CSfC Selections for Session Border Controller

Session Border Controller products used in CSfC solutions shall be validated by NIAP/CCEVS or CCRA partnering schemes as complying with the current requirements of NIAP's Network Device collaborative Protection Profile (NDcPP) version 2.0 and NDcPP Extended Package Session Border Controller NDcPP EP SBC version 1.1. This validated compliance shall include the selectable requirements contained in this document.

CSfC selections for NDcPP evaluations:

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

- RSA schemes using cryptographic key sizes of **3072-bit** or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;
- ECC schemes using "NIST curves" [selection: **P384**] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;

FCS_CKM.2.1 The TSF shall perform cryptographic key establishment in accordance with at least one of the following specified cryptographic key establishment method(s): [selection:

- RSA-based key establishment schemes that meet the following: NIST Special Publication 800-56B Revision 1, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography";
- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";

FCS_COP.1.1/Data Encryption The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm [assignment: **AES** used in [selection: **GCM**] mode and cryptographic key sizes [assignment: **256 bits**] that meet the following: [assignment: **AES as specified in ISO 18033-3,** [selection: **GCM as specified in ISO 19772**].

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

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [assignment: **3072 bits** or greater].
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [assignment: **256 bits** or greater]
  ]
  that meet the following: [selection:
- For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,
- For ECDSA 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
  ]

FCS_COP.1.1/Hash The TSF shall perform cryptographic hashing services in accordance with a specific cryptographic algorithm [selection: **SHA-384**] and message digest sizes [selection: **384**] bits that meet the following: [assignment ISO/IEC 10118-3:2004].

FCS_COP.1.1/KeyedHash The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [selection: **HMAC-SHA-1**] and cryptographic key sizes [assignment: key size (in bit) used in HMAC] and message digest sizes [selection: 160, 256, 384, 512] bits that meet the following: [assignment: ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: [assignment: number of software-based sources] software-based noise source, [assignment: number of hardware-based sources] hardware-based noise source] with a minimum of [selection: **256 bits**] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

FTP_ITC.1.1 The TSF shall be capable of using at least one of the following [selection: **IPsec, SSH, TLS**] to provide a trusted communication channel between itself and 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 disclosure and detection of modification of the channel data.

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

CSfC selections for NDcPP EP SBC evaluations:

FCS_SRTP_EXT.1.2 The TSF shall implement SDES-SRTP supporting at least one of the following ciphersuites [selection:

- AES_256_CM_HMAC_SHA1_80, in accordance with RFC 6188,
- AES_256_CM_HMAC_SHA1_32, in accordance with RFC 6188,
- AEAD_AES_256_GCM, in accordance with RFC 7714]