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

Overview

Internet Protocol Security (IPsec) Virtual Private Network (VPN) Gateway products (as defined in the Commercial Solutions for Classified (CSfC) Capability Packages (CP)) 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:

- collaborative Protection Profile (PP) for Network Devices Version 4.0; and
- PP-Module for Virtual Private Network (VPN) Gateways Version 2.0; and
- Functional Package for X.509 Version 1.0; and
- If the Target of Evaluation (TOE) use Transport Layer Security (TLS): Functional Package for TLS Version 2.1; and
- If the TOE uses Secure Shell (SSH): Functional Package for SSH Version 2.0

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

IPsec VPN Gateways can be used/implemented in many different ways, threats and technology continuously progress, and IPsec VPN Gateways 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 Gateways 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 Gateway functionality. If needed, functionality and/or configurations outside the scope of CSfC IPsec VPN Gateways that conflict with the CSfC selections could be NIAP validated without using a separate iteration of the Security Functional Requirement (SFR) if the product can be configured to use only the CSfC selections. The Security Target (ST) author should document a specific CSfC IPsec VPN Gateways 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 Gateways Use Cases. The CSfC IPsec VPN Gateways 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 Gateways.

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.1.11 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.1.11.
- 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.

Network Devices Collaborative Protection Profile Version 4.0 Selections

FAU_STG_EXT.1.6 The TSF shall provide the following mechanisms for administrative access to locally stored audit records [*selection: ~~none~~, manual export, ability to view locally*].

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: ~~*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]
FFC-ERB	FFC-ERB - Extra Random Bits	Static domain parameters approved for [selection: • *IKE Groups [selection: ~~MODP-2048,~~ MODP-3072, MODP-4096, MODP-6144, MODP-8192*], • *TLS Groups [selection: ~~ffdhe-2048,~~ 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-2048,~~ MODP-3072, MODP-4096, MODP-6144, MODP-8192*], • *TLS Groups [selection: ~~ffdhe-2048,~~ 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]]

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. As of publication, for CSfC solutions, if FFDHE is selected for HTTPS/TLS, RFC 7919 group ffdhe3072 must be used.

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 Key Generation Algorithm	Cryptographic Algorithm 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: • I*KE Groups [selection: ~~MODP-2048~~, MODP-3072, MODP-4096, MODP-6144, MODP-8192]*, • *TLS Groups [selection: ~~ffdhe2048~~, 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, for CSfC solutions, if FFDHE is selected for IPsec, RFC 3526 MODP-3072 or MODP-4096 must be used. As of publication, for CSfC solutions, if FFDHE is selected for HTTPS/TLS, RFC 7919 group ffdhe3072 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 and Multi-Site Connectivity (MSC) CP for more details.

FCS_COP.1.1/SigGen The TSF shall perform digital signature generation in accordance with ~~a~~ 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 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: $0 \leq sLen \leq hLen$ (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*~~, *P384*, ~~*P-521*~~], per-message secret number generation [selection: *extra random bits*, *rejection sampling*, *deterministic*] and hash function using [selection: ~~*SHA256,*~~ *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 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.

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.1.1/SigVer The TSF shall perform digital signature verification in accordance with ~~*a*~~ 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 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]
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]	RFC 8554 [LMS], NIST SP 800-208 [parameters]
XMSS	Tree height = [selection: *5*, *10*, *15*, *20*, *25*] 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.

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.1.1/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*]

Application Note 19

The HMAC minimum key sizes in the table are specified in ISO/IEC 9797-2:2021, which requires that the minimum key size be equal to the digest size. The FIPS standard specifies no minimum or maximum key sizes, so if FIPS PUB 198-1 is selected, larger or smaller key sizes may be used. This is indicated by the parenthesized annotations in the Cryptographic Key Sizes column.

FCS_COP.1/KeyWrap Cryptographic Operation - Key Wrapping

This is a selection-based SFR, to be included in the ST if “key wrapping” is selected in FCS_CKM.2.1.

FCS_COP.1.1/KeyWrap The TSF shall perform key wrapping 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/KeyWrap.

Identifier	Cryptographic Algorithm	Cryptographic Algorithm Parameters	List of Standards
AES-KW	AES in KW mode	256 bits	[selection: ISO/IEC 18033-3:2010 (Subclause 5.2), FIPS PUB 197] [AES] [selection: ISO/IEC 19772:2020 (clause 6), NIST SP 800-38F (Section 6.2)] [KW mode]
AES-KWP	AES in KWP mode	256 bits	[selection: ISO/IEC 18033-3:2010 (Subclause 5.2), FIPS PUB 197] [AES] NIST SP 800- 38F (Section 6.3) [KWP mode]
~~AES-CCM~~	~~AES in CCM mode with unpredictable, nonrepeating nonce, minimum size of 64 bits~~	~~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]~~

FCS_COP.1/SKC Cryptographic Operation - Symmetric Key Cryptography

This is a selection-based SFR, to be included in the ST if CBC mode, CTR mode, or XTS mode are selected in FCS_COP.1/DataEncryption.

FCS_COP.1.1/SKC The TSF shall perform symmetric-key encryption/decryption 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/SKC.

