Mapping Between

collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, 01-February-2019

and

NIST SP 800-53 Revision 5

Important Caveats

- **Product vs. System.** The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 1, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 5, CNSSI № 1253) are used for the assessment and authorization of mission systems. **Products cannot satisfy controls outside of the system context**. Products may support a system satisfying particular controls, but typically satisfaction also requires the implementation of operational procedures; further, given that systems are typically the product of integration of multiple products configured to meet mission requirements, an overall system assessment is required to determine if the control is satisfied in the overall system context.
- **SA-4(7).** Perhaps it is needless to say, but satisfaction of any NIAP PP supports system satisfaction of SA-4(7), which is the implementation of CNSSP № 11.
- **SC-28/SC-28(1).** The cPP as a whole supports SC-28 and SC-28(1) by acting as a mechanism to encrypt stored data at rest. Note that many of the SFRs in this PP are low-level in nature. Although they may technically contribute to many controls, the most significant impact overall is the support of SC-28 and SC-28(1) by compliant products as a whole.
- **System context of supported controls.** For a conformant TOE to support these controls in the context of an information system, the selections and assignments completed in the TOE's Security Target must be congruent with those made for the supported controls. For example, the TOE's ability to perform self-testing only supports SI-6 to the extent that performing self-tests at initial startup (as defined by FPT_TST_EXT.1.1) is consistent with the verification conditions assigned by part (b) of the control. The security control assessor must compare the TOE's functional claims to the behavior required for the system to determine the extent to which the applicable controls are supported. In general, the various ancillary security functions that a conformant TOE includes are subordinate to the primary use case of the TOE, which is to ensure that SC-28 and SC-28(1) are enforced to secure data at rest through encryption of the data stored on the organizational asset on which the TOE is deployed.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
Mandatory Requirements				
FCS_CKM.1(c)	**Cryptographic Key Generation (Data Encryption Key)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE provides a key generation function in support of the key lifecycle process.
		SC-12(2)	**Cryptographic Key Establishment and Management:** Symmetric Keys	The TOE will implement the key generation function using symmetric keys.
FCS_CKM.4(a)	**Cryptographic Key Destruction (Power Management)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the enforcement of this control by ensuring the destruction of stored cryptographic data, either through the TSF or through reliance on the operational environment.
FCS_CKM_EXT.4(a)	**Cryptographic Key and Key Material Destruction (Destruction Timing)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to destroy keys when appropriate in order to conform to organizational policy and standards.
FCS_CKM_EXT.4(b)	**Cryptographic Key and Key Material Destruction (Power Management)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to destroy keys when appropriate in order to conform to organizational policy and standards.
FCS_CKM_EXT.6	**Cryptographic Key Destruction Types**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will perform key destruction using an appropriate method.
FCS_KYC_EXT.2	**Key Chaining (Recipient)**	SC-12	**Cryptographic Key Establishment and Management**	The ability of a conformant TOE to maintain a key chain satisfies the key access portion of this control.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE will ensure that its cryptographic keys are protected at rest using an appropriate method.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FCS_SNI_EXT.1	**Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE's use of salts, nonces, and/or IVs as needed ensures that generated cryptographic keys have sufficient strength.
FCS_VAL_EXT.1	**Validation**	AC-3	**Access Enforcement**	A conformant TOE will ensure that encrypted data at rest is not decrypted unless a valid authorization factor is provided.
FDP_DSK_EXT.1	**Protection of Data on Disk**	SC-28	**Protection of Information at Rest**	The primary purpose of the TOE is to ensure that data at rest is protected against unauthorized access.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A conformant TOE will encrypt data at rest using AES.
FMT_SMF.1	**Specification of Management Functions**	CM-6	**Configuration Settings**	A conformant TOE may satisfy one or more optional capabilities defined in this SFR. In general, a conformant TOE will satisfy this control to the extent that the TOE provides a method to configure its behavior in accordance with organizational requirements. Specific additional controls may be supported depending on the functionality claimed by the TOE.
FPT_KYP_EXT.1	**Protection of Key and Key Material**	IA-5	**Authenticator Management**	A conformant TOE has the ability to protect key data that may be used an authenticator, satisfying part (g) of the control.
		IA-5(7)	**Authenticator Management:** No Embedded Unencrypted Static Authenticators	A conformant TOE ensures that key data (including authenticators for file system access and any keys that can be used to derive them) are not placed in

