB - Extra Random Bits	Elliptic Curve [selection: *P-256, P-384, P-521*]	NIST FIPS PUB 186-5 (Section A.2.1), NIST SP 800-186 (Section 3) [NIST Curves]
ECC-RS	ECC-RS - Rejection Sampling	Elliptic Curve [selection: *P-256, P-384, P-521*]	NIST FIPS PUB 186-5 (Section A.2.2), NIST SP 800-186 (Section 3) [NIST Curves]

[Remaining rows from Table 3 omitted for brevity]

{/old}

{new}

Identifier	**Cryptographic Key Generation Algorithm**	**Cryptographic Algorithm Parameters**	**List of Standards**
RSA	RSA	Modulus of size [selection: *2048, 3072, 4096, 6144, 8192*] bits	[selection: *NIST FIPS PUB 186-5 (Section A.1.1),* *NIST FIPS PUB 186-4 (Appendix B.3.1*)]

ECC-ERB	ECC-ERB - Extra Random Bits	Elliptic Curve [selection: *P-256, P-384, P-521*]	[selection: *NIST FIPS PUB 186-5 (Section A.2.1), NIST FIPS PUB 186-4 (Section B.4.1)*] NIST SP 800-186 (Section 3) [NIST Curves]
ECC-TC	ECC-TC – Testing Candidates	Elliptic Curve [selection: *P-256, P-384, P-521*]	NIST FIPS PUB 186-4 (Section B.5.2) NIST SP 800-186 (Section 3) [NIST Curves]
ECC-RS	ECC-RS - Rejection Sampling	Elliptic Curve [selection: *P-256, P-384, P-521*]	NIST FIPS PUB 186-5 (Section A.2.2) NIST SP 800-186 (Section 3) [NIST Curves]

[Remaining rows from Table 3 omitted for brevity]

{/new}

Update FCS_COP.1/SigGen, Table 5

{old}

Cryptographic Key Generation Algorithm	**Cryptographic Algorithm Parameters**	**List of Standards**
RSASSA-PKCS1-v1_5	Modulus of size [selection: *2048, 3072, 4096, 6144, 8192*] bits and hash [selection: *SHA-256, SHA-384, SHA-512*]	RFC 8017 (Section 8.2) [PKCS #1 v2.2], FIPS PUB 186-5 (Section 5.4) [RSASSA-PKCS1-v1_5]
RSASSA-PSS	Modulus of size [selection: *2048, 3072, 4096, 6144, 8192*] bits and hash [selection: *SHA-256, SHA-384, SHA-512*], Salt Length (*sLen*) such that [*assignment: 0 ≤ sLen ≤ hLen (Hash Output Length*)] and Mask Generation Function = MGF1]	RFC 8017 (Section 8.1) [PKCS#1 v2.2], FIPS PUB 186-5 (Section 5.4) [RSASSA-PSS]
ECDSA	Elliptic Curve [selection: *P-256, P-384, P-521*], per-message secret number generation [selection: *extra random bits, rejection sampling, deterministic*] and hash	[selection: *ISO/IEC 14888-3:2018 (Subclause 6.6), FIPS PUB 186-5 (Sections 6.3.1, 6.4.1]*][ECDSA]

	function using [selection: *SHA-256, SHA-384, SHA-512*]	NIST SP-800 186 (Section 4) [NIST Curves]

[*Remaining rows from Table 5 omitted for brevity*]

{/old}

Application Note 16

The ST author should choose the cryptographic algorithms, parameters, and standards implemented to perform digital signature generation. For the algorithm chosen, the ST author should make the appropriate assignments/selections to specify the parameters that are implemented for that algorithm.

{new}

Cryptographic Key Generation Algorithm	**Cryptographic Algorithm Parameters**	**List of Standards**
RSASSA-PKCS1-v1_5	Modulus of size [selection: *2048, 3072, 4096, 6144, 8192*] bits and hash [selection: *SHA-256, SHA-384, SHA-512*]	[selection: *RFC 8017 (Section 8.2) [PKCS #1 v2.2] and FIPS PUB 186-5 (Section 5.4),* *FIPS PUB 186-4 (Section 5.5) using PKCS #1 v2.1 Signature Schemes*] [RSASSA-PKCS1-v1_5]
RSASSA-PSS	Modulus of size [selection: *2048, 3072, 4096, 6144, 8192*] bits and hash [selection: *SHA-256, SHA-384, SHA-512*], Salt Length (*sLen*) such that [*assignment: 0 ≤ sLen ≤ hLen (Hash Output Length*)] and Mask Generation Function = MGF1]	[selection: *RFC 8017 (Section 8.1) [PKCS#1 v2.2] and FIPS PUB 186-5 (Section 5.4),* *FIPS PUB 186-4 (Section 5.5) using PKCS #1 v2.1 Signature Schemes*] [RSASSA-PSS]
ECDSA	Elliptic Curve [selection: *P-256, P-384, P-521*], per-message secret number generation [selection: *extra random bits, rejection sampling, testing candidates, deterministic*] and hash function	[selection: *ISO/IEC 14888-3:2018 (Subclause 6.6), FIPS PUB 186-5 (Sections 6.3.1, 6.4.1), FIPS PUB 186-4 (Sections B.4.1, B.4.2)*] [ECDSA]

	using [selection: *SHA-256, SHA-384, SHA-512*]	NIST SP-800 186 (Section 4) [NIST Curves]

