Commercial Solutions for Classified (CSfC) Selections for Internet Protocol Security (IPsec) Virtual Private Network (VPN) Client

Overview

Internet Protocol Security (IPsec) Virtual Private Network (VPN) Client products (as defined in the Commercial Solutions for Classified (CSfC) Capability Packages (CPs)) used in CSfC solutions must be validated by National Information Assurance Partnership (NIAP)/Common Criteria Evaluation and Validation Scheme (CCEVS) or Common Criteria Recognition Arrangement (CCRA) partnering schemes as complying with the current requirements of NIAP's:

- Base Protection Profile (one of the following):
  - Protection Profile for General Purpose Operating Systems (GPOS PP), Version 5.0
  - Protection Profile for Mobile Device Fundamentals (MDF PP), Version 4.0
  - Protection Profile for Application Software Version 2.0
- Protection Profile Module (PP-Module) for VPN Client Version 3.0; and
- Functional Package for X.509 Version 1.0

This validated compliance must include the selectable requirements contained in this document.

IPsec VPN Client can be used/implemented in many different ways, threats and technology continuously progress, and IPsec VPN Client continue to evolve, which may cause the below selections to change or become obsolete. Vendors are encouraged to review the CSfC CPs to ensure the product functions appropriately in CSfC solutions. The objective of the below selections is to provide information to enable the use of the Commercial National Security Algorithm (CNSA) Suite and facilitate the use of IPsec VPN Clients in CSfC solutions.

Please provide questions, comments on usability, applicability, and/or shortcomings to the CSfC Program (csfc@nsa.gov).

Notes

Note 1: The following selections apply to CSfC IPsec VPN Client functionality. If needed, functionality and/or configurations outside the scope of a CSfC IPsec VPN Client that conflict with the CSfC selections could be NIAP validated without using a separate iteration of the Security Functional Requirement (SFR). The Security Target (ST) author should document a specific CSfC IPsec VPN Client configuration in the product's Administrative Guide with a note that the configuration should be considered the NIAP-certified evaluated configuration for CSfC IPsec VPN Client Use Cases. The CSfC IPsec VPN Client configuration should be used to validate compliance with CSfC selections.

Note 2: The below SFRs/Selections contain some mandatory SFRs without Selections or modifications. The exclusion of other mandatory SFRs in the below Selections does not indicate that mandatory PP SFRs are not required (i.e., Compliance with the requirements as prescribed by the PP, Functional Packages, and outlined in the Overview Section above are required). Some mandatory SFRs are included in the below Selections to highlight some SFRs relevant to CSfC IPsec VPN Client.

Note 3: Some of the below SFRs contain CSfC selections that are only applicable based on specific configurations, include the statement "at least one of" but may require more than one selection due to dependencies on other SFR that specify the selections required, and/or are only permitted for use in CSfC solutions for specific Use Cases. If needed, the CSfC CP, CSfC Application Notes, and the NIAP PP Application Notes provide more details on selection dependencies. For example:

- In FCS_CKM.1.1/AKG and FCS_CKM_EXT.7.1, Elliptic Curve P-384/ECDH P-384 must be selected because FCS_IPSEC_EXT.1.8 requires IKE DH Group 20 (384-bit Random ECP). Selecting RSA 3072 or MODP-3072/MODP-4096 does not satisfy that ECDH dependency.
- In FCS_CKM.1.1/AKG FFDHE selections such as MODP-3072 and/or MODP-4096 for IPsec and ffdhe3072 for Hypertext Transfer Protocol Secure (HTTPS)/Transport Layer Security (TLS) may also be required when finite-field Diffie-Hellman is selected for those Use Cases, but they do not replace the PP mandatory ECDH P-384 support for FCS_IPSEC_EXT.1.8.

In FCS_CKM.1.1/AKG, for CSfC solutions Leighton-Micali Signature (LMS) and Xtended Merkle Signature Scheme (XMSS) are encouraged but only permitted for digitally signing firmware and software.

Document Conventions

The conventions used in descriptions of the document are as follows:

- Assignment completed within a selection in the PP: the completed assignment text is indicated with *italicized and underlined text*
- Assignment partially completed in the PP: indicated with *italicized text*
- Refinement text is indicated with ~~strikethroughs~~
- CSfC specific selections, refinements (e.g., underline, strikethrough) are highlighted in light blue text (i.e., CSfC mandatory completed assignments/selections unless otherwise indicated by the `light blue Courier New Text` "at least one of the following underlined selections").
- Additional clarifying text or CSfC specific language is indicated with `light blue Courier New Text`
- Links to sources, additional information, and email addresses are indicated with blue underlined text.

Protection Profile Module (PP-Module) for VPN Client Version 3.0 Selections

FCS_IPSEC_EXT.1.2 The TSF shall implement [**selection**: *tunnel mode*, *transport mode*].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [*IKEv2 SA*] lifetimes can be configured by [**selection**: *an administrator*, *a VPN gateway*] based on [**selection**: *number of packets/number of bytes*,

length of time]]. If length of time is used, it must include at least one option that is 24 hours or less for IKE SAs and eight hours or less for Child SAs.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that IKE implements DH Groups

- 20 (384-bit Random ECP) according to RFC 5114 and

[**selection**:

- *15 (3072-bit MODP) according to RFC 3526*
- *16 (4096-bit MODP) according to RFC 3526*
- *17 (6144-bit MODP) according to RFC 3526*
- *18 (8192-bit MODP) according to RFC 3526*
- ~~*21 (521-bit Random ECP) according to RFC 5114*~~

].

Application Note: As of publication, for CSfC solutions, if FFDHE is selected for IPsec, RFC 3526 MODP-3072 and/or MODP-4096 must be used. In 2027, when applicable, new CSfC Components List components will be required to support ML-KEM-1024 and ML-DSA-87 for IPsec. See the CSfC CP for more details.

FCS_IPSEC_EXT.1.11 The TSF shall ensure that [*IKEv2*] performs peer authentication using [*[**selection**: RSA, ECDSA] that use X.509v3 certificates that conform to RFC 4945 and [**selection**: Pre-shared Keys that conform to RFC 8784, Pre-shared Keys transmitted via EAP-TTLS, EAP-TLS, no other method]*].

Application Note: For IPsec VPN Clients, vendors are highly encouraged but not required to select Pre-Shared Keys (PSK) that conform to Internet Engineering Task Force (IETF) Request for Comments (RFC) 8784/implement RFC 8784-compliant implementations of Internet Key Exchange (IKE) v2 in compliance with the CSfC Symmetric Key Management Requirements Annex. X.509v3 certificate-based peer authentication using RSA and/or ECDSA is required for data plane IKEv2 in CSfC solutions. PSK that conform to RFC 8784 are selected as an additional factor and do not replace X.509 certificate-based peer authentication (i.e., RFC 8784 PSK/PPKonly authentication is not permitted in CSfC solutions). If implemented, on the data plane, CSfC IPsec VPN clients must be configurable by an administrator or configured to require the use of PSK for IPsec VPN Connections by setting mandatory_or_not flag to True, to ensure an externally generated bit-based PSK is required to establish a connection in CSfC solutions.