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				unencrypted static locations.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will ensure that secret key and keying material data are not stored in plaintext except in specific cases where appropriate.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE will ensure that its cryptographic keys are protected at rest using an appropriate method.
FPT_PWR_EXT.1	**Power Saving States**	N/A	N/A	While the TOE will perform cryptographic operations to secure data at rest when certain power state transitions occur, this SFR only pertains to the definition of the power states themselves and therefore does not address any security controls on its own.
FPT_PWR_EXT.2	**Timing of Power Saving States**	N/A	N/A	While the TOE will perform cryptographic operations to secure data at rest when certain power state transitions occur, this SFR only pertains to when power state transitions occur and therefore does not address any security controls on its own.
FPT_TST_EXT.1	**TSF Testing**	SI-6	**Security and Privacy Function Verification**	A conformant TOE will run automatic tests to ensure correct operation of its own functionality.
FPT_TUD_EXT.1	**Trusted Update**	CM-14	**Signed Components**	A conformant TOE has the ability to require a signed update by the manufacturer prior to installing those updates. Note that this may be a signed update or an authenticated firmware update mechanism, which also uses a digital signature.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE has the ability to verify the integrity of updates to it.
Optional Requirements				
FPT_FAC_EXT.1	**Firmware Access Control**	AC-3	**Access Enforcement**	A conformant TOE will not permit application of a firmware update unless proper authorization is provided.
		AC-6(1)	**Least Privilege:** Authorize Access to Security Functions	A conformant TOE will enforce least privilege on the firmware update function.
		AC-11	**Re-Authentication**	A conformant TOE prompts for authentication when a firmware update is initiated, which enforces this control in the case of the "when the execution of privileged functions occurs" clause.
FPT_RBP_EXT.1	**Rollback Protection**	SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE ensures that the integrity of the TSF is maintained by preventing firmware rollbacks to potentially insecure versions.
FCS_CKM.4(e)	**Cryptographic Key Destruction (Key Cryptographic Erase)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to destroy encrypted keys through destruction of a key encryption key.
Selection-Based Requirements				
FCS_CKM.1(a)	**Cryptographic Key Generation (Asymmetric Keys)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE provides a key generation function in support of the key lifecycle process.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	The TOE will implement the key generation function using asymmetric keys.
FCS_CKM.1(b)	**Cryptographic Key Generation (Symmetric Keys)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE provides a key generation function in support of the key lifecycle process.
		SC-12(2)	**Cryptographic Key Establishment and Management:** Symmetric Keys	The TOE will implement the key generation function using symmetric keys.
FCS_CKM.4(b)	**Cryptographic Key Destruction (TOE-Controlled Hardware)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys.
FCS_CKM.4(c)	**Cryptographic Key Destruction (General Hardware)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys.
FCS_CKM.4(d)	**Cryptographic Key Destruction (Software TOE, 3rd Party Storage)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys.
FCS_COP.1(a)	**Cryptographic Operation (Signature Verification)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform signature verification using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(b)	**Cryptographic Operation (Hash Algorithm)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform hashing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(c)	**Cryptographic Operation (Message Authentication)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform keyed-hash message authentication using NSA-approved and FIPS-validated algorithms.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FCS_COP.1(d)	**Cryptographic Operation (Key Wrapping)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform key wrapping using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(e)	**Cryptographic Operation (Key Transport)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform key transport using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(f)	**Cryptographic Operation (AES Data Encryption / Decryption)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform AES encryption and decryption using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(g)	**Cryptographic Operation (Key Encryption)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform key encryption-using NSA-approved and FIPS-validated algorithms.
FCS_KDF_EXT.1	**Cryptographic Key Derivation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to derive keys in support of the key lifecycle process.
FCS_RBG_EXT.1	**Random Bit Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE's use of an appropriate DRBG ensures that generated keys provide an appropriate level of security.
FCS_SMC_EXT.1	**Submask Combining**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to perform submask combining in support of key generation functions.
FPT_FUA_EXT.1	**Firmware Update Authentication**	CM-14	**Signed Components**	A conformant TOE has the ability to require a signed update.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	The TOE has the ability to verify the integrity of updates to itself.