# Commercial Solutions for Classified (CSfC) Selections for Operating Systems

## Overview

Operating System (OS) 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:

- Protection Profile (PP) for General Purpose Operating Systems (GPOS PP), Version 5.0;
- Functional Package for X.509 Version 1.0;
- If the Target of Evaluation (TOE) uses Transport Layer Security (TLS): Functional Package for Transport Layer Security (TLS) Version 2.1;
- If the TOE uses Secure Shell (SSH): Functional Package for SSH Version 2.0;
- If the TOE includes a built-in Mobile Device Management (MDM) Agent: PP-Module for Mobile Device Management Agent, version 1.0; and
- If the TOE includes a built-in Internet Protocol Security (IPsec) Virtual Private Network (VPN) Client: CSfC selections for IPsec VPN Client

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

OS can be used/implemented in many different ways, threats and technology continuously progress, and OS continue to evolve, which may cause the below selections to change or become obsolete. Manufacturers/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 OS 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 OS functionality. If needed, functionality and/or configurations outside the scope of a CSfC OS 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 OS configuration in the product's Administrative Guide with a note that the configuration should be considered the NIAP-certified evaluated configuration for CSfC OS Use Cases. The CSfC OS 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 Operating System.

**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:

- If TLS is used, in FCS_CKM.1.1/AKG, selecting RSA 3072 would also require selecting ffdhe-3072 or Elliptic Curve P-384 to enable compliance with the selections for FCS_CKM_EXT.7.1.
- In FCS_CKM.1.1/AKG, either one or more selections for Elliptic Curve/Finite Field Diffie-Hellman are required based on the selections in FCS_TLSC_EXT.1 and/or 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 for General Purpose Operating System v5.0 Selections

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

a. Start-up and shut-down of the audit functions;
b. All auditable events for the [not specified] level of audit;
c. Specifically defined auditable events listed in Table 2
   [
d.
   - *Authentication events (Success/Failure);*

- *Use of privileged/special rights events (Successful and unsuccessful security, audit, and configuration changes);*
- *Privilege or role escalation events (Success/Failure);*
- *[**selection**:*
  - *Auditable events as defined in the Functional Package for Secure Shell (SSH), version 2.0*
  - *Auditable events as defined in the Functional Package for Transport Layer Security (TLS), version 2.1*
  - *Auditable events as defined in the Functional Package for X.509, version 1.0*
  - *File and object events (Successful and unsuccessful attempts to create, access, delete, modify, modify permissions)*
  - *User and Group management events (Successful and unsuccessful add, delete, modify, disable, enable, and credential change)*
  - *Audit and log data access events (Success/Failure)*
  - *Cryptographic verification of software (Success/Failure)*
  - *Attempted application invocation with arguments (Success/Failure e.g., due to software restriction policy)*
  - *System reboot, restart, and shutdown events (Success/Failure)*
  - *Kernel module loading and unloading events (Success/Failure)*
  - *Administrator or root-level access events (Success/Failure)*
  - *[**assignment**: other specifically defined auditable events].*

*]*

].

**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:<br>• *IKE Groups [**selection**: MODP-3072, MODP-4096, MODP-6144, MODP-8192*],<br>• *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:<br>• *IKE Groups [**selection**: MODP-3072, MODP-4096, MODP-6144, MODP-8192*],<br>• *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]*] |
| 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_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]<br>[**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]<br>[**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 TLS, IPsec, and/or SSH.

**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] |
| 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 TLS and/or 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**:<br>• *192 bits with [**selection**: SHA-256/192, SHAKE256/192]*<br>• *256 bits with [**selection**: SHA-256, SHAKE256]*<br>]<br>Winternitz parameter = [selection: 1, 2, 4, 8]<br>Tree height = [**selection**: *5*, *10*, *15*, *20*, *25*] | RFC 8554 [LMS], NIST SP 800-208 [parameters] |
| XMSS | XMSS private key size [**selection**:<br>• *192 bits with [**selection**: SHA-256/192, SHAKE256/192]*<br>• *256 bits with [**selection**: SHA-256, SHAKE256]]*<br>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.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 RBG functionality.