[*Remaining rows from Table 5 omitted for brevity*]

Application Note 16

The ST author should choose the cryptographic algorithms, parameters, and standards implemented to perform digital signature generation. For the algorithm chosen, the ST author should make the appropriate assignments/selections to specify the parameters that are implemented for that algorithm. For the ECDSA algorithm, the selection of "testing candidates" applies only to FIPS PUB 186-4. "Rejection Sampling" and "deterministic" apply only to FIPS PUB 186-5. "Extra random bits" may be selected for FIPS PUB 186-4 or FIPS PUB 186-5.

{/new}

Update FCS_COP.1/SigVer, Table 6

{old}

Cryptographic Key Generation Algorithm	**Cryptographic Algorithm Parameters**	**List of Standards**
RSASSA-PKCS1-v1_5	Modulus of size [selection: *2048, 3072, 4096, 6144, 8192*] bits and hash [selection: *SHA-256, SHA-384, SHA-512*]	RFC 8017 (Section 8.2) [PKCS #1 v2.2], FIPS PUB 186-5 (Section 5.4) [RSASSA-PKCS1-v1_5]
RSASSA-PSS	Modulus of size [selection: *2048, 3072, 4096, 6144, 8192*] bits and hash [selection: *SHA-256, SHA-384, SHA-512*]	RFC 8017 (Section 8.1) [PKCS#1 v2.2], FIPS PUB 186-5 (Section 5.4) [RSASSA-PSS]
ECDSA	Elliptic Curve [selection: P-256, P-384, P-521] using hash [selection: SHA-256, SHA-384, SHA-512]	[selection: ISO/IEC 14888-3:2018 (Subclause 6.6), FIPS PUB 186-5 (Section 6.4.2)][ECDSA] NIST SP-800 186 (Section 4) [NIST Curves]

[Remaining rows from Table 6 omitted for brevity]
{/old}

{new}

Cryptographic Key Generation Algorithm	**Cryptographic Algorithm Parameters**	**List of Standards**
RSASSA-PKCS1-v1_5	Modulus of size [selection: *2048, 3072, 4096, 6144, 8192*] bits and hash [selection: *SHA-256, SHA-384, SHA-512*]	[selection:

		RFC 8017 (Section 8.2) [PKCS #1 v2.2] and FIPS PUB 186-5 (Section 5.4), *FIPS PUB 186-4 (Section 5.5) using PKCS #1 v2.1 Signature Schemes*] [RSASSA-PKCS1-v1_5]
RSASSA-PSS	Modulus of size [selection: *2048, 3072, 4096, 6144, 8192*] bits and hash [selection: *SHA-256, SHA-384, SHA-512*]	[selection: *RFC 8017 (Section 8.1) [PKCS#1 v2.2] and FIPS PUB 186-5 (Section 5.4),* *FIPS PUB 186-4 (Section 5.5) using PKCS #1 v2.1 Signature Schemes*] [RSASSA-PSS]
ECDSA	Elliptic Curve [selection: P-256, P-384, P-521] using hash [selection: SHA-256, SHA-384, SHA-512]	[selection: *ISO/IEC 14888-3:2018 (Subclause 6.6), FIPS PUB 186-5 (Section 6.4.2), FIPS PUB 186-4 (Section 6.4)*][ECDSA] NIST SP-800 186 (Section 4) [NIST Curves]

[Remaining rows from Table 6 omitted for brevity]

{/new}

Glossary

NIST Curves

{old}

NIST-approved elliptic curves specified in NIST SP 800-186. Refers to the P-256, P-384, and P-521 curves defined in FIPS 186-5 for elliptic curve cryptography.

{/old}

{new}

NIST-approved elliptic curves specified in NIST SP 800-186. Refers to the P-256, P-384, and P-521 curves approved for elliptic curve cryptography and referenced by FIPS PUB 186-4 and FIPS PUB 186-5.

{/new}

{new}

PKCS #1 v2.1

Public-Key Cryptography Standards #1 version 2.1. RSA cryptography standard specifying RSA encryption and signature schemes.