FMT_SMF.1/VPN Specification of Management Functions (VPN)

FMT_SMF.1.1/VPN The TSF shall be capable of performing the following management functions: [**selection**:

- *Specify VPN gateways to use for connections*
- *Specify IPsec VPN clients to use for connections*
- *Specify IPsec-capable network devices to use for connections*
- *Specify client credentials to be used for connections*

- *Configure the reference identifier of the peer*
- *[**assignment**: any additional management functions]*

]

Protection Profile for General Purpose Operating System v5.0 Security Functional Requirements Direction and Selections

FCS_CKM.1/AKG Cryptographic Key Generation – Asymmetric Key

FCS_CKM.1.1/AKG The TSF shall generate **asymmetric** cryptographic keys in accordance with ~~a~~ at least one of the following underlined specified cryptographic key generation algorithm: [**selection:** *cryptographic key generation algorithm*] and at least one of the corresponding underlined specified cryptographic **algorithm parameters** ~~key sizes~~ [**selection**: *cryptographic algorithm parameters*] that meet the following: [**selection:** *list of standards*].

Identifier	Cryptographic Key Generation Algorithm	Cryptographic Algorithm Parameters	List of Standards
RSA	RSA	Modulus of size [**selection**: *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]
FFC-ERB	FFC-ERB - Extra Random Bits	Static domain parameters approved for [selection: • *IKE Groups [**selection**: MODP-3072, MODP-4096, MODP-6144, MODP-8192*], • *TLS Groups [**selection**: ffdhe-3072, ffdhe-4096, ffdhe-6144, ffdhe-8192*]]	NIST SP 800-56A Revision 3 (Section 5.6.1.1.3), [**selection**: *RFC 3526* [IKE groups], *RFC 7919* [TLS groups]]
FFC-RS	FFC-RS - Extra Random Bits	Static domain parameters approved for [selection:	NIST SP 800-56A Revision 3 (Section

		• *IKE Groups [**selection**: MODP-3072, MODP-4096, MODP-6144, MODP-8192*], • *TLS Groups [**selection**: ffdhe-3072, ffdhe-4096, ffdhe-6144, ffdhe-8192*]]	5.6.1.1.3), [**selection**: *RFC 3526* [IKE groups], *RFC 7919* [TLS groups]]
ML-KEM	ML-KEM	Parameter set = ML-KEM-1024	NIST FIPS PUB 203
ML-DSA	ML-DSA	Parameter set = ML-DSA-87	NIST FIPS PUB 204

Application Note:

See Note 3 above for example SFR dependencies for CSfC solutions.

In 2027, where applicable ML-KEM-1024, ML-DSA-87, LMS, and/or XMSS will be required for new CSfC Components List components. See the CSfC CP for more details.

If RSA is selected, 3072 must be selected. For RSA, the TOE can also support 4096, 6144, and 8192 but must support 3072. See Application Note for FCS_COP.1.1/SigGen for more details.

As of publication, for CSfC solutions, if FFDHE is selected for IPsec, RFC 3526 MODP-3072 or MODP-4096 must be used.

FCS_COP.1/AEAD Cryptographic Operation – Authenticated Encryption with Associated Data

FCS_COP.1.1/AEAD The TSF shall perform authenticated encryption with associated data in accordance with a specified cryptographic algorithm [**selection**: *cryptographic algorithm*] and cryptographic key sizes [**selection**: *cryptographic key sizes*] that meet the following: [**selection**: *list of standards*]

The following table provides the allowed choices for completion of the selection operations of FCS_COP.1/AEAD.

Identifier	Cryptographic Algorithm	Cryptographic key sizes	List of Standards
AES-CCM	AES in CCM mode with unpredictable, nonrepeating nonce, minimum size of 64 bits	[**selection**: ~~*128,*~~ *256]* bits	[**selection**: *ISO/IEC 18033-3:2010 (Subclause 5.2), FIPS PUB 197*] [AES]

			[**selection**: *ISO/IEC 19772:2020 (Clause 7), NIST SP 800-38C*] [CCM]
AES-GCM	AES in GCM mode with non-repeating IVs using [**selection**: *deterministic, RBG-based*], IV construction; the tag must be of length [**selection**: *96, 104, 112, 120, 128*] bits.	*256* bits	[**selection**: *ISO/IEC 18033-3:2010 (Subclause 5.2), FIPS PUB 197*] [AES] [**selection**: *ISO/IEC 19772:2020 (Clause 10), NIST SP 800- 38D*] [GCM]

Application Note: AES-GCM-256 must be selected and supported. GCM mode is mandatory in order to address the requirements for FCS_IPSEC_EXT.1

FCS_COP.1.1/Hash The TSF shall perform cryptographic hashing in accordance with ~~a~~ at least one of the following underlined specified cryptographic algorithm [selection: *SHA-256*, *SHA-384, SHA-512*, *SHA3-256*, *SHA3-384*, *SHA3-512*] that meets the following: [selection: *ISO/IEC 10118-3:2018 [SHA, SHA3], FIPS PUB 180-4 [SHA], FIPS PUB 202 [SHA3]*].

Application Note: In accordance with Committee on National Security Systems (CNSS) Policy 15 and the CSfC CP:

- SHA-1 hash is no longer permitted to be used as a hash function,
- SHA-256 is permitted only as part of LMS or XMSS.

The hash selection should be consistent with the overall strength of the algorithm used for signature generation.

FCS_COP.1.1/KeyedHash The TSF shall perform keyed hash message authentication in accordance with a specified cryptographic algorithm [**selection**: *keyed hash algorithm*, *implicit*] and cryptographic key sizes [selection: *cryptographic key sizes*] that meet the following: [**selection**: *list of standards*].

The following table provides the allowed choices for completion of the selection operations of FCS_COP.1.1/KeyedHash.

Keyed Hash Algorithm	**Cryptographic Key Sizes**	**List of Standards**
~~HMAC-SHA256~~	~~256 bits~~	~~[selection: *ISO/IEC 9797-2:2021 (Section 7 "MAC Algorithm 2"), FIPS PUB 198-1*]~~

HMAC-SHA384	[**selection**: *384 (ISO, FIPS), 256 (FIPS)*] bits	[**selection**: *ISO/IEC 9797-2:2021 (Section 7 "MAC Algorithm 2"), FIPS PUB 198-1*]
HMAC-SHA512	[**selection**: *512 (ISO, FIPS), 384 (FIPS), 256 (FIPS)*] bits	[**selection**: *ISO/IEC 9797-2:2021 (Section 7 "MAC Algorithm 2"), FIPS PUB 198-1*]

FCS_COP.1/SigGen Cryptographic Operation - Signature Generation

FCS_COP.1.1/SigGen The TSF shall perform digital signature generation in accordance with `at least one of the following underlined` specified cryptographic algorithm [**selection**: *cryptographic algorithm*] and `at least one of the corresponding underlined` cryptographic key sizes [selection: *cryptographic key sizes*] that meet the following: [**selection**: *list of standards*].

The following table provides the allowed choices for completion of the selection operations of FCS_COP.1.1/SigGen.

Cryptographic Algorithm	**Cryptographic Key Sizes**	**List of Standards**
RSASSA-PKCS1- v1_5	Modulus of size [**selection**: *3072, 4096, 6144, 8192*] bits and hash [selection: *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**: *3072, 4096, 6144, 8192*] bits and hash [**selection**: *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-384*, ~~*P-521*~~], per-message secret number generation [**selection**: *extra random bits, rejection sampling, deterministic*] and hash function using [**selection**: *SHA-384, SHA-512*]	[**selection**: *ISO/IEC 14888-3:2018 (Subclause 6.6), FIPS PUB 186-5 (Sections 6.3.1, 6.4.1)*][ECDSA], NIST SP-800 186 (Section 4) [NIST Curves]

Module-Lattice Based Digital Signature Algorithm	ML-DSA-87	NIST FIPS PUB 204 (Section 5.2)

Application Note: As of publication, for CSfC solutions, X.509 v3 certificates used for IPsec must be signed with ECDSA or RSA. In 2027, where applicable, ML-DSA-87, LMS and/or XMSS for digitally signing firmware and software and ML-DSA-87 for certificate digital signatures will be required for new CSfC Components List components. See the MA CP for more details.