Identifier	Cryptographic Algorithm	Cryptographic Algorithm Parameters	List of Standards
AES-CBC	AES in CBC mode with non-repeating and unpredictable IVs	[selection: ~~*128,*~~ *256]* bits	[selection: *ISO/IEC 18033-3:2010 (Subclause 5.2), FIPS PUB 197*] [AES] [selection: *ISO/IEC 10116:2017 (Clause 7), NIST SP 800-38A*] [CBC]
AES-CTR	AES in CTR mode with a non-repeating initial counter and with no repeated use of counter values across multiple messages with the same secret key	[selection: ~~*128,*~~ *256]* bits	[selection: *ISO/IEC 18033-3:2010 (Subclause 5.2), FIPS PUB 197*] [AES] [selection: *ISO/IEC 10116:2017 (Clause 10), NIST SP 800- 38A*] [CTR]
XTS-AES	AES in XTS mode with unique tweak values that are consecutive nonnegative integers starting at an arbitrary nonnegative integer	[selection: ~~*256,*~~ *512]* bits	[selection: *ISO/IEC 18033-3:2010 (Subclause 5.2), FIPS PUB 197*] [AES] [selection: *IEEE Std. 1619-2018, NIST SP 800- 38E*] [XTS]

FCS_RBG.1.1 The TSF shall perform deterministic random bit generation services using [selection: *DRBG algorithm*] in accordance with [selection: *list of standards*] after initialization.

The following table provides the allowed choices for completion of the selection operations of FCS_RBG.1.1.

Identifier	DRBG Algorithm	List of Standards
HASH_DRBG	Hash_DRBG with [selection: ~~SHA-256,~~ SHA-384, SHA-512, ~~SHA3-256, SHA3-384, SHA3- 512~~]	[selection: ISO/IEC 18031: 2025 (Section C.2.2), NIST SP 800-90A Revision 1 Section 10.1.1]
HMAC_DRBG	HMAC_DRBG with [selection: ~~SHA-256,~~ SHA-384, SHA-512, ~~SHA3-256, SHA3-384, SHA3- 512~~]	[selection: ISO/IEC 18031: 2025 (Section C.2.3), NIST SP800-90A Revision 1 Section 10.1.2]

CTR_DRBG	CTR_DRBG with [selection: ~~AES-128, AES-192,~~ AES-256]	[selection: ISO/IEC 18031: 2025 (Section C.3.2), NIST SP800-90A Revision 1 Section 10.2.1]

Application Note: For Hash_DRBG and HMAC_DRBG, SHA-384 is permitted, but SHA-512 is preferred and will be required in the future for CSfC solutions.

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

FCS_RBG.2 Random Bit Generation (External Seeding - VS platform)

This component is included if the TOE uses a Virtualization System (VS) for DRBG seeding and "TSF interface for seeding" is selected in FCS_RBG.1.2

FCS_RBG.2.1 The TSF shall be able to accept a minimum input of [assignment: *minimum input length of 256 bits or more*] from a TSF interface for obtaining entropy.

FCS_RBG.3 Random Bit Generation (Internal Seeding - Single Source)

This component is included if "TSF entropy source" is selected in FCS_RBG.1.2

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 [assignment: *256 or more*] bits of min-entropy.

FCS_RBG.4 Random Bit Generation (Internal Seeding - Multiple Sources)
This component is included if "multiple TSF entropy sources" is selected in FCS_RBG.1.2

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

FCS_RBG.5 Random Bit Generation (Combining Entropy Sources)
This component is included if "multiple TSF entropy sources" is selected in FCS_RBG.1.2

FCS_RBG.5.1 The TSF shall [selection: *hash, concatenate and hash, XOR, input into a linear feedback shift register, [assignment: combining operation]*] [selection: *output from TSF entropy source(s), input from TSF interface(s) for obtaining entropy*] resulting in a minimum of [assignment: *256 or more*] bits of min-entropy to create the entropy input into the derivation function as defined in [selection: *ISO/IEC 18031:2011*, *NIST SP 800-90A Revision 1*]

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

a. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers and the following special characters: [selection: *"!"*, *"@"*, *"#"*, *"$"*, *"%"*, "^", *"&"*, "*", *"("*, *")*", [*assignment: other characters*]];

b. Minimum password length shall be *configurable to between [assignment: minimum number of characters supported by the TOE] and [assignment: number of characters greater than or equal to ~~15~~ 112 bits of entropy] characters.*

Application Note: The objective of the CSfC specific language for administrative passwords is to ensure that randomly generated administrative passwords support at least 112 bits of entropy to enable compliance with the CSfC CP and CSfC selections.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- *Ability to administer the TOE remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the remote session inactivity time before session termination;*
- *Ability to update the TOE, and to verify the updates using* digital signature *capability prior to installing those updates;*
- [at least the following underlined selections:
  - *Ability to start and stop services;*
  - *Ability to configure local audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full; changes to local audit storage size);*
  - *Ability to modify the behaviour of the transmission of audit data to an external IT entity;*
  - *Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;*
  - *Ability to manage the cryptographic keys;*
  - *Ability to configure the cryptographic functionality;*
  - *Ability to configure thresholds for SSH rekeying;*
  - *Ability to configure the lifetime for IPsec SAs;*
  - *Ability to configure the list of supported (D)TLS ciphers;*
  - *If applicable due to a Distributed TOE, ability to configure the interaction between TOE components;*
  - *Ability to enable or disable automatic checking for updates or automatic updates;*
  - *Ability to re-enable an Administrator account;*
  - *Ability to set the time which is used for time-stamps;*
  - *Ability to configure NTP;*
  - *Ability to configure the reference identifier for the peer;*
  - *Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;*
  - *Ability to generate Certificate Signing Request (CSR) and process CA certificate response;*

- *Ability to administer the TOE locally;*
- *Ability to configure the local session inactivity time before session termination or locking;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
- *Ability to manage the trusted public keys database;*
- *Ability to manage the public key or certificate used to validate the digital update;*
- *No other capabilities*].

