CSfC Selections for End User Device/Mobile Platform

End User Device/Mobile Platform products used in CSfC solutions shall be validated by NIAP/CCEVS or CCRA partnering schemes as complying with the current requirements of:

NIAP's Protection Profile (PP) for Mobile Device Fundamentals (MDF) version 3.1

or

NIAP's Protection Profile for General Purpose Operating Systems (GP OS PP) and GP OS PP /MDF PP Extended Package (EP) Wireless Local Area Network (WLAN) Clients and the CSfC Selections for Software/Hardware Full Drive Encryption (SW/HW-FDE) and optionally the PP-Module for Virtual Private Network (VPN) Client.

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

CSfC selections for Mobile Device Fundamentals (MDF) version 3.1 evaluations:
All requirements and associated actions listed in Table 9: High-Security Template (Appendix F, Use Case 2 of the MDF PP v3.1)

or

CSfC selections for General Purpose Operating Systems (GP OS PP) version 4.2 evaluations:

FCS_CKM.1.1 The OS shall generate asymmetric cryptographic keys in accordance with at least one of the following specified cryptographic key generation algorithm [selection:

- RSA schemes using cryptographic key sizes of 2048-bit [and 3072-bit] or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3,
- ECC schemes using "NIST curves" P-256, P-384 and [selection: P-521, no other curves] that meet the following: FIPS-PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4,

Note: if ECC schemes are selected in FCS_CKM.1.1., make the following selections:

- FCS_CKM.2.1 in accordance with a specified cryptographic key establishment method: … and [selection: **Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography**"]
- FCS_TLSC_EXT.2.1 The OS shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [selection: **secp384r1**].

FCS_COP.1.1(1) The OS shall perform encryption/decryption services for data … and cryptographic key sizes [selection: **256-bit**]

FCS_COP.1.1(2) The OS shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1 and [selection: **SHA-384**]

FCS_COP.1.1(3) The OS shall perform cryptographic signature services (generation and verification) in accordance with at least one of the following specified cryptographic algorithm [selection:

- RSA schemes using cryptographic key sizes of 2048-bit [and 3072-bit] or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 4,

- ECDSA schemes using "NIST curves" P-256, P-384 and [selection: P-521, no other curves] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5

FCS_RBG_EXT.1.2 The deterministic RBG used by the OS shall be seeded by an entropy source that accumulates entropy from a [selection:

- software-based noise source,
- platform-based noise source]

with a minimum of [selection: **256 bits**] of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

FCS_TLSC_EXT.1.1 The OS shall implement TLS 1.2 (RFC 5246) supporting at least one of the following cipher suites: [selection:

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289].

FDP_IFC_EXT.1.1 The OS shall support at least one of the following [selection:

- provide an interface which allows a VPN client to protect all IP traffic using IPsec,
- provide a VPN client which can protects all IP traffic using IPsec]

Note: If the VPN client is provided, the CSfC selections for IPsec VPN Client must for also be met.

CSfC selections for GP OS PP/MDF PP Extended Package (EP) Wireless Local Area Network (WLAN) Clients version 1.0 evaluations:

FCS_TLSC_EXT.1.1/WLAN The TSF shall implement TLS 1.0 and [selection: **TLS 1.2 (RFC 5246)**] in support of the EAP-TLS protocol as specified in RFC 5216 supporting at least one of the following ciphersuites:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5430
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

CSfC selections for Software/Hardware Full Drive Encryption (SW/HW-FDE)

Available at:

https://www.nsa.gov/resources/everyone/csfc/components-list/assets/files/selections/sw-fde.pdf

Optional: CSfC selections for IPsec VPN Client

Available at:

https://www.nsa.gov/resources/everyone/csfc/components-list/assets/files/selections/vpn-clients.pdf

Last Updated: October 17, 2018