If RSASSA-PKCS1- v1_5 and/or RSASSA-PSS is selected, 3072 must be selected. For RSASSA-PKCS1- v1_5 or RSASSA-PSS, the TOE can also support 4096, 6144, and 8192 but must support 3072.

FCS_COP.1/SigVer Cryptographic Operation - Signature Verification

FCS_COP.1.1/SigVer The TSF shall perform digital signature verification in accordance with at least one of the following underlined specified cryptographic algorithms [**selection**: *cryptographic algorithm*] and at least one of the corresponding underlined cryptographic key sizes [**selection**: *cryptographic key sizes*] that meet the following: [**selection**: *list of standards]*.

The following table provides the allowed choices for completion of the selection operations of FCS_COP.1.1/SigVer.

Cryptographic Algorithm	**Cryptographic Key Sizes**	**List of Standards**
RSASSA-PKCS1- v1_5	Modulus of size [**selection**: ~~*2048,*~~ *3072*, *4096*, *6144*, *8192*] bits and hash [**selection**: *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-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-384*, ~~*P-521*~~] using hash [**selection**: *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]
LMS	Private key size = [**selection**:	RFC 8554 [LMS], NIST SP 800-208 [parameters]

	• *192 bits with [**selection**: SHA-256/192, SHAKE256/192]* • *256 bits with [**selection**: SHA-256, SHAKE256]*] Winternitz parameter = [selection: 1, 2, 4, 8] Tree height = [**selection**: *5, 10, 15, 20, 25*]	
XMSS	XMSS private key size [**selection**: • *192 bits with [**selection**: SHA-256/192, SHAKE256/192]* • *256 bits with [**selection**: SHA-256, SHAKE256]]* Tree height = [**selection**: *10, 16, 20*]	RFC 8391 [XMSS], NIST SP 800-208 [parameters]
ML-DSA	ML-DSA-87	NIST FIPS PUB 204 (Section 5.3)

Application Note: As of publication, for CSfC solutions, X.509 v3 certificates used for IPsec and HTTPS/TLS must be signed with ECDSA or RSA. In 2027, where applicable, ML-DSA-87, LMS and/or XMSS for digitally signing firmware and software and ML-DSA-87 for certificate digital signatures will be required for new CSfC Components List components. See the MA CP for more details.

FCS_RBG.1.2 The TSF shall use a [**selection**: *TSF entropy source [assignment: name of entropy source**], multiple independent TSF entropy sources [assignment: names of entropy sources]***, *TSF interface for obtaining entropy*] for initialization and reseeding.

FCS_RBG.2.1 The TSF shall be able to accept a minimum input of [*384 bits of min-entropy*] from a TSF interface for obtaining entropy.

Application Note: The objective of this SFR selection is to invoke/use a hardware-based noise/entropy source for DRBG functionality.

FCS_CKM_EXT.7 Cryptographic Key Agreement

FCS_CKM_EXT.7.1 The TSF shall derive shared cryptographic keys with input from multiple parties in accordance with at least one of the following underlined specified cryptographic key agreement algorithms [**selection**: cryptographic algorithm] and at least one of the

corresponding underlined specified cryptographic parameters [**selection**: cryptographic parameters] that meet the following: [**selection**: list of standards]

The following table provides the allowed choices for completion of the selection operations of FCS_CKM_EXT.7.1.

Identifier	Cryptographic Algorithm	Cryptographic Parameters	List of Standards
~~KAS2~~	~~RSA~~	~~Modulus size [selection: 3072, 4096, 6144, 8192] bits~~	~~NIST SP 800-56B Revision 2 (Section 8.3) [KAS2]~~
DH	Finite Field Cryptography Diffie-Hellman	If selected, at least one of the following underlined static domain parameters approved for [**selection**: • *IKE Groups [**selection**: MODP-3072, MODP-4096, MODP-6144, MODP-8192],* • *TLS Groups [**selection**: ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192]]*	NIST SP 800-56A Revision 3 (Section 5.7.1.1), [**selection**: *RFC 3526 [IKE groups], RFC 7919 [TLS groups]*]
ECDH	Elliptic Curve Diffie-Hellman	Elliptic Curve [**selection**: ~~*P-256*~~, *P-384*, ~~*P-521*~~]	NIST SP 800-56A Revision 3 (Section 5.7.1.2) [ECDH], NIST SP 800-186 (Section 3.2.1) [NIST Curves]

Application Note: As of publication, ECDH P-384 must be selected. As of publication, for CSfC solutions, if FFDHE is selected for IPsec, RFC 3526 MODP-3072 or MODP-4096 must be used. In 2027, where applicable, ML-KEM-1024 will be required for new CSfC Components List components. See the Mobile Access (MA) CP for more details.

Protection Profile for Mobile Device Fundamentals v4.0 Security Functional Requirements Direction and Selections

FCS_CKM.1.1/AKG The TSF shall generate **asymmetric** cryptographic keys in accordance with-a at least one of the following underlined specified cryptographic key generation algorithms: [selection: *cryptographic key generation algorithm*] and at least one of the corresponding underlined specified cryptographic **algorithm parameters** ~~key sizes~~ [selection: *cryptographic algorithm parameters*] that meet the following: [selection: *list of standards*].

Identifier	Cryptographic Key Generation Algorithm	Cryptographic Algorithm Parameters	List of Standards
RSA	RSA	Modulus of size [**selection**: *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]
FFC-ERB	FFC-ERB - Extra Random Bits	Static domain parameters approved for [selection: • *IKE Groups [**selection**: MODP-3072, MODP-4096, MODP-6144, MODP-8192*], • *TLS Groups [**selection**: ffdhe-3072, ffdhe-4096, ffdhe-6144, ffdhe-8192*]]	NIST SP 800-56A Revision 3 (Section 5.6.1.1.3), [**selection**: *RFC 3526* [IKE groups], *RFC 7919* [TLS groups]]
FFC-RS	FFC-RS - Extra Random Bits	Static domain parameters approved for [selection: • *IKE Groups [**selection**: MODP-3072, MODP-4096, MODP-6144, MODP-8192*], • *TLS Groups [**selection**: ffdhe-3072, ffdhe-4096, ffdhe-6144, ffdhe-8192*]]	NIST SP 800-56A Revision 3 (Section 5.6.1.1.3), [**selection**: *RFC 3526* [IKE groups], *RFC 7919* [TLS groups]]

EdDSA	EdDSA	Domain parameters approved for elliptic curves [*Edwards25519*]	NIST FIPS PUB 186-5 (section 6.2.1)[key-pair generation] NIST SP 800-186 (Section 3.2.3)[Edwards Curves]
LMS	LMS	private key size [**selection**: • *192 bits with [**selection**: SHA-256/192, SHAKE256/192*], • *256 bits with [**selection**: SHA-256, SHAKE256*]] Winternitz parameter = [**selection**: *1, 2, 4, 8*], Tree height = [**selection**: *5, 10, 15, 20, 25*]	RFC 8554 [LMS], NIST SP 800-208 [parameters]
XMSS	XMSS	private key size [**selection**: • *192 bits with [**selection**: SHA-256/192, SHAKE256/192*] • *256 bits with [**selection**: SHA-256, SHAKE256*]] Tree height = [**selection**: *10, 16, 20*]	RFC 8391 [XMSS], NIST SP 800-208 [parameters]
ML-KEM	ML-KEM	Parameter set = ML-KEM-1024	NIST FIPS PUB 203
ML-DSA	ML-DSA	Parameter set = ML-DSA-87	NIST FIPS PUB 204

Application Note:

See Note 3 above for example SFR dependencies for CSfC solutions.

In 2027, where applicable ML-KEM-1024, ML-DSA-87, LMS, and/or XMSS will be required for new CSfC Components List components. See the CSfC CP for more details.

If RSA is selected, 3072 must be selected. For RSA, the TOE can also support 4096, 6144, and 8192 but must support 3072. See Application Note for FCS_COP.1.1/SigGen for more details. As of publication, for CSfC solutions, if FFDHE is selected for IPsec, RFC 3526 MODP-3072 or MODP-4096 must be used.

FCS_CKM_EXT.7/UNLOCKED Cryptographic Key Agreement

FCS_CKM_EXT.7.1/UNLOCKED The TSF shall derive shared cryptographic keys with input from multiple parties in accordance with at least one of the following underlined specified

cryptographic key agreement algorithms [**selection**: cryptographic algorithm] and at least one of the corresponding underlined specified cryptographic parameters [**selection**: cryptographic parameters] that meet the following: [**selection**: list of standards]

The following table provides the allowed choices for completion of the selection operations of FCS_CKM_EXT.7/UNLOCKED.

Identifier	Cryptographic Algorithm	Cryptographic Parameters	List of Standards
DH	Finite Field Cryptography Diffie-Hellman	If selected, at least one of the following underlined static domain parameters approved for [**selection**: • *IKE Groups [**selection**: MODP-3072, MODP-4096, MODP-6144, MODP-8192],* • *TLS Groups [**selection**: ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192]]*	NIST SP 800-56A Revision 3 (Section 5.7.1.1), [**selection**: *RFC 3526 [IKE groups], RFC 7919 [TLS groups]*]
ECDH	Elliptic Curve Diffie-Hellman	Elliptic Curve [**selection**: ~~*P-256*~~, *P-384*, ~~*P-521*~~]	NIST SP 800-56A Revision 3 (Section 5.7.1.2) [ECDH], NIST SP 800-186 (Section 3.2.1) [NIST Curves]

Application Note: As of publication, ECDH P-384 must be selected. As of publication, for CSfC solutions, if FFDHE is selected for IPsec, RFC 3526 MODP-3072 or MODP-4096 must be used. In 2027, where applicable, ML-KEM-1024 will be required for new CSfC Components List components. See the Mobile Access (MA) CP for more details.

FCS_COP.1/AEAD Cryptographic Operation – Authenticated Encryption with Associated Data

FCS_COP.1.1/AEAD The TSF shall perform authenticated encryption with associated data in accordance with a specified cryptographic algorithm [selection: *cryptographic algorithm*] and cryptographic key sizes [selection: *cryptographic key sizes*] that meet the following: [selection: *list of standards*]

The following table provides the allowed choices for completion of the selection operations of FCS_COP.1/AEAD.

Identifier	Cryptographic Algorithm	Cryptographic Algorithm Parameters	List of Standards

AES-CCM	AES in CCM mode with unpredictable, nonrepeating nonce, minimum size of 64 bits	[**selection**: ~~*128,*~~ *256]* bits	[**selection**: *ISO/IEC 18033-3:2010 (Subclause 5.2), FIPS PUB 197*] [AES] [**selection**: *ISO/IEC 19772:2020 (Clause 7), NIST SP 800-38C*] [CCM]
AES-GCM	AES in GCM mode with non-repeating IVs using [**selection**: *deterministic, DRBG-based*], IV construction; the tag must be of length [**selection**: *96, 104, 112, 120, 128*] bits.	256 bits	[**selection**: *ISO/IEC 18033-3:2010 (Subclause 5.2), FIPS PUB 197*] [AES] [**selection**: *ISO/IEC 19772:2020 (Clause 10), NIST SP 800- 38D*] [GCM]

Application Note: AES-GCM-256 must be selected and supported. GCM mode is mandatory in order to address the requirements for FCS_IPSEC_EXT.1

FCS_COP.1.1/Hash The TSF shall perform cryptographic hashing in accordance with ~~a~~ at least one of the following underlined specified cryptographic algorithm [selection: *SHA-256, SHA-384, SHA-512, SHA3-256, SHA3-384, SHA3-512*] that meets the following: [selection: *ISO/IEC 10118-3:2018 [SHA, SHA3], FIPS PUB 180-4 [SHA], FIPS PUB 202 [SHA3]*].

Application Note: In accordance with Committee on National Security Systems (CNSS) Policy 15 and the CSfC CP:

- SHA-1 hash is no longer permitted to be used as a hash function,
- SHA-256 is permitted only as part of LMS or XMSS.

The hash selection should be consistent with the overall strength of the algorithm used for signature generation.

FCS_COP.1.1/KeyedHash The TSF shall perform keyed hash message authentication in accordance with a specified cryptographic algorithm [selection: *keyed hash algorithm, implicit*] and cryptographic key sizes [selection: *cryptographic key sizes*] that meet the following: [selection: *list of standards*].

The following table provides the allowed choices for completion of the selection operations of FCS_COP.1.1/KeyedHash.

Keyed Hash Algorithm	**Cryptographic Key Sizes**	**List of Standards**
~~HMAC-SHA256~~	~~256 bits~~	~~[selection: *ISO/IEC 9797-2:2021 (Section 7 "MAC Algorithm 2"), FIPS PUB 198-1*]~~

HMAC-SHA384	[selection: *384 (ISO, FIPS), 256 (FIPS)*] bits	[**selection**: *ISO/IEC 9797-2:2021 (Section 7 "MAC Algorithm 2"), FIPS PUB 198-1*]
HMAC-SHA512	[selection: *512 (ISO, FIPS), 384 (FIPS), 256 (FIPS)*] bits	[**selection**: *ISO/IEC 9797-2:2021 (Section 7 "MAC Algorithm 2"), FIPS PUB 198-1*]

FCS_COP.1/SigGen Cryptographic Operation - Signature Generation

FCS_COP.1.1/SigGen The TSF shall perform digital signature generation in accordance with `at least one of the following underlined` specified cryptographic algorithms [selection: *cryptographic algorithm*] and `at least one of the corresponding underlined` cryptographic key sizes [selection: *cryptographic key sizes*] that meet the following: [selection: *list of standards*].

The following table provides the allowed choices for completion of the selection operations of FCS_COP.1.1/SigGen.