Application Note: The objective of this CSfC Selection is to ensure that only the options listed in this CSfC Selections document are supported/configured/used with IPsec VPN Gateways in CSfC solutions. If the objective of this selection is achieved by other methods (e.g., default and only configuration is compliant with the CSfC selections) and detailed in the product's Administrative Guide, please contact the CSfC Program (csfc_components@nsa.gov) to determine options.

FPT_STM_EXT.1.2 The TSF shall be capable of at least one of the following underlined selections [selection: *allow the Security Administrator to set the time, synchronise time with an NTP server, obtain time from the underlying virtualization system*].

Application Note: If the TSF obtains time from the underlying Virtualization System (VS), the VS must be able to automatically synchronize time to an external time source to meet the CSfC CP requirements and comply with the CSfC selections.

FTP_ITC.1.1 The TSF **shall be capable of using** at least one of the following selections **[selection: *IPsec, SSH as defined in the Functional Package for SSH, TLS as defined in the Functional Package for TLS, ~~DTLS as defined in the Functional Package for TLS~~, HTTPS*] to** provide a **trusted** communication channel between itself and ~~another trusted IT product~~ **authorized IT entities supporting the following capabilities: audit server, [selection: *authentication server, [assignment: other capabilities], no other capabilities***] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from ~~modification or~~ disclosure **and detection of modification of the channel data.**

Application Note: SSH, TLS, and/or IPsec are all acceptable selections for audit server connections in CSfC Solutions.

FTP_TRP.1.1/Admin The TSF shall **be capable of using** at least one of the following **[selection: *IPsec, SSH as defined in the Functional Package for SSH, TLS as defined in the Functional Package for TLS, ~~DTLS as defined in the Functional Package for TLS~~, HTTPS*]** to provide a communication path between itself and authorized remote **Administrators** ~~users~~ that is logically distinct from other communication paths and provides assured identification of its endpoints and protection of the communicated data from disclosure **and provides detection of modification of the channel data**.

Application Note: For CSfC solutions, IPsec VPN Gateways must only be managed over an interface dedicated for management.

FAU_STG.2.1 The TSF shall protect the stored audit data in the audit trail from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to prevent unauthorized modifications to the stored audit data in the audit trail.

FPT_ITT.1.1 If applicable due to a distributed TOE, the TSF shall protect TSF data from disclosure **and detect its modification** when it is transmitted between separate parts of the TOE through **the use of [selection:** ***IPsec, SSH as defined in the Functional Package for SSH, TLS as defined in the Functional Package for TLS, ~~DTLS as defined in the Functional Package for TLS~~, HTTPS*****]**.

FAU_STG_EXT.5.1 If applicable due to a distributed TOE, each TOE component which does not store security audit data locally shall be able to buffer security audit data locally until it has been transferred to another TOE component that stores or forwards it. All transfer of audit records between TOE components shall use a protected channel according to [**Selection:** *FPT_ITT.1, FTP_ITC.1*].

PP-Module for Virtual Private Network (VPN) Gateways Version 2.0 Selections

FCS_COP.1.1/DataEncryption The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES operating in **GCM mode as defined in FCS_COP.1/AEAD** and [selection:

- *CBC mode as defined in FCS_COP.1/SKC,*
- *CTR mode as defined in FCS_COP.1/SKC,*
- *XTS mode as defined in FCS_COP.1/SKC,*
- *CCM mode as defined in FCS_COP.1/AEAD,*
- ***no other modes***

].

FCS_COP.1.1/AEAD The he 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	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 claimed and supported.

FCS_IPSEC_EXT.1.3 The TSF shall implement [selection: *tunnel mode*, *transport mode*].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [

- *IKEv2 as defined in RFC 7296 [**selection**: ~~with no support for NAT traversal~~, with mandatory support for NAT traversal as specified in RFC 7296, Section 2.23], and [RFC 4868 for hash functions]*

]

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [

- *IKEv2 SA lifetimes can be configured by a Security Administrator based on [selection:*
  - *number of bytes;*
  - *length of time, where the time values can be configured between [assignment: minimum configurable rekey time] and [assignment: 24 hours]*

  ]

].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that

- *[IKEv2 Child SA lifetimes can be configured by a Security Administrator based on [selection:*
  - *number of bytes;*
  - *length of time, where the time values can be configured between [assignment: minimum configurable rekey time] and [assignment: 8 hours]*

  ]

].

FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH groups [

- ***20 (384-bit Random ECP) and [selection: ~~21 (521-bit Random ECP, no other groups)~~ according to RFC 5114***

] **and** [

- [***selection****: 15 (3072-bit MODP), 16 (4096-bit MODP), 17 (6144-bit MODP), 18 (8192-bit MODP), no other groups] according to RFC 3526*

].

