CSfC Selections for VoIP Applications

VoIP Application 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 for Voice Over IP (VoIP) Applications, and this validated compliance shall include the selectable requirements contained in this document.

CSfC selections for VoIP Application evaluations:

FCS_CKM.1.1(1) **Refinement:** The [selection, choose at least one of: VoIP client application, client device platform] shall generate **asymmetric** cryptographic keys **used for key establishment in** accordance with:

- 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 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard").

FCS_CKM.1.1(2) **Refinement:** The [selection, choose at least one of: VoIP client application, client device platform] shall generate **asymmetric** cryptographic keys **used for authentication** in accordance with a specified cryptographic key generation algorithm:

- FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4 for ECDSA schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves]

FCS_COP.1.1 **Refinement:** The [selection, choose at least one of: VoIP client application, client device platform] shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *AES operating in* **CTR, CBC, GCM** *(as defined in NIST SP800-38D), [selection: [assignment: one or more modes], no other modes]]* and cryptographic key sizes 128-bits, 256-bits and *[selection: 192 bits, no other key sizes]* that meets the following:

- *FIPS PUB 197, "Advanced Encryption Standard (AES)"*
- *NIST SP 800-38A, NIST SP 800-38D*

FCS_COP.1.1(2) **Refinement:** The [selection, choose at least one of: VoIP client application, client device platform] shall perform **cryptographic signature services (generation and verification)** in accordance with a specified cryptographic algorithm:

- ***FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4 for Elliptic Curve Digital Signature Algorithm (ECDSA) schemes and implementing "NIST curves" P-256, P-384, and [selection: P-521, no other curves]***

FCS_COP.1.1(3) **Refinement:** The [selection, choose at least one of: VoIP client application, client device platform] shall perform **cryptographic hashing** in accordance with a specified cryptographic

algorithm SHA-1, SHA-256, SHA-384, and [selection: SHA-512, no other algorithms] and **message digest sizes** 160, 256, 384 bits and [selection: 512 bits, no other message digest sizes] that meet the following: *FIPS PUB 180-3, "Secure Hash 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, a platform-based RBG*] 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 hashes that it will generate.

FCS_TLS_EXT.1.1 The [selection, choose at least one of: VoIP client application, client device platform] shall implement one or more of the following protocols [TLS 1.2 (RFC 5246)] using mutual authentication with certificates and supporting the following ciphersuites:

- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*