Cryptographic Algorithm	**Cryptographic Key Sizes**	**List of Standards**
RSASSA-PKCS1- v1_5	Modulus of size [**selection**: *3072, 4096, 6144, 8192*] bits and hash [**selection**: *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**: *3072, 4096, 6144, 8192*] bits and hash [**selection**: *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-384*, ~~*P-521*~~], per-message secret number generation [**selection**: *extra random bits, rejection sampling, deterministic*] and hash function using [**selection**: *SHA-384, SHA-512*]	[**selection**: *ISO/IEC 14888-3:2018 (Subclause 6.6), FIPS PUB 186-5 (Sections 6.3.1, 6.4.1)*][ECDSA], NIST SP-800 186 (Section 4) [NIST Curves]

ML-DSA Signature Generation	Parameter set = ML-DSA-87	NIST FIPS PUB 204 (Section 5.2)

Application Note: As of publication, for CSfC solutions, X.509 v3 certificates used for IPsec must be signed with ECDSA or RSA. In 2027, where applicable, ML-DSA-87, LMS and/or XMSS for digitally signing firmware and software and ML-DSA-87 for certificate digital signatures will be required for new CSfC Components List components. See the MA CP for more details.

If RSASSA-PKCS1- v1_5 and/or RSASSA-PSS is selected, 3072 must be selected. For RSASSA-PKCS1- v1_5 or RSASSA-PSS, the TOE can also support 4096, 6144, and 8192 but must support 3072.

FCS_COP.1/SigVer Cryptographic Operation - Signature Verification

FCS_COP.1.1/SigVer The TSF shall perform digital signature verification in accordance with at least one of the following underlined specified cryptographic algorithm [selection: *cryptographic algorithm*] and at least one of the corresponding underlined cryptographic key sizes [selection: *cryptographic key sizes*] that meet the following: [selection: *list of standards]*.

The following table provides the allowed choices for completion of the selection operations of FCS_COP.1.1/SigVer.

Cryptographic Algorithm	**Cryptographic Key Sizes**	**List of Standards**
RSASSA-PKCS1- v1_5	Modulus of size [**selection**: *3072, 4096, 6144, 8192*] bits and hash [**selection**: *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**: *3072, 4096, 6144, 8192*] bits and hash [**selection**: *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-384*, ~~*P-521*~~] using hash [**selection**: *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]
LMS	Private key size = [**selection**: • *192 bits with [**selection**: SHA-256/192, SHAKE256/192]*	RFC 8554 [LMS], NIST SP 800-208 [parameters]

	• *256 bits with [**selection**: SHA-256, SHAKE256]*] Winternitz parameter = [**selection**: 1, 2, 4, 8] Tree height = [**selection**: *5, 10, 15, 20, 25*]	
XMSS	XMSS private key size [**selection**: • *192 bits with [**selection**: SHA-256/192, SHAKE256/192]* • *256 bits with [**selection**: SHA-256, SHAKE256]*] Tree height = [**selection**: *10, 16, 20*]	RFC 8391 [XMSS], NIST SP 800-208 [parameters]
ML-DSA Signature Verification	Parameter set = ML-DSA-87	NIST FIPS PUB 204 (Section 5.3)

Application Note: As of publication, for CSfC solutions, X.509 v3 certificates used for IPsec and HTTPS/TLS must be signed with ECDSA or RSA. In 2027, where applicable, ML-DSA-87, LMS and/or XMSS for digitally signing firmware and software and ML-DSA-87 for certificate digital signatures will be required for new CSfC Components List components. See the MA CP for more details.

FCS_RBG.1.2 The TSF shall use a [**selection**: *TSF entropy source [**assignment**: name of entropy source]*, ***multiple independent TSF entropy sources [assignment: names of entropy sources]***, ~~*TSF interface for obtaining entropy*~~] for initialization and reseeding.

FCS_RBG.3.1 The TSF shall be able to seed the DRBG using a [**selection, choose one of**: *TSF software-based entropy source*, *TSF hardware-based entropy source*] [**assignment**: *name of entropy source*] with [*a minimum of 384*] bits of min-entropy.

FCS_RBG.4.1 The TSF shall be able to seed the DRBG using [selection: [*assignment: number] independent TSF software-based entropy source(s)*, *[assignment: one or more] independent TSF hardware-based entropy source(s)]*.

FDP_IFC_EXT.1: Subset Information Flow Control

This SFR is identical to its definition in the Base-PP except that the selection item that requires the TOE to implement its own VPN client is always selected when the TOE's conformance claim includes this PP-Module.

The text of the requirement is replaced with:

FDP_IFC_EXT.1.1 The TSF shall [

- *provide a VPN client which can protect all IP traffic using IPsec as defined in the PP-Module for VPN Client*

] with the exception of IP traffic needed to manage the VPN connection, and [**selection:** *[**assignment:** ~~traffic needed for correct functioning of the TOE~~ `IKEv2, network address configuration, time synchronization, name resolution traffic required to establish the IPsec tunnel`], no other traffic*] when the VPN is enabled.

Protection Profile for Application Software Version 2.0 Security Functional Requirements Direction and Selections

FCS_CKM.1/AK: Cryptographic Asymmetric Key Generation

This SFR is selection-based in the App PP depending on the selection made in FCS_CKM_EXT.1. Because key generation services (whether implemented by the TOE or invoked from the platform) are required for IPsec, this SFR is mandatory for any TOE that claims conformance to this PP-Module.

This SFR is functionally identical to what is defined in the App PP except that ECC key generation with P-384 has been made mandatory in support of IPsec due to the mandated support for DH group 20 in FCS_IPSEC_EXT.1.8. RSA remains present as a selection since it may be used by parts of the TOE that are not specifically related to VPN client functionality. The selection for "no other key generation methods" was added in case the algorithms that IPsec requires are the TSF's only use of key generation.

The text of the requirement is replaced with:

The **application** shall [**selection**:

- *invoke platform-provided functionality*
- *implement functionality*

] to generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm

- ***[ECC schemes] using ["NIST curves" P-384 and [selection: ~~P-521~~, no other curves]] that meet the following: [FIPS PUB 186-5, "Digital Signature Standard (DSS)," Appendix A.2]***

and [**selection**:

- ***[RSA schemes]*** *using cryptographic key sizes of [**assignment**: 3072-bit or greater] that meet the following: [FIPS PUB 186-5, "Digital Signature Standard (DSS)," Appendix A.1]*
- ***[FFC Schemes]*** *using ["safe-prime" groups] [**selection**:*
    - *MODP-3072*
    - *MODP-4096*
    - *MODP-6144*
    - *MODP-8192*
    - *ffdhe-3072*
    - *ffdhe-4096*
    - *ffdhe-6144*
    - *ffdhe-8192*

*] that meet the following: [NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [**selection**: RFC 3526, RFC 7919]]*

- ***Leighton-Micali Signature*** *Algorithm using the parameter sets*
    - *LMS_SHAKE_M24_H5*
    - *LMS_SHAKE_M24_H10*
    - *LMS_SHAKE_M24_H15*
    - *LMS_SHAKE_M24_H25*
    - *LMS_SHAKE_M32_H5*
    - *LMS_SHAKE_M32_H10*
    - *LMS_SHAKE_M32_H15*
    - *LMS_SHAKE_M32_H25*
    - *LMS_SHA256_M24_H5*
    - *LMS_SHA256_M24_H10*
    - *LMS_SHA256_M24_H15*
    - *LMS_SHA256_M24_H25*
    - *LMS_SHA256_M32_H5*
    - *LMS_SHA256_M32_H10*
    - *LMS_SHA256_M32_H15*
    - *LMS_SHA256_M32_H25*

] that meet the following: [NIST SP 800-208, "Recommendation for Stateful Hash-Based Signature Schemes"]

- ***eXtended Merkle Signature Scheme*** *Algorithm using the parameter sets*
    - *XMSS-SHA2_10_192*
    - *XMSS-SHA2_16_192*
    - *XMSS-SHA2_20_192*
    - *XMSS-SHA2_10_256*

- *XMSS-SHA2_16_256*
- *XMSS-SHA2_20_256*
- *XMSS-SHAKE_10_192*
- *XMSS-SHAKE_16_192*
- *XMSS-SHAKE_20_192*
- *XMSS-SHAKE_10_256*
- *XMSS-SHAKE_16_256*
- *XMSS-SHAKE_20_256*

] bits that meets the following: [NIST SP 800-208, "Recommendation for Stateful Hash-Based Signature Schemes"]

- ***Module-Lattice-Based Key-Encapsulation Mechanism Standard** using the parameter set ML-KEM-1024 that meets the following: [FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard]*
- ***Module-Lattice-Based Digital Signature Standard** using the parameter set ML-DSA-87 that meets the following [FIPS 204, Module-Lattice-Based Digital Signature Standard]*
- ***no other key generation methods***

].