{/new}

RSASSA-PKCS1-v1_5

{old}
RSA Signature Scheme with Appendix using PKCS1 v1.5 padding. A digital signature scheme specified in RFC 8017 Section 8.2 and FIPS 186-5 Section 5.4.
{/old}

{new}
RSA Signature Scheme with Appendix using PKCS1 v1.5 padding. A digital signature scheme specified in RFC 8017 Section 8.2, with Digital Signature Standard requirements defined in FIPS PUB 186-4 Section 5.5 and FIPS PUB 186-5 Section 5.4.
{/new}

RSASSA-PSS

{old}
RSA Signature Scheme with Appendix using Probabilistic Signature Scheme. A digital signature scheme specified in RFC 8017 Section 8.1 and FIPS 186-5 Section 5.4.
{/old}

{new}
RSA Signature Scheme with Appendix using Probabilistic Signature Scheme. A digital signature scheme specified in RFC 8017 Section 8.1, with Digital Signature Standard requirements defined in FIPS PUB 186-4 Section 5.5 and FIPS 186-5 Section 5.4.
{/new}

ND Supporting Document v4.0

7. Paragraph 56 — RSA Key Generation

{old}
RSA Key Generation

FIPS PUB 186-5 Key Pair generation specifies five methods for generating the primes p and q. These are:

a. Random provable primes
b. Random probable primes
c. Provable primes with conditions based on auxiliary provable primes
d. Probable primes with conditions based on auxiliary provable primes
e. Probable primes with conditions based on auxiliary probable primes

In addition to the key generation method, the input parameters are:

- Modulus [3072, 4096, 6144, 8192]
- Hash algorithm [SHA-384, SHA-512] (methods 1, 3, 4 only)
- Rabin-Miller prime test [2100, 2Security String] (methods 2, 4, 5 only)
- p mod 8 value [0,1,3,5,7]
- q mod 8 value [0,1,3,5,7]
- Private key format [standard, Chinese Remainder Theorem]
- Public exponent [fixed value, random]

The evaluator shall verify the ability of the TSF to correctly produce values for the RSA 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.
{/old}

{new}

RSA Key Generation

FIPS PUB 186-5 specifies five methods for generating the primes p and q. Implementations conformant to FIPS PUB 186-4 use equivalent prime-generation approaches. These are:

a. Random provable primes
b. Random probable primes
c. Provable primes with conditions based on auxiliary provable primes
d. Probable primes with conditions based on auxiliary provable primes
e. Probable primes with conditions based on auxiliary probable primes

In addition to the key generation method, the input parameters are:

- Modulus [3072, 4096, 6144, 8192]
- Hash algorithm [SHA-384, SHA-512] (methods 1, 3, 4 only)
- Rabin-Miller prime test [2100, 2Security String] (methods 2, 4, 5 only)
- p mod 8 value [0,1,3,5,7]
- q mod 8 value [0,1,3,5,7]
- Private key format [standard, Chinese Remainder Theorem]
- Public exponent [fixed value, random]

The evaluator shall verify the ability of the TSF to correctly produce values for the RSA 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.
{/new}

8. Paragraph 59 — ECC Key Generation

{old}

Elliptic Curve Key Generation

59. To test the TOE’s ability to generate asymmetric cryptographic keys using elliptic curves, the evaluator shall perform the ECC Key Generation Test and the ECC Key Validation Test using the following input parameters:

a. Elliptic curve [P-256, P-384, P-521]
b. Key pair generation method [extra random bits, rejection sampling]

{/old}

{new}

Elliptic Curve Key Generation

59. To test the TOE's ability to generate asymmetric cryptographic keys using elliptic curves, the evaluator shall perform the ECC Key Generation Test and the ECC Key Validation Test using the following input parameters:

a. Elliptic curve [P-256, P-384, P-521]
b. Key pair generation method [extra random bits, rejection sampling, testing candidates]

i. 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.

ii. 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

iii. 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.

iv. 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.

{/new}

9. Paragraph 103 — ECDSA Signature Generation

{old}
To test the TOE's ability to perform ECDSA Digital Signature Generation using extra random bits or rejection sampling for secret number generation, the evaluator shall perform the Algorithm Functional Test using the following input parameters:

- Elliptic Curve [P-256, P-384, P-521]
- Hash algorithm [SHA-256, SHA-384, SHA-512]

{/old}

{new}
To test the TOE's ability to perform ECDSA Digital Signature Generation using extra random bits, rejection sampling, or testing candidates for secret number generation, the evaluator shall perform the Algorithm Functional Test using the following input parameters:

- Elliptic Curve [P-256, P-384, P-521]

- Hash algorithm [SHA-256, SHA-384, SHA-512]

{/new}

10. Section 7 — References

{old}
[FIPS 186-5] FIPS PUB 186-5, Digital Signature Standard (DSS), February 2023
{/old}

{new}
[FIPS 186-4] FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013

[FIPS 186-5] FIPS PUB 186-5, Digital Signature Standard (DSS), February 2023
{/new}

Rationale:

See issue description above.

Further Action:

Action by Network iTC: