CSfC Selections for File Encryption Applications

File Encryption software 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 Application Software (ASPP) as well as the ASPP Extended Package: File Encryption. This validated compliance shall include the selectable requirements contained in this document.

CSfC selections for ASPP evaluations:

FCS_RBG_EXT.2.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from a platform-based DRBG and [selection: a software-based noise source, no other 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 hashes that it will generate.

FCS_COP.1.1(1)
The application shall perform encryption/decryption in accordance with a specified cryptographic algorithm

- AES-CBC (as defined in NIST SP 800-38A) mode;

and [**selection**:

AES-GCM (as defined in NIST SP 800-38D),
no other modes

] and cryptographic key sizes 128-bit key sizes and [*256-bit key sizes*] .

CSfC selections for ASPP Extended Package: File Encryption evaluations:

FCS_CKM_EXT.2.1 The TSF shall generate FEK cryptographic keys
[selection:

using a Random Bit Generator as specified in FCS_RBG_EXT.1 *(from the AS PP)* and with entropy corresponding to the security strength of AES key sizes of [256 bit];

conditioned from a password/passphrase as defined in FCS_CKM.1(A)
]

FCS_COP.1.1(1) **Refinement:** The application shall [selection: implement platform-provided AES encryption, implement AES encryption] shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in**
[selection:
CBC (as defined in NIST SP 800-38A);
XTS (as defined in NIST SP 800-38E)]
mode and cryptographic key sizes[256 bits].

FCS_CKM.1.1(A) **Refinement:** A password/passphrase used to generate a password authorization factor shall enable up to [assignment: *positive integer of 64 or more*] characters in the set of {upper case characters, lower case characters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")", and [assignment: *other supported special characters*] and shall perform [**Password-based Key Derivation Functions**] in accordance with a specified cryptographic algorithm [**HMAC-[selection: SHA-256, SHA-384, SHA-512]**], with [assignment: *positive integer of 4096 or more*] iterations, and output cryptographic key sizes [256] that meet the following: [**NIST SP 800-132**].

FCS_CKM_EXT.1.2 All KEKs shall be [256-bit] keys corresponding to at least the security strength of the keys encrypted by the KEK.