Application Note:

See Note 3 above for example SFR dependencies for CSfC solutions.

As of publication, for CSfC solutions, if FFDHE is selected for IPsec, RFC 3526 MODP-3072 or MODP-4096 must be used.

In 2027, where applicable ML-KEM-1024, ML-DSA-87, LMS, and/or XMSS will be required for new CSfC Components List components. See the CSfC CP for more details.

If RSA is selected, 3072 must be selected. For RSA, the TOE can also support 4096, 6144, and 8192 but must support 3072. See Application Note for FCS_COP.1.1/SigGen for more details.

FCS_CKM.2: Cryptographic Key Establishment

This SFR differs from its definition in the App PP by moving elliptic curve-based key establishment schemes from selectable to mandatory due to the mandated support for DH group 20 in FCS_IPSEC_EXT.1.8. The selection for "no other schemes" was added in case the algorithms that IPsec requires are the TSF's only use of key establishment.

The text of the requirement is replaced with:

The **application** shall **[selection:**

- ***invoke platform-provided functionality***
- ***implement functionality***

] to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method:

- **[Elliptic curve-based key establishment schemes] that meet the following: [NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"]**

[**selection:**

- ***[RSA-based key establishment schemes]*** *that meet the following:* ***[NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization 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:*** *RFC 3526, RFC 7919]*
- ***Module-Lattice-Based Key-Encapsulation Mechanism Standard*** *using* ***the parameter set ML-KEM-1024*** *that meets the following: [FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard]*
- ***no other key establishment schemes***

].

Application Note: As of publication, for CSfC solutions, if FFDHE is selected for IPsec, RFC 3526 MODP-3072 or MODP-4096 must be used. In 2027, where applicable, ML-KEM-1024 will be required for new CSfC Components List components. See the Mobile Access (MA) CP for more details.

FCS_CKM_EXT.1.1 The application shall [**selection**:

- ~~*generate no asymmetric cryptographic keys*~~
- *invoke platform-provided functionality for asymmetric key generation*
- *implement asymmetric key generation*

].

FCS_RBG_EXT.1.1

The application shall [selection:

- ~~*use no DRBG functionality*~~
- *invoke platform-provided DRBG functionality*
- ~~*implement DRBG functionality*~~

] for its cryptographic operations.

FCS_STO_EXT.1 Storage of Credentials

FCS_STO_EXT.1.1 The application shall [**selection**:

- *not store any credentials*
- *invoke the functionality provided by the platform to securely store [**assignment**: list of credentials]*
- *securely store [**assignment**: list of credentials] with platform provided [**selection**:*
  - *[**selection**:*
    - *AES-CBC (as defined in NIST SP 800-38A) mode*
    - *AES-GCM (as defined in NIST SP 800-38D) mode*
    - *AES-XTS (as defined in NIST SP 800-38E) mode*

    ] and cryptographic key size of 256-bits.
  - *PBKDF2 function that uses [**selection**:*
    - ~~*HMAC-SHA256*~~
    - *HMAC-SHA384*
    - *HMAC-SHA512*

    *] with [**assignment**: positive integer of 1,000 or greater] iterations and output cryptographic key size of [**assignment**: positive integer of 256 of greater] bits that meet the following [NIST SP 800-132].*

  ]
- *implement functionality to securely store [**assignment**: list of credentials] according to [**selection**: FCS_COP.1/SKC, FCS_PBKDF_EXT.1]*

] to non-volatile memory.

Application Note: This requirement ensures that persistent credentials (secret keys, PKI private keys, passwords, etc) are stored securely, and never persisted in cleartext form. Application developers are encouraged to use platform mechanisms for the secure storage of credentials. Depending on the platform that may include hardware-backed protection for credential storage. Application developers must choose a selection, or multiple selections, based on all credentials that the application stores. If "**not store any credentials**" is selected, then the application must not store any credentials. If "**invoke the functionality provided by the platform to securely store**" is selected, then the application developer must closely review the EA for their platform and provide documentation indicating which platform mechanisms are used to store credentials. If "**securely store**" is selected, the application shall leverage platform cryptographic APIs to implement storage of credentials. If "**implement functionality to securely store credentials**" is selected, then the following components must be included in the ST: (FCS_COP.1/SKC and FCS_SNI_EXT.1) or FCS_PBKDF_EXT.1. If the OS is Linux and Java KeyStores are used to store credentials, "**implement functionality to securely store credentials**" must be selected.

FCS_COP.1/Hash Cryptographic Operation - Hashing

FCS_COP.1.1/Hash The **application** shall perform [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm [**selection**:

- *SHA-256*

- *SHA-384*
- *SHA-512*

] and **message digest** sizes [**selection**:

- *256*
- *384*
- *512*

] **bits** that meet the following: [FIPS Pub 180-4, "Secure Hash Standard"].

Application Note: In accordance with Committee on National Security Systems (CNSS) Policy 15 and the CSfC CP:

- SHA-1 hash is no longer permitted to be used as a hash function,
- SHA-256 is permitted only as part of LMS or XMSS. The hash selection should be consistent with the overall strength of the algorithm used for signature generation.

FCS_COP.1/KeyedHash Cryptographic Operation - Keyed-Hash Message Authentication

FCS_COP.1.1/KeyedHash The **application** shall perform [*keyed-hash message authentication*] in accordance with a specified cryptographic algorithm [**selection**:

- ~~*HMAC-SHA-256*~~
- *HMAC-SHA-384*
- *HMAC-SHA-512*

] **with** key sizes [**assignment**: key size (in bits) used in HMAC] **and message digest sizes** [**selection**: 256, 384, 512] bits that meet the following: [FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code," and FIPS Pub 180-4, "Secure Hash Standard"].

FCS_COP.1/SigGen Cryptographic Operation - Signing Generation

FCS_COP.1.1/SigGen The **application** shall perform [*cryptographic signature services (generation)*] in accordance with a specified cryptographic algorithm [**selection**:

- *CNSA 2.0 Compliant Algorithm:*
  - ***Module-Lattice-Based Digital Signature Standard** using the parameter set ML-DSA-87 that meets the following [FIPS 204, Module-Lattice-Based Digital Signature Standard]*
- *CNSA 1.0 Compliant Algorithms: [**selection**:*
  - ***RSA schemes** using cryptographic key sizes of [3072-bit or greater] that meet the following: [FIPS PUB 186-5, "Digital Signature Standard (DSS)," Section 5]*
  - ***ECDSA schemes** using ["NIST curves" [**selection**: P-384, ~~P-521~~]] that meet the following: [FIPS PUB 186-5, "Digital Signature Standard (DSS)," Section 6]*

  ]

].