**FIA_AFL.1.1** The TSF shall detect when [**selection**:

- ***[assignment**: ~~positive integer number~~ **Selection:** [3, 10] See Application Note below]*
- *an administrator configurable positive integer within [**assignment**: ~~range of acceptable values~~ 1 – 10 See Application Note]*

] unsuccessful authentication attempts occur related to the below applicable underlined **events with** [**selection**:

- *authentication based on user name and password*
- ***authentication based on user name and a PIN that releases an asymmetric key stored in OE-protected storage***
- *authentication based on X.509 certificates*
- ***authentication based on biometric in accordance with the Biometric Enrollment and Verification, version 2.0***
- ***hybrid***

].

**Application Note:** As of publication, for CSfC solutions, the OS must implement at least one of the following: 1) a wipe of all protected data after 10 or less authentication failures or 2) lock the account after three consecutive authentication failures where Administrator intervention is required to unlock.

**FIA_AFL.1.2** When the defined number of unsuccessful authentication attempts **for an account** has been [met], The TSF shall implement at least one of the following underlined to align with the CSfC Application Note for FIA_AFL.1.1: [**selection**: ***Account Lockout, Account Disablement**, **Mandatory Credential Reset**, **Wipe Sensitive Data**, **[assignment: list of actions]***].

**FIA_UAU.5 Multiple Authentication Mechanisms**

**FIA_UAU.5.1** The **OS** shall provide **[selection:**

- ***authentication based on username and password***
- ***authentication based on username and a PIN that releases an asymmetric key stored in OE-protected storage***
- ***combination of authentication based on user name, password, and time-based one-time password***
- ***authentication based on X.509 certificates***
- ***for use in SSH only, SSH public key-based authentication as specified by the Functional Package for Secure Shell (SSH), version 2.0***

**]** and [**selection**: ~~*biometric in accordance with the Biometric Enrollment and Verification, version 2.0, hybrid*~~, *no other mechanism*] to support user authentication.

**FMT_SMF_EXT.1 Specification of Management Functions**

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

**Table 11: Management Functions**

Status Markers:
M - Mandatory
O - Optional/Objective

**Application Note:** For any function in the below table where M is required for Administrator (as defined in the PP Application Note for FMT_MOF.1.1), all CSfC selections must be met for at least one Use Case (e.g., Administrator, Administrator (When managed with an MDM), and/or Administrator Only (When managed with an MDM)). The Use Case and how to achieve compliance with the CSfC selections must be documented in the Administrative Guide.

| # | Management Function | User | Administrator | Administrator (When managed with an MDM) | Administrator Only (When managed with an MDM) |
|---|---|---|---|---|---|
| 1 | Configure password policy:<br>• minimum password length<br>• minimum password complexity<br>• maximum password lifetime | O | M | M | M |
| 2 | Configure screen/session locking policy:<br>• enable/disable [**selection**: *screen* | O | M | M | M |

| | | | | | |
|---|---|---|---|---|---|
| | *lock*, *session*] inactivity timeout<br>• [**selection**: *screen lock*, *session*] inactivity timeout value<br>• number of authentication failures to trigger lockout | | | | |
| 3 | Enable/disable the VPN protection:<br>• Across device<br>[**selection**:<br>• *on a per-app basis*<br>• *on a per-group of applications processes basis*<br>• *no other method*<br>] | O | ~~O~~M | M | O |
| 4 | Enable/disable [**assignment**: *list of all radios*] | O | ~~O~~M | M | O |
| 5 | Enable/disable [**assignment**: *list of audio or visual collection devices*]:<br>• Across device<br>[**selection**:<br>• *on a per-app basis*<br>• *on a per-group of applications processes basis*<br>• *no other method*<br>] | O | O | M | O |
| 6 | Transition to the locked state | O | O | M | O |
| 7 | If wipe of data is supported, TSF wipe of sensitive data | O | ~~O~~M | M | O |

| | | | | | |
|---|---|---|---|---|---|
| 8 | Configure application installation policy by<br><br>[**selection**:<br><br>• *restricting the sources of applications*<br>• *specifying a set of allowed applications based on [**assignment**: application characteristics] (an application allowlist)*<br>• *denying installation of applications*<br><br>] | O | ~~O~~M | M | M |
| 9 | Import keys or secrets into the secure key storage | O | ~~O~~M | M | O |
| 10 | Destroy imported keys or secrets and [**selection**: *no other keys or secrets, [**assignment**: list of other categories of keys or secrets]*] in the secure key storage | O | O | M | O |
| 11 | Import X.509v3 certificates into the Trust Anchor Database | O | ~~O~~M | M | O |
| 12 | Remove imported X.509v3 certificates and [**selection**: *no other X.509v3 certificates, [**assignment**: list of other categories of X.509v3 certificates]*] in the Trust Anchor Database | O | ~~O~~M | M | O |
| 13 | Enroll the TOE in management | O | ~~O~~M | M | O |
| 14 | Remove applications | O | ~~O~~M | M | O |
| 15 | Update system software | O | ~~O~~M | M | O |
| 16 | Install applications | O | ~~O~~M | M | O |
| 17 | Remove Enterprise applications | O | ~~O~~M | M | O |
| 18 | Enable/disable display notification in the locked state of: [**selection**: | O | ~~O~~M | M | O |

- ~~*email notifications*~~
- ~~*calendar appointments*~~
- ~~*contact associated with phone call notification*~~
- ~~*text message notification*~~
- ~~*[assignment: other application-based notifications]*~~
- *all notifications*

]

| | | | | | |
|---|---|---|---|---|---|
| 19 | Enable sensitive data protection | O | O | M | O |
| 20 | Enable removable media's sensitive data protection | O | O | M | O |
| 21 | Enable/disable location services:<br>• Across device<br>[**selection**:<br>• *on a per-app basis*<br>• *on a per-group of applications processes basis*<br>• *no other method*<br>] | O | ~~O~~M | M | O |
| 22 | Enable/disable the use of `all applicable` [**selection**: *Biometric Authentication Factor*, *Hybrid Authentication Factor*] | O | ~~O~~M | O | O |
| 23 | Configure whether to allow or disallow establishment of [**assignment**: *configurable trusted channel in FTP_ITC_EXT.1.1 or FDP_UPC_EXT.1.1/APPS*] if the peer or server certificate is deemed invalid. | O | ~~O~~M | O | O |
| 24 | Enable/disable all data signaling over `all applicable` [**assignment**: *list of externally accessible hardware ports*] | O | ~~O~~M | O | O |

| | | | | | |
|---|---|---|---|---|---|
| 25 | Enable/disable `all` [**assignment**: *list of protocols where the device acts as a server*] | O | ~~O~~M | O | O |
| 26 | Enable/disable developer modes | O | ~~O~~M | O | O |
| 27 | Enable/disable bypass of local user authentication | O | ~~O~~M | O | O |
| 28 | Wipe Enterprise data | O | O | O | O |
| 29 | Approve [**selection**: *import*, *removal*] by applications of X.509v3 certificates in the Trust Anchor Database | O | ~~O~~M | O | O |
| 30 | Configure whether to allow or disallow establishment of a trusted channel if the TSF cannot establish a connection to determine the validity of a certificate | O | ~~O~~M | O | O |
| 31 | Enable/disable the cellular protocols used to connect to cellular network base stations | O | ~~O~~M | O | O |
| 32 | Read audit logs kept by the TSF | O | O | O | O |
| 33 | Configure [**selection**: *certificate*, *public-key*] used to validate digital signature on applications | O | ~~O~~M | O | O |
| 34 | Approve exceptions for shared use of keys or secrets by multiple applications | O | O | O | O |
| 35 | Approve exceptions for destruction of keys or secrets by applications that did not import the key or secret | O | O | O | O |
| 36 | Configure the unlock banner | O | O | M | M |
| 37 | Configure the auditable items | O | ~~O~~M | O | O |
| 38 | Retrieve TSF-software integrity verification values | O | O | O | O |
| 39 | Enable/disable `all applicable` [**selection**: | O | ~~O~~M | O | O |