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.1.13 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: X.509v3 certificate-based peer authentication using RSA and/or ECDSA is required for data plane IKEv2 in CSfC solutions. Pre-shared keys 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/PPK-only authentication is not permitted in CSfC solutions). For CSfC solutions, on the data plane, the TOE must support RFC 8784 PSK but the TOE can be configurable to require RFC 8784 PSK support and/or EAP-TLS support, which would enable the TOE to support different Use Case requirements in CSfC solutions (see the CSfC CP for more details). On the data plane, CSfC IPsec VPN Gateways 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.

FCS_EAP_EXT.1.1 If the TOE uses EAP-TLS in support of VPN Client/Peer authentication, the TSF shall support [**selection**: *EAP-TLS as specified in RFC 5216 and updated by RFC 8996*, ~~*EAP-TTLS as specified in RFC 5281 and updated by RFC 8996*~~] over a protected channel per FTP_ITC.1 **from the Base-PP** with an authentication server.

FIA_PSK_EXT.1 Pre-Shared Key Composition

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec and [selection: *IKEv2*, *multifactor authentication filtering*].

FIA_PSK_EXT.1.2 The TSF shall be able to accept the following as pre-shared keys: [selection: *generated bit-based*, ~~*password-based*~~, *HMAC-based one-time password*, *time-based one-time password*,

combination of a generated bit-based and HMAC-based one-time password, combination of a generated bit-based and time-based one-time password, combination of a password-based and HMAC-based one-time password, combination of a password-based and time-based one-time password] keys.

Application Note: If pre-shared keys that conform to RFC 8784 are selected in FCS_IPSEC_EXT.1.13, FIA_PSK_EXT.1 must be included and an externally generated, bit-based PSK must be used.

FIA_PSK_EXT.2 Generated Pre-Shared Keys

FIA_PSK_EXT.2.1 The TSF shall be able to [selection: *accept externally generated pre-shared keys*, generate [selection: ~~*128*~~, *256*] bit-based pre-shared keys via FCS_RBG.1].

Application Note: For CSfC solutions, externally generated PSKs must be generated by an appropriate RBG.

FAU_GEN.1.1/VPN The TSF shall be able to generate audit data of the following auditable events:

a. Start-up and shutdown of the audit functions
b. All auditable events for the [*not specified*] level of audit;
c. [*Indication that TSF self-test was completed*
d. Failure of self-test
e. auditable events defined in the Auditable Events for Mandatory Requirements table].

Application Note: If permitted by NIAP/CCEVS and feasible for the product, the below additional audit events and details should be included in the ST and Administrative Guide. For CSfC solutions, the below auditing events support compliance with the CSfC Continuous Monitoring Annex (see CSfC CP for more details).

Auditable Events for Mandatory Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FTP_ITC.1/VPN	Initiation of the trusted channel	• IP Address of the non-TOE endpoint of the attempted connection • If available, X.509v3 certificate Subject Distinguished Name and an identifier (e.g., Fingerprint, Issuer and Serial Number) of the non-TOE endpoint of the attempted connection
	Termination of the trusted channel	• IP Address of non-TOE endpoint of the connection
	Failure of the trusted channel functions	• Identification of the initiator and target of failed trusted channel establishment attempt

		• IP Address of the non-TOE endpoint of the attempted connection • If available, X.509v3 certificate Subject Distinguished Name, Issuer, Serial Number, and Fingerprint of the non-TOE endpoint of the attempted connection

Functional Package for Transport Layer Security (TLS) Version 2.1 Selections

FCS_TLS_EXT.1.1 If the TOE uses TLS, the TSF shall implement [**selection**:

- *TLS as a client*
- *TLS as a server*
- ~~*DTLS as a client*~~
- ~~*DTLS as a server*~~

].

Application Note: In 2027, when applicable, new CSfC Components List components will be required to support for ML-KEM-1024 and ML-DSA-87 for TLS Servers and Clients. See the CSfC CP for more details.

FCS_TLSC_EXT.1.1 If the TOE has a TLS Client, the TSF shall implement [**selection**: ~~*TLS 1.2 (RFC 5246)*~~, *TLS 1.3 (RFC 8446)*] as a client that supports additional functionality for session renegotiation protection and [**selection**:

- *mutual authentication*
- *supplemental downgrade protection*
- ~~*session resumption*~~
- ~~*no optional functionality*~~

] and shall abort attempts by a server to negotiate any TLS or SSL version prior to supporting only TLS 1.2 (RFC 5246).

Application Note: The objective of this CSfC Selection is to ensure TLS Clients in CSfC solutions only use TLS 1.3.

