CSfC Selections for Certificate Authorities

Certificate Authorities 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 for Certificate Authorities Version 2.0 (CA PP). This validated compliance shall include the selectable requirements contained in this document.

CSfC selections for Certificate Authority evaluations:

FCS_CKM.1.1(1) The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with at least one of the following:

- NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 (as defined in FIPS PUB 186-4, "Digital Signature Standard")
- NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes

  and specified cryptographic key sizes [assignment: equivalent to, or greater than, a symmetric key strength of 128 bits]

FCS_CKM.1.1(2) The TSP shall generate asymmetric cryptographic keys used for authentication in accordance with at least one of the following cryptographic key generation algorithms:

- FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3 and for RSA schemes
- FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4 for ECDSA schemes and implementing "NIST curves" P-256, P-384

  and specified cryptographic key sizes [assignment: equivalent to, or greater than, a symmetric key strength of 128 bits]

FCS_COP.1.1(1) The TSF shall perform [encryption and decryption] in accordance with the following specified cryptographic algorithm:

- AES-CBC (as defined in NIST SP 800-38) mode,
- AES-GCM (as defined in NIST SP 800-38D) mode,

  and cryptographic key size [256-bit].

FCS_COP.1.1(2) The TSF shall perform [cryptographic signature services] in accordance with at least one of the following specified cryptographic algorithms

- RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of [3072 bits or greater] that meets FIPS-PUB 186-4, "Digital Signature Standards",
- Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 or greater that meets FIPS PUB 186-4, "Digital Signature Standard" with "NIST curves" P-256, P384 (as defined in FIPS PUB 186-4, "Digital Signature Standard"),

FCS_COP.1.1(3) The TSF shall perform [cryptographic hashing services] in accordance with a specified cryptographic algorithm [SHA-384] and message digest sizes [384] bits that meet the following: [FIPS Pub 180-4, “Secure Hashing Standard”].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [selection: a software-based noise source, TSF hardware-based noise source] with a minimum of [256 bits] of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and authorization factors that it will generate.