| | | | | | |
|---|---|---|---|---|---|
| | • *USB mass storage mode*<br>• *USB data transfer without user authentication*<br>• *USB data transfer without authentication of the connecting system*<br><br>] | | | | |
| 40 | Enable/disable backup of [**selection**: *all applications*, *selected applications*, *selected groups of applications*, *configuration data*] to [**selection**: *locally connected system*, *remote system*] | O | O | O | O |
| 41 | Enable/disable `all applicable` [**selection**:<br><br>• *Hotspot functionality authenticated by [**selection**: pre-shared key, passcode, no authentication]*<br>• *USB tethering authenticated by [**selection**: pre-shared key, passcode, no authentication]*<br><br>] | O | ~~O~~ *M* | O | O |
| 42 | Approve exceptions for sharing data between [**selection**: *applications*, *groups of applications*] | O | O | O | O |
| 43 | Place applications into application groups based on [**assignment**: *enterprise configuration settings*] | O | O | O | O |
| 44 | Unenroll the TOE from management | O | ~~O~~ *M* | O | O |
| 45 | Enable/disable the Always On VPN protection:<br><br>• Across device | O | ~~O~~ *M* | O | O |

| | | | | | |
|---|---|---|---|---|---|
| | [**selection**:<br>• *on a per-app basis*<br>• *on a per-group of applications processes basis*<br>• *no other method*<br>] | | | | |
| 46 | Revoke Biometric template | O | O | O | O |
| 47 | Configure local audit storage capacity | O | ~~O~~M | O | O |
| 48 | Configure lockout policy for unsuccessful authentication attempts through [**selection**: *timeouts between attempts, limiting number of attempts during a time period*] | O | ~~O~~M | O | O |
| 49 | Configure host-based firewall | O | ~~O~~M | O | O |
| 50 | Configure name/address of directory server with which to bind | O | ~~O~~M | O | O |
| 51 | Configure name/address of audit/logging server to which to send audit/logging records | O | ~~O~~M | O | O |
| 52 | Configure name/address of network time server | O | ~~O~~M | O | O |
| 53 | Enable/disable automatic software update | O | ~~O~~M | O | O |
| 54 | [**assignment**: *list of other management functions to be provided by the TSF*] | O | O | O | O |

**FTP_ITC_EXT.1.1** The TSF shall use [**selection**:

- *TLS as conforming to the Functional Package for Transport Layer Security (TLS), version 2.1 as a [**selection**: client, ~~server~~]*
- ~~*DTLS as conforming to the Functional Package for Transport Layer Security (TLS), version 2.1 as a [selection: client, server]*~~
- *IPsec as conforming to the PP-Module for Virtual Private Network (VPN) Clients, version 3.0*

] and [**selection**:

- *SSH as conforming to the Functional Package for Secure Shell (SSH), version 2.0 as a [**selection**: client, ~~server~~]*
- *Mutually authenticated TLS in accordance with the [Functional Package for Transport Layer Security (TLS), version 2.1] as a [**selection**: client, ~~server~~]*
- ~~*Mutually authenticated DTLS in accordance with the [Functional Package for Transport Layer Security (TLS), version 2.1] as a [selection: client, server]*~~
- *HTTPS*
- *no other protocols*

] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: [**selection**: *audit server, authentication server, management server, [assignment: other capabilities]*] using [**selection**: *certificates as defined in Functional Package for X.509, version 1.0, SSH host keys as defined in Functional Package for Secure Shell (SSH), version 2.0*] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

**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** |
|---|---|---|---|
| ~~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**:<br>• I*KE Groups [selection: MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192],*<br>• *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:** The CSfC selections for this SFR apply to all applicable protocols. As of publication, for CSfC solutions, if FFDHE is selected for HTTPS/TLS, RFC 7919 group ffdhe3072 must be used. 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 CSfC CP for more details.

**FCS_CKM_EXT.8.1** If the TOE uses/claims password-based key derivation functions, the TSF shall perform password-based key derivation functions in accordance with a specified cryptographic algorithm [*HMAC-[**selection**: ~~SHA-256~~, SHA-384, SHA-512*], with iteration count of [***assignment**: number of iterations*] using a randomly generated salt of length [***assignment**: equal to or greater than 128*] and output cryptographic key sizes [***selection**: 256, 384, 512*] bits that meet the following standard: [*NIST SP 800-132 (Section 5.3) [PBKDF2]*].

