CSfC Selections for Software Full Drive Encryption (SW-FDE) and Hardware Full Drive Encryption (HW-FDE)

Software Full Disk Encryption and Hardware Full Disk Encryption products used in CSfC solutions shall be validated by NIAP/CCEVS or CCRA partnering schemes as complying with the current requirements of NIAP’s collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition (FDE AA) and the collaborative Protection Profile for Full Drive Encryption – Encryption Engine (FDE EE). This validated compliance shall include the selectable requirements contained in this document.

CSfC selections for FDE AA CPP evaluations:

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [selection:
- One, using a submask as the BEV;
- Intermediate keys originating from one or more submask(s) to the BEV using the following method(s): [selection:
  - key derivation as specified in FCS_KDF_EXT.1,
  - key wrapping as specified in FCS_COP.1(d),
  - key combination as specified in FCS_SMC_EXT.1,
  - key transport as specified in FCS_COP.1(e),
  - key encryption as specified in FCS_COP.1(g)]

FCS_COP.1.1(a) Refinement: The TSF shall perform [cryptographic signature services (verification)] in accordance with at least one of the following: [selection:
- RSA Digital Signature Algorithm with a key size (modulus) of [selection: 3072-bits or greater],
- Elliptic Curve Digital Signature Algorithm with a key size of 256 bits or greater
That meet the following: [selection:
- FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1-v1 5;ISO/IEC 9796-2, Digital signature scheme 2 or digital signature scheme 3, for RSA schemes
- FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST curves” [selection: P-384]; ISO/IEC 14888-3, Section 6.4, for ECDSA schemes


FCS_COP.1.1(g) Refinement: The TSF shall perform [key encryption and decryption] in accordance with a specified cryptographic algorithm [AES used in [selection: CBC, GCM] mode] and cryptographic key sizes
that meet the following: [AES as specified in ISO /IEC 18033-3, [selection: CBC as specified in ISO/IEC 10116, GCM as specified in ISO/IEC 19772]].

**CSfC selections for FDE EE cPP evaluations:**

FCS_KYC_EXT.2.2 The TSF shall maintain a chain of intermediary keys originating from the BEV to DEK using the following method(s): [selection:

- asymmetric key generation as specified in FCS_CKM.1(a),
- symmetric key generation as specified in FCS_CKM.1(b),
- key derivation as specified in FCS_KDF_EXT.1,
- key wrapping as specified in FCS_COP.1(d),
- key combination as specified in FCS_SMC_EXT.1,
- key transport as specified in FCS_COP.1(e),
- key encryption as specified in FCS_COP.1(g)]

FCS_COP.1.1(a) Refinement: The TSF shall perform [cryptographic signature services (verification)] in accordance with at least one of the following: [selection:

- RSA Digital Signature Algorithm with a key size (modulus) of [selection: 3072-bits or greater],
- Elliptic Curve Digital Signature Algorithm with a key size of 256 bits or greater
That meet the following: [selection:

- FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1-v1 5;ISO/IEC 9796-2, Digital signature scheme 2 or digital signature scheme 3, for RSA schemes
- FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST curves” [selection: P-384]; ISO/IEC 14888-3, Section 6.4, for ECDSA schemes


FCS_COP.1.1(g) Refinement: The TSF shall perform [key encryption and decryption] in accordance with a specified cryptographic algorithm [AES used in [selection: CBC, GCM] mode] and cryptographic key sizes [selection: 256 bits] that meet the following: [AES as specified in ISO /IEC 18033-3, [selection: CBC as specified in ISO/IEC 10116, GCM as specified in ISO/IEC 19772]].