FCS_TLSC_EXT.1.2 If the TOE has a TLS Client, the TSF shall be able to support the following [**selection**:

- ~~*TLS 1.2 ciphersuites: [selection:*~~
  - ~~*CNSA 1.0 compliant [selection:*~~

- ~~*TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 and RFC 8422*~~
- ~~*TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 and RFC 8422*~~
- ~~*TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*~~
- ~~*TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*~~
- ~~*TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 and RFC 8422*~~
- ~~*TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 and RFC 8422*~~
- ~~*ciphersuites using pre-shared secrets: [selection:*~~
  - ~~*TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384 as defined in RFC 8442*~~
  - ~~*TLS_DHE_PSK_WITH_AES_256_GCM_SHA384 as defined in RFC 5487*~~
  - ~~*TLS_RSA_PSK_WITH_AES_256_GCM_SHA384 as defined in RFC 5487*~~

  ~~*]*~~

~~*]*~~

- ~~*non-CNSA compliant [selection:*~~
  - ~~*TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246*~~
  - ~~*TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246*~~
  - ~~*TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*~~
  - ~~*TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*~~
  - ~~*TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*~~
  - ~~*TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*~~
  - ~~*TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246*~~
  - ~~*TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246*~~
  - ~~*TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246]*~~
  - ~~*ciphersuites using pre-shared secrets: [selection:*~~
    - ~~*TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256 as defined in RFC 8442*~~
    - ~~*TLS_DHE_PSK_WITH_AES_128_GCM_SHA256 as defined in RFC 5487*~~
    - ~~*TLS_RSA_PSK_WITH_AES_128_GCM_SHA256 as defined in RFC 5487]*~~

    ~~*]*~~

~~*]*~~

] and no other TLS 1.2 ciphersuites,

- *TLS 1.3 ciphersuites [selection:*
  - *CNSA 2.0 compliant TLS_AES_256_GCM_SHA384 as defined in RFC 8446*

~~o non-CNSA compliant [selection:~~
~~▪ TLS_AES_128_GCM_SHA256 as defined in RFC 8446~~
~~▪ [assignment: other TLS 1.3 ciphersuites]~~
]
] and no other TLS 1.3 ciphersuites
] offering the supported ciphersuites in a ClientHello message in preference order: [**assignment**: list of supported ciphersuites].

Application Note: Any additional algorithms listed in accordance with TD1025, must conform to Note 1 above to demonstrate compliance with the CSfC selections.

FCS_TLSC_EXT.1.4 If the TOE has a TLS Client, the TSF shall be able to support the following TLS ClientHello message extensions:

- signature_algorithms extension (RFC 8446) indicating support for CNSA 1.0 compliant [**selection**:
  - *ecdsa_secp384r1_sha384 (RFC 8446)*
  - *rsa_pkcs1_sha384 (RFC 8446)*
-], and [**selection**:
  - *CNSA 1.0 compliant [selection:*
    - *rsa_pss_pss_sha384 (RFC 8446)*
    - *rsa_pss_rsae_sha384 (RFC 8446)*

    ]
  - ~~*[**assignment**: other non-deprecated, non-CNSA compliant signature algorithms]*~~
  - *no other signature algorithms*

  ] and

[**selection**:

- *signature_algorithms_cert extension (RFC 8446) indicating support for CNSA 1.0 compliant [**selection**:*
  - *ecdsa_secp384r1_sha384 (RFC 8446)*
  - *rsa_pkcs1_sha384 (RFC 8446)*

  *], and [**selection**:*
  - *CNSA 1.0-compliant [**selection**:*
    - *rsa_pss_pss_sha384 (RFC 8446)*
    - *rsa_pss_rsae_sha384 (RFC 8446)*

    ]
  - ~~*non-CNSA compliant [**selection**:*~~
    - ~~*rsa_pkcs1_sha256 (RFC 8446)*~~
    - ~~*rsa_pss_rsae_sha256 (RFC 8446)*~~

    ]
  - ~~*[**assignment**: other non-deprecated, non-CNSA compliant signature algorithms]*~~
  - *no other signature algorithms*

] and

- *supported_versions extension (RFC 8446) indicating support for TLS 1.3 and [**selection**: TLS 1.2, no other versions]*
- *supported_groups extension indicating support for [**selection**:*
    - *CNSA 1.0 compliant [**selection**:*
        - *secp384r1 (RFC 8446)*
        - *ffdhe3072 (RFC 7919)*
        - *ffdhe4096 (RFC 7919)*

      ]
    - ~~*non-CNSA compliant [selection:*~~
        - ~~*secp256r1 (RFC 8446)*~~
        - ~~*ffdhe2048 (RFC 7919)*~~

      ]
    - *and [**selection**:*
        - ~~*secp521r1 (RFC 8446)*~~
        - *ffdhe6144(RFC 7919)*
        - *ffdhe8192 (RFC 7919)*
        - *no other supported groups*

      ]

]

- *key_share extension (RFC 8446)*
- *post_handshake_auth (RFC 8446), pre_shared_key (RFC 8446), tls_cert_with_extern_psk (RFC 8773), and psk_key_exchange_modes (RFC 8446) indicating psk_dhe_ke (DHE or ECDHE) mode*
- *extended_master_secret extension (RFC 7627) enforcing server support, and [**selection**: allowing legacy servers, no other enforcement mode]*
- *no other extensions*
-] and shall not send the following extensions:
    - early_data
    - psk_key_exchange_modes indicating PSK only mode.

Application Note:
As of publication, TLS Clients must claim and support the applicable ffdhe3072 and/or ECDHE secp384r1 extensions. See FCS_TLS_EXT.1.1 and FCS_CKM_EXT.7.1 Application Note for more details.