Application Note: As of publication, for CSfC solutions, X.509 v3 certificates used for IPsec and HTTPS/TLS must be signed with ECDSA or RSA.

In 2027, where applicable, ML-DSA-87 will be required for new CSfC Components List components. See the MA CP for more details.

FCS_COP.1/SigVer Cryptographic Operation - Signing Verification

FCS_COP.1.1/SigVer The **application** shall perform [*cryptographic signature services (verification)*] in accordance with a specified cryptographic algorithm [**selection**:

- *CNSA 2.0 Compliant Algorithms: [**selection**:*
  - ***Leighton-Micali Signature Algorithm** for verification using cryptographic key sizes of [**selection**: 192, 256] bits that meet the following [NIST SP 800-208, "Recommendation for Stateful Hash-Based Signature Schemes"]*
  - ***eXtended Merkle Signature Scheme Algorithm** for verification using cryptographic key sizes of [**selection**: 192, 256] bits that meets the following: [NIST SP 800-208, "Recommendation for Stateful Hash-Based Signature Schemes"]*
  - ***Module-Lattice-Based Digital Signature Standard** using the parameter set ML-DSA-87 that meets the following [FIPS 204, Module-Lattice-Based Digital Signature Standard]*

  ]
- *CNSA 1.0 Compliant Algorithms: [**selection**:*
  - ***RSA schemes** using cryptographic key sizes of [3072-bit or greater] that meet the following: [FIPS PUB 186-5, "Digital Signature Standard (DSS)," Section 5]*
  - ***ECDSA schemes** using ["NIST curves" [**selection**: P-384, ~~P-521~~]] that meet the following: [FIPS PUB 186-5, "Digital Signature Standard (DSS)," Section 6]*

  ]

].

Application Note: As of publication, for CSfC solutions, X.509 v3 certificates used for IPsec must be signed with ECDSA or RSA. In 2027, where applicable, ML-DSA-87, LMS and/or XMSS for digitally signing firmware and software and ML-DSA-87 for certificate digital signatures will be required for new CSfC Components List components. See the MA CP for more details.

If RSASSA-PKCS1- v1_5 and/or RSASSA-PSS is selected, 3072 must be selected. For RSASSA-PKCS1- v1_5 or RSASSA-PSS, the TOE can also support 4096, 6144, and 8192 but must support 3072.

FCS_RBG.1 Random Bit Generation (RBG)

The inclusion of this selection-based component depends upon selection in FCS_RBG_EXT.1.1.

FCS_RBG.1.1 The TSF shall perform deterministic random bit generation services using [**selection**:

- *Hash_DRBG (*[**selection:** *SHA-384, SHA-512*]*)*
- *HMAC_DRBG (*[**selection:** *SHA-384, SHA-512*]*)*
- *CTR_DRBG (AES-CTR-256)*

] in accordance with [NIST SP 800-90A] after initialization with a seed.

FCS_RBG.1.2 The TSF shall use a [**selection**: ~~*TSF noise source [assignment: name of noise source]*~~, *multiple TSF noise sources [assignment: names of noise sources], TSF interface for seeding*] for initialized seeding.

Application Note: The objective of the RBG selections is to ensure the TOE uses a TSF interface for a hardware-based noise source to seed the DRBG.

FCS_RBG.2 Random Bit Generation (External Seeding)

The inclusion of this selection-based component depends upon selection in FCS_RBG.1.2.

FCS_RBG.2.1 The TSF shall be able to accept a minimum input of [**assignment**: *256-bits*] from a TSF interface for the purpose of seeding.

Application Note: If CTR_DRBG is selected in FCS_RBG.1.1 and there is no derivation function, then the minimum bits of entropy must be at least 384.

FCS_RBG.5 Random Bit Generation (Combining Noise Sources)

The inclusion of this selection-based component depends upon selection in FCS_RBG.1.2.

FCS_RBG.5.1 The TSF shall [**assignment**: *combining operation*] [**selection**: *output from TSF noise source(s), input from TSF interface(s) for seeding*] to create the entropy input into the derivation function as defined in [**assignment**: *list of standards*] , resulting in a minimum of [**assignment**: *256*] bits of min-entropy.

Functional Package for X.509 Version 1.0 Selections

FIA_XCU_EXT.1 Implementation of X.509 Functions

FIA_XCU_EXT.1.1 The TSF shall [**selection**: *verify, assert*] identities included in X.509 certificates.

Application Note: The ST author claims "verify" when the TOE associates identities included in X.509 certificates with users, external entities or inter-TOE entities authorized to exercise TOE functionality. The ST author claims "assert" when the TOE represents itself or its functions to internal or external entities.

If "verify" is selected, then FIA_X509_EXT.1 and FIA_X509_EXT.2 must be included. If "assert" is selected, FIA_XCU_EXT.2 must be included.

FIA_ESTC_EXT.1 EST Client Certificate Enrollment

The inclusion of this selection-based component depends upon `if the TOE uses EST and` ***selection in FIA_X509_EXT.3.1***.

FIA_ESTC_EXT.1.4 The TSF shall [**selection**: *invoke platform-provided functionality*, *provide functionality*] to authenticate its certificate enrollment request to receive [**assignment**: *list of certificates*] from an authorized EST server using [**selection**:

- ~~*HTTP basic authentication transported over TLS (HTTPS) in accordance with RFC 7030 section 3.2.3*~~
- ~~*HTTP digest authentication using a cryptographic hash algorithm transported over TLS (HTTPS) in accordance with RFC 7030 section 3.2.3*~~
- *Certificate-based authentication in accordance with RFC 7030 section 3.3.2 using [**assignment**: pre-existing certificate authorized by the EST server]*

].

Application Note: This SFR with the indicated selection is to be included if EST is implemented by the TOE. EST may be required in CSfC Solutions in the future.

FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1.1 The TSF shall [**selection**: *invoke platform-provided functionality*, *implement functionality*] to validate certificates in accordance with the following rules:

- Certification path validation meets requirements of RFC 5280 for certificate paths of [**selection**: *unlimited path length*, *maximum path length of [**assignment**: number greater than or equal to 0] certificates*] and certificate paths exceeding the maximum path length are invalid.
- The current time is within the notBefore and notAfter values of all certificates in the certification path.
- The certification path shall terminate at a trust anchor element appropriate for the supported function.
- Certificates containing subjectUniqueID or issuerUniqueID fields are considered invalid.
- Certificates are signed using cryptographic signatures and hashes in accordance with RFC 8603, and [**selection**:
    - ~~*[**assignment**: list of supported cryptographic algorithms]*~~
    - *no other algorithms*

  ] and certificates signed using other cryptographic algorithms are considered invalid.
- [**selection**:
    - *CRLs are signed using cryptographic signatures and hashes in accordance with RFC 8603 and [**selection**:*
        - ~~*[**assignment**: list of supported cryptographic algorithms]*~~
        - *no other algorithms*

      ] and CRLs signed using other cryptographic algorithms are considered invalid;
    - *OCSP responses are signed using [**selection**:*

- *sha384WithRSAEncryption with key size of 3072 bits or greater,*
- *ecdsa-with-SHA384 using [**selection**: secp384r1, ~~secp521r1~~],*
- *ecdsa-with-SHA512 using [**selection**: secp384r1, ~~secp521r1~~],] and [**selection**:*
- ~~*[**assignment**: list of other supported algorithms]*~~
- *no other algorithms*

] requested using the preferredSignatureAlgorithm extension and OCSP responses are considered invalid if using other algorithms;

- ~~*no other algorithm constraints*~~

]

FIA_X509_EXT.1.2 The TSF shall [**selection**: *invoke platform-provided functionality*, *implement*] processing of the extensions indicated in RFC 5280, section 4.2,

- Authority Key Identifier,
- Subject Key Identifier
- keyUsage

and [**selection**:

- *basicConstraints*
- *authorityInfoAccess and/or* (See Application Note below)
- *cRLDistributionPoints* (See Application Note below)
- *certificatePolicies*
- *policyMapping*
- *Subject alternate name containing any of the following name types [**selection**:*
  - *rfc822Name*
  - *dNSName*
  - *directoryName*
  - *uniformResourceIdentifier*
  - *IPAddress*
  - *[**assignment**: other name types]*

  ]

- *extendedKeyUsage*
- *nameConstraints*
- *[**assignment**: other extensions]*
- *no other extensions*

].