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

If the TOE uses TLS, the auditable events in the table below are included in a Security Target if both the associated requirement is included and the incorporating PP or PP-Module supports audit event reporting through FAU_GEN.1 and any other criteria in the incorporating PP or PP-Module are met.

**Table 2: Auditable Events for Selection-based Requirements**

| Requirement | Auditable Event | Additional Audit Record Contents |
|---|---|---|
| FCS_TLSC_EXT.1 | [**selection, choose one of**: *Failure to establish a TLS session*, ~~*none*~~] | [**selection, choose one of**: *Reason for failure and non-TOE endpoint of attempted connection (IP Address)*, ~~*None*~~] |
| | [**selection, choose one of**: *Failure to verify presented identifier*, ~~*none*~~] | [**selection, choose one of**: *Presented identifier and reference identifier*, ~~*None*~~] |
| | [**selection, choose one of**: *Establishment and termination of a TLS session*, ~~*none*~~] | [**selection, choose one of**: *Non-TOE endpoint of connection*, ~~*None*~~] |

**Application Note:** Table 2 is only required if the TOE uses TLS/has a TLS Client.

**FCS_TLS_EXT.1 TLS Protocol**

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 Clients. See the Mobile Access (MA) CP for more details.

**FCS_TLSC_EXT.1 TLS Client Protocol**

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

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 TLS 1.2 (RFC 5246).

**Application Note:** If the TOE includes a built-in MDM Agent that uses TLS, TLS 1.3 mutual authentication is required to be claimed in the ST and supported. For other Use Cases, TLS 1.3 mutual authentication is encouraged but not required. 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 and no other TLS 1.3 ciphersuites*
  - ~~*non-CNSA compliant [**selection:***~~
    - ~~*TLS_AES_128_GCM_SHA256 as defined in RFC 8446*~~
    - ~~*[**assignment:** 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**:
    - o *ecdsa_secp384r1_sha384 (RFC 8446)*
    - o *rsa_pkcs1_sha384 (RFC 8446)*

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

      *]*
    - ~~o *[assignment: other non-deprecated, non-CNSA compliant signature algorithms]*~~

  ] and 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]*~~

  *] and 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 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.

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

### FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

FCS_TLSC_EXT.2.1 If the TOE includes a built-in MDM Agent that uses TLS, the TSF shall support mutual TLS authentication using X.509v3 certificates during the handshake and [**selection**: ~~*in support of post-handshake authentication requests*~~, *at no other time*], in accordance with [**selection**: ~~*RFC 5246, Section 7.4.4*~~, *RFC 8446, Section 4.3.2*].

### FCS_TLSC_EXT.4 TLS Client Support for Renegotiation

FCS_TLSC_EXT.4.1 If the TOE has a TLS Client, the TSF shall support secure TLS renegotiation through use of [**selection**:

- ~~*the "renegotiation_info" TLS extension*~~

- ~~*the TLS_EMPTY_RENEGOTIATION_INFO_SCSV signaling ciphersuite signaling value in accordance with RFC 5746*~~
- *rejection of all renegotiation attempts*

] and shall terminate the session if an unexpected ServerHello is received or [**selection**: *hello request message is received, in no other case*].

# 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* `(if MDM-Agent and/or IPsec VPN Client)`] 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.

`Application Note: If the TOE includes a built-in MDM Agent and/or IPsec VPN Client, the TOE must be able to request a certificate from an external CA and support/claim mutual X.509v3 certificate based authentication for the applicable protocol (e.g., IKEv2/IPsec for an IPsec VPN Client). For other Use Cases, the ability to request a certificate from an external CA is encouraged but not required.`

**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 at least one of the following underlined protocols [**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 If the TOE includes a built-in MDM Agent or IPsec VPN Client, 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 (if MDM-Agent), DTLS, IPsec or IKE (If IPsec Client), 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]]*

].

**Application Note:** If the TOE includes a built-in MDM Agent and/or IPsec VPN Client, the TOE must be able to request a certificate from an external CA and support/claim mutual X.509v3 certificate based authentication for the applicable protocol (e.g., IKEv2/IPsec for an IPsec VPN Client). For other Use Cases, the ability to request a certificate from an external CA and mutual authentication is encouraged but not required.

## 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**:*
    - *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)*~~

  *]*

] 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)*~~

]