Any additional algorithms listed in accordance with TD1025, must conform to Note 1 above to demonstrate compliance with the CSfC selections

FCS_TLSS_EXT.1.1 If the TOE has a TLS Server, the TSF shall implement [**selection**: ~~*TLS 1.2 (RFC 5246)*~~, *TLS 1.3 (RFC 8446)*] as a server that supports additional functionality for session renegotiation protection and [**selection**:

- *mutual authentication*
- *supplemental downgrade protection*

- ~~*session resumption*~~
- ~~*no optional functionality*~~

] and shall reject connection attempts from clients supporting only TLS 1.1, TLS 1.0, or SSL versions.

Application Note: The objective of this CSfC Selection is to ensure TLS Servers in CSfC solutions only accept TLS 1.3 connections.

FCS_TLSS_EXT.1.2 If the TOE has a TLS Server, the TSF shall be able to support the following [**selection**:

- ~~*TLS 1.2 ciphersuites: [selection:*~~
  - ~~*CNSA 1.0 compliant [selection:*~~
    - ~~*TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in* RFC *5289 and RFC 8422*~~
    - ~~*TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in* RFC *5289 and RFC 8422*~~
    - ~~*TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in* RFC *5288*~~
    - ~~*TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in* RFC *5288*~~
    - ~~*TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 and RFC 8422*~~
    - ~~*TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 and RFC 8422*~~
    - ~~*ciphersuites using pre-shared secrets: [**selection:***~~
      - ~~*TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384 as defined in RFC 8442*~~
      - ~~*TLS_DHE_PSK_WITH_AES_256_GCM_SHA384 as defined in RFC 5487*~~
      - ~~*TLS_RSA_PSK_WITH_AES_256_GCM_SHA384 as defined in RFC 5487*~~

    ~~*]*~~

  ]
- ~~*non-CNSA compliant [**selection:***~~
  - ~~*TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246*~~
  - ~~*TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246*~~
  - ~~*TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*~~
  - ~~*TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*~~
  - ~~*TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*~~
  - ~~*TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*~~
  - ~~*TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246*~~
  - ~~*TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246*~~
  - ~~*TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246]*~~
  - ~~*ciphersuites using pre-shared secrets: [**selection:***~~

- ~~*TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256 as defined in RFC 8442*~~
- ~~*TLS_DHE_PSK_WITH_AES_128_GCM_SHA256 as defined in RFC 5487*~~
- ~~*TLS_RSA_PSK_WITH_AES_128_GCM_SHA256 as defined in RFC 5487]*~~

~~*]*~~

~~*]*~~

] and no other TLS 1.2 ciphersuites,

- *TLS 1.3 ciphersuites [**selection**:*
  - *CNSA 2.0 compliant TLS_AES_256_GCM_SHA384 as defined in RFC 8446*
  - ~~*non-CNSA compliant [**selection**:*~~
    - ~~*TLS_AES_128_GCM_SHA256 as defined in RFC 8446*~~
    - ~~*[**assignment**: other TLS 1.3 ciphersuites]*~~

  ~~*]*~~

] and no other TLS 1.3 ciphersuites

] using a preference order based on [**selection**: ~~*RFC 9151 priority*~~, *ClientHello ordering, [**assignment**: additional priority]*].

Application Note: Any additional algorithms listed in accordance with TD1025, must conform to Note 1 above to demonstrate compliance with the CSfC selections.

FCS_TLSS_EXT.1.4 If the TOE has a TLS Server, the TSF shall be able to process the following TLS ClientHello message extensions:

- signature_algorithms extension (RFC 8446) indicating support for CNSA 1.0 compliant [**selection**:
  - *ecdsa_secp384r1_sha384 (RFC 8446)*
  - *rsa_pkcs1_sha384 (RFC 8446)*

  ], and [**selection**:
  - *CNSA 1.0 compliant [**selection**:*
    - *rsa_pss_pss_sha384 (RFC 8446)*
    - *rsa_pss_rsae_sha384 (RFC 8446)*

    ]
  - ~~*[**assignment**: other non-deprecated, non-CNSA compliant signature algorithms]*~~
  - *no other signature algorithms*

  ], and

[**selection**:

- *signature_algorithms_cert extension (RFC 8446) indicating support for CNSA 1.0 compliant [**selection**:*
  - *ecdsa_secp384r1_sha384 (RFC 8446)*
  - *rsa_pkcs1_sha384 (RFC 8446)*

  *], and [**selection**:*

- *CNSA 1.0-compliant [**selection**:*
  - *rsa_pss_pss_sha384 (RFC 8446)*
  - *rsa_pss_rsae_sha384 (RFC 8446)*

  ]
- ~~*non-CNSA compliant [**selection:***~~
  - ~~*rsa_pkcs1_sha256 (RFC 8446)*~~
  - ~~*rsa_pss_rsae_sha256 (RFC 8446)*~~

  ~~*]*~~
- ~~*[**assignment**: other non-deprecated, non-CNSA compliant signature algorithms]*~~
- *no other signature algorithms*

]

- *supported_versions extension (RFC 8446) indicating support for TLS 1.3 and [**selection**: TLS 1.2, no other versions]*
- *supported_groups extension indicating support for [**selection**:*
  - *CNSA 1.0 compliant [selection:*
    - *secp384r1 (RFC 8446)*
    - *ffdhe3072 (RFC 7919)*
    - *ffdhe4096 (RFC 7919)*

    ]
  - ~~*non-CNSA compliant [**selection:***~~
    - ~~*secp256r1 (RFC 8446)*~~
    - ~~*ffdhe2048 (RFC 7919)*~~

    ~~*]*~~
  - *and [**selection**:*
    - ~~*secp521r1 (RFC 8446)*~~
    - *ffdhe6144(RFC 7919)*
    - *ffdhe8192 (RFC 7919)*
    - *no other supported groups*

    ]

  ]
- *key_share extension (RFC 8446)*
- *post_handshake_auth (RFC 8446), pre_shared_key (RFC 8446), tls_cert_with_extern_psk (RFC 8773), and psk_key_exchange_modes (RFC 8446) indicating psk_dhe_ke (DHE or ECDHE) mode*
- *extended_master_secret extension (RFC 7627) enforcing server support, and [**selection**: allowing legacy clients, no other enforcement mode]*
- *no other extensions*

].