Application Note: If the TOE supports an applicable certificate revocation status checking mechanism, the TOE must claim and support the applicable extension authorityInformationAccess and/or cRLDistributionPoints based on the X.509 certificate revocation status checking mechanism used (e.g., CRL Distribution Point (CDP), Online Certificate Status Protocol (OCSP)) to comply with the CSfC selections and CP requirements.

FIA_X509_EXT.1.3 The TSF shall [**selection**: *invoke platform-provided functionality*, *implement functionality*] to validate revocation status of the certificate using [**selection**:

- *The Online Certificate Status Protocol (OCSP) as specified in RFC 6960*
- *Certificate Revocation Lists (CRL) as specified in RFC 5280 and refined by RFC 8603*
- ~~*Certificate Revocation Lists as specified in RFC 5280*~~
- ~~*Based on validity period: Certificates expiring within [**assignment**: time less than 24 hours] of the current time are considered valid when no other valid revocation status information is available*~~
- *Administrative notification of revocation: [**assignment**: administrative action upon notification] using [**assignment**: method to invalidate use of certificates in supported functions] when the certificate is revoked.*
- *Direct association with Certification Authority: [**assignment**: direct revocation status information implementations]*

].

Application Note: CRLs, CDPs with CRLs, or OCSP are all acceptable in CSfC solutions.

FIA_X509_EXT.1.4 The TSF shall [**selection**:

- ~~*not obtain revocation status information by the TSF due to [**selection**: determining that the certificate expires within [**assignment**: time less than 24 hours], determining that the [**assignment**: supported function] validates revocation status using [**assignment**: methods supported by the function]]*~~
- *invoke platform-provided functionality*
- *implement functionality*

] to obtain supported revocation status information via [selection:

- *Network connection to [**selection**: ~~CA~~, CRL distribution point, OCSP responder, [~~**assignment**: alternate sources~~]]*
- *Local revocation status information from [**selection**: cached CRL~~, embedded CA repository, local OCSP responder, administrator configuration~~]*
- ~~*An OCSP TLS Status Request Extension (OCSP stapling) as specified in RFC 6066,*~~
- ~~*An OCSP TLS Multiple Certificate Status Request Extension (OCSP multi-stapling) as specified in RFC 6961*~~

]

Application Note: Any of the following X.509 certificate revocation status checking mechanisms, CRL Distribution Point (CDP) and/or Online Certificate Status Protocol (OCSP) are permitted in CSfC solutions. If the TOE uses a cached CRL, the TOE must attempt to download the latest CRL from a CDP at least once every 24 hours to comply with the CSfC selections and CP requirements. See the MA CP, Campus WLAN, and Key Management Requirements Annex for more details.

FIA_X509_EXT.2 X.509 Certificate Support for Functions

FIA_X509_EXT.2.1 The TSF shall [**selection**: *invoke platform-provided functionality to validate, validate*] X.509v3 certificates in accordance with FIA_X509_EXT.1 to support [**assignment**: *supported functions*] using [**selection**:

- *[**selection**: TLS, DTLS, IPsec or IKE, SMIME, SSH, [**assignment**: other authenticated communications protocol]]*
- *[**selection**: code signing for system software updates, code signing for software integrity testing, integrity verification for TSF protected data, administrator authentication, user authentication , [**assignment**: other uses]]*

]

FIA_X509_EXT.2.2 For each function indicated in FIA_X509_EXT.2.1, the TSF shall [**selection**: *invoke the TOE platform to determine, determine*] whether the [**selection**: *administrator is allowed to configure certificate acceptance, supported function determines acceptance via [**assignment**: method of determining acceptance], ~~certificate is accepted~~, certificate is not accepted*] when valid certificate revocation status information cannot be obtained from a source indicated in FIA_X509_EXT.1.3.

Application Note: For CSfC solutions, ingress and egress of Certificate Revocation traffic (e.g., OCSP queries, HTTP GET to CDP) on the Black Interface is prohibited. See the MA CP and Campus WLAN CP for more details.

FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall [**selection**: *invoke the TOE platform to generate, generate*] Certificate Requests as specified by [**selection**:

- *RFC 2986 (PKCS-10)*
- *RFC 7030 as updated by RFC 8996 (EST)*
- *RFC 5272 as updated by RFC 6402 (CMC)*
- *RFC 5272 as updated by RFC 8756 (CNSA CMC)*
- *RFC 4210 as updated by RFC 6712 and RFC 9481 (v2 CMP)*
- *RFC 4210 as updated by RFC 6712 and RFC 9480 (v3 CMP)*

] and be able to provide the following information in the request: public key, [**selection**:

- *Subject DN consisting of values for [**selection**:*
  - *U*
  - *O*
  - *OU*
  - *CN*
  - *[**assignment**: other subject attributes]*

  ]
- *one or more of the following SAN types [**selection**:*
  - *rfc822Name*
  - *dNSName*
  - *directoryName*

    - *uniformResourceIdentifier*
    - *iPAddress*
    - *[**assignment**: other SAN types]*

  ]

] and [**selection**:

- *[**assignment**: list of other certificate field and extension values]*
- *[**assignment**: list of identifying information]*
- *no other information.*

]

Application Note: The supported certificate request mechanisms are claimed in the first selection. PKCS-10 is claimed whether a manual request process is used or if the PKCS-10 request is posted to the certification authority (for embedded CAs or as in ACME implementations). Other options embed the certificate request in a formalized certificate management protocol. If EST is claimed, FIA_ESTC_EXT.1 is also claimed; if CMC or CNSA CMC are claimed, FIA_CMCC_EXT.1 is also claimed; if v2 or v3 CMP is claimed, FIA_CMPC_EXT.1 is also claimed.

Application Note: PKCS-10 must be selected and supported. RFC 7030 as updated by RFC 8996 (EST) and RFC 5272 as updated by RFC 8756 (CNSA CMC) may also be selected and supported.

FIA_XCU_EXT.2 X.509 Certificate Acquisition

FIA_XCU_EXT.2.1 The TSF shall [**selection**:

- *request certificates from an [**selection**: external, embedded] CA,*
- ~~*obtain certificates from an embedded CA*~~

] to represent [**assignment**: *TOE functions*] for [**selection**:

- *[**selection**: TLS, DTLS, IPsec or IKE, SMIME, SSH, [**assignment**: other authenticated communications protocol]]*
- *[**selection**: code signing for system software updates, code signing for software integrity testing, integrity verification for TSF protected data, administrator authentication, user authentication, [**assignment**: other uses]]*

].