Application Note:
As of publication, TLS Servers must claim and support the applicable ffdhe3072 and/or ECDHE secp384r1 extensions. See CSfC Selections for

FCS_CKM_EXT.7.1 for more details. See FCS_TLS_EXT.1.1 and FCS_CKM_EXT.7.1 Application Note for details on ML-KEM-1024 and ML-DSA-87 support.

Any additional algorithms listed in accordance with TD1025, must conform to Note 1 above to demonstrate compliance with the CSfC selections.

FCS_TLSS_EXT.1.5 If the TOE has a TLS Server, the TSF shall perform key establishment for TLS using [**selection**:

- ~~*RSA with [selection:*~~
  - ~~*CNSA 1.0 compliant size [selection: 3072, 4096]*~~
  - ~~*non-CNSA compliant size 2048*~~

] bits and no other sizes

- *[**selection**:*
  - *CNSA 1.0 compliant Diffie-Hellman groups [**selection**: ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192]*
  - ~~*non-CNSA compliant Diffie-Hellman group ffdhe2048*~~

*] and no other groups, consistent with the client's supported_groups extension and [**selection**: key_share extension, no other] extension*

- *ECDHE parameters using [**selection**:*
  - *CNSA 1.0 compliant elliptic curves [**selection**: secp384r1, ~~secp521r1~~]*
  - ~~*non-CNSA compliant elliptic curve secp256r1*~~

*] and no other curves, consistent with the client's supported_groups extension and [**selection**: key_share extension, no other] extension and using non-compressed formatting for points*

].

Application Note: As of publication, TLS Servers must claim and support the applicable ffdhe3072 and/or ECDHE secp384r1 extensions. See FCS_TLS_EXT.1.1 and FCS_CKM_EXT.7.1 Application Note for more details.

Any additional algorithms listed in accordance with TD1025 must conform to Note 1 above to demonstrate compliance with the CSfC selections.

FCS_TLSS_EXT.2.3 If the TOE has a TLS Server and supports TLS mutual authentication, the TSF shall be able to reject the establishment of a trusted channel if the requested client certificate is invalid and [**selection**:

- ~~*continue establishment of a server-only authenticated TLS channel in accordance with FCS_TLSS_EXT.1 in support of [selection: all applications, [assignment: list of calling applications that accept both authenticated and unauthenticated client sessions]] when an empty certificate message is provided by the client*~~
- *continue establishment of a mutually authenticated TLS channel when revocation status information for the [**selection**:*
  - ~~*client's leaf certificate*~~
  - ~~*[assignment: specific intermediate CA certificates]*~~

- *any non-trust store certificate in the certificate chain*

*] is not available in support of [**selection**:*

- ~~*all supported functions*~~
- *[**assignment**: list of calling supported functions configurable to perform certificate status information bypass processing]*

*] as [**selection**:*

- *configured by an administrator*
- ~~*confirmed by the supported function user*~~
- ~~*a TLS-specific default for [assignment: subset of supported functions]*~~

~~*]*~~

- *no other processing options for missing or invalid client certificates*

].

Application Note: If TLS mutual authentication is used, CSfC solutions must reject missing or invalid client certificates. The only CSfC-selected exception is administrator-configured continuation of a mutually authenticated TLS channel when revocation status information is unavailable for configured non-trust-store certificates in the client certificate chain. Server-only fallback for an empty client certificate, supported-function-user confirmation, and TLS-specific default bypass processing are not selected. If the TOE does not support administrator-configured revocation-status bypass processing, only select "no other processing options for missing or invalid client certificates". TLS mutual authentication support is preferred but not required on the management plane in CSfC solutions.

FCS_TLSS_EXT.4.1 If the TOE has a TLS Server, the TSF shall support secure TLS renegotiation through the use of [**selection**: *the "renegotiation_info" TLS extension in accordance with RFC 5746, not allowing session renegotiation*].

FCS_TLSS_EXT.4.2 If the TOE has a TLS Server, the TSF shall [**selection**: *indicate support for renegotiating a TLS 1.2 session by including the renegotiation_info extension in the ServerHello message when a ClientHello with the renegotiation_info extension is received and shall terminate a session if neither of the renegotiation_info or TLS_EMPTY_RENEGOTIATION_INFO_SCSV signaling ciphersuites are indicated in the client hello, not allow renegotiation*].

Functional Package for X.509 Version 1.0 Selections

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 Enrollment over Secure Transport (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.1.1 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*
- *authorityInformationAccess* 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: 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 at least one of the following underlined selections [**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]*

].

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]]*~~
- *[**selection**: 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: The TOE must claim and support one of the following X.509 certificate revocation status checking mechanisms, CRL Distribution Point (CDP) and/or Online Certificate Status Protocol (OCSP) to comply with the CSfC selections and CP requirements. 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.

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: The objective of this CSfC Selection is to ensure that only IPsec communication with mutual authentication of IPsec VPN clients using X.509v3 certificates is permitted/supported/used on the data plane interface between IPsec VPN Gateway and IPsec VPN Clients in CSfC solutions.

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.2.1 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]]*

].

Functional Package for Secure Shell (SSH) Version 2.0 Selections

FCS_SSH_EXT.1

If the TOE uses SSH, the auditable events specified in this Package are included in an ST if the incorporating PP, cPP, or PP-Module supports audit event reporting through FAU_GEN.1, and if all other criteria in the incorporating PP or PP-Module are met.

Requirement	Auditable Events	Additional Audit Record Contents
FCS_SSH_EXT.1	**[**selection**:** *Failure to establish SSH connection*, ~~*None*~~**]**	**[**selection**:** *Reason for failure and non-TOE endpoint of attempted connection (IP Address)*, ~~*No additional information*~~**]**
	[selection**:** *Establishment of SSH connection*, ~~*None*~~**]**	**[**selection**:** *Non-TOE endpoint of connection (IP Address)*, ~~*No additional information*~~**]**
	[selection**:** *Termination of SSH connection session*, ~~*None*~~**]**	**[**selection**:** *Non-TOE endpoint of connection (IP Address)*, ~~*No additional information*~~**]**
	[selection: *Dropping of packets outside defined size limits, None***]**	**[selection:** *Packet size, No additional information***]**

FCS_SSH_EXT.1.1
If the TOE uses SSH, the TOE shall implement SSH acting as a [**selection**: *client*, *server*] that complies with RFCs 4251, 4252, 4253, 4254, [**selection**: *4256*, ~~*4344*~~, *5647*, *5656*, *6187*, *6668*, *8268*, *8308*, *8332*, ~~*no other RFCs*~~*] and [no other standard*].

FCS_SSH_EXT.1.2
If the TOE uses SSH, the TSF shall ensure that the SSH protocol implementation supports the following authentication methods: [**selection**:

- *password, complying with [**selection**: RFC 4252, RFC 4256 keyboard-interactive methods]*
- *publickey" (RFC 4252): [**selection**:*
    - o *rsa-sha2-512 (RFC 8332)*
    - o *ecdsa-sha2-nistp384 (RFC 5656)*
    - o ~~*ecdsa-sha2-nistp521 (RFC 5656)*~~
    - o *x509v3-ecdsa-sha2-nistp384 (RFC 6187)*
    - o ~~*x509v3-ecdsa-sha2-nistp521 (RFC 6187)*~~

  ]

] and no other methods.

FCS_SSH_EXT.1.4
If the TOE uses SSH, the TSF shall protect data in transit from unauthorised disclosure using the following mechanisms: [**selection**:

- *AEAD_AES_256_GCM (RFC 5647)*
- *aes256-gcm@openssh.com (RFC 5647)*

] and no other mechanisms.

FCS_SSH_EXT.1.5
If the TOE uses SSH, the TSF shall protect data in transit from modification, deletion, and insertion using: [**selection**:

- *AEAD_AES_256_GCM (RFC 5647)*
- *implicit*

] and no other mechanisms.

FCS_SSH_EXT.1.6

If the TOE uses SSH, the TSF shall stablish a shared secret with its peer using: [**selection**:

- *diffie-hellman-group15-sha512 (RFC 8268)*
- *diffie-hellman-group16-sha512 (RFC 8268)*
- ~~*diffie-hellman-group17-sha512 (RFC 8268)*~~
- ~~*diffie-hellman-group18-sha512 (RFC 8268)*~~
- *ecdh-sha2-nistp384 (RFC 5656)*
- ~~*ecdh-sha2-nistp521 (RFC 5656)*~~

] and no other mechanisms.

FCS_SSHC_EXT.1.1

If the TOE has an SSH client, the TSF shall authenticate its peer (SSH server) using: [**selection**:

- *a local database by associating each host name with a public key corresponding to the following list: [**selection**:*
  - *rsa-sha2-512 (RFC 8332)*
  - *ecdsa-sha2-nistp384 (RFC 5656)*
  - ~~*ecdsa-sha2-nistp521 (RFC 5656)*~~

  ]
- *a list of trusted certification authorities when the public key is in the following formats: [**selection**:*
  - *x509v3-ecdsa-sha2-nistp384 (RFC 6187)*
  - ~~*x509v3-ecdsa-sha2-nistp521 (RFC 6187)*~~

  ]

] as described in RFC 4251, Section 4.1.

FCS_SSHS_EXT.1.1

If the TOE has an SSH server, the TSF shall authenticate itself to its peer (SSH client) using: [**selection**:

- *rsa-sha2-512 (RFC 8332)*
- *ecdsa-sha2-nistp384 (RFC 5656)*
- ~~*ecdsa-sha2-nistp521 (RFC 5656)*~~
- *x509v3-ecdsa-sha2-nistp384 (RFC 6187)*
- ~~*x509v3-ecdsa-sha2-nistp521 (RFC 6187)*~~

]