Mapping Between
Protection Profile Module for File Encryption, Version 1.0, 25 July 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 2, 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-Module supports system satisfaction of SA-4(7), which is the implementation of CNSSP № 11.
- **SA-28.** Independent of any individual SFRs, the primary purpose of this TOE is to support the enforcement of SA-28 and SA-28(1) by facilitating the cryptographic protection of data at rest.
- **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 protect data at rest only supports SC-28(1) to the extent that any sensitive data that is encrypted as per FDP_DAR_EXT.1 is included in the set of "organization-defined information at rest" assigned by that 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 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_EXT.2	**File Encryption Key (FEK) Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely generate or import keys.
FCS_CKM_EXT.4	**Cryptographic Key Destruction**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy keys.
FCS_IV_EXT.1	**Initialization Vector Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE's use of IVs as needed ensures that cryptographic keys are generated appropriately.
FCS_KYC_EXT.1	**Key Chaining and Key Storage**	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.
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.
		AC-14	**Permitted Actions without Identification or Authorization**	A conformant TOE will ensure that data cannot be decrypted without presentation of a valid authorization factor.
FDP_PRT_EXT.1	**Protection of Selected User Data**	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.
FDP_PRT_EXT.2	**Destruction of Plaintext Data**	SC-4	**Information in Shared System Resources**	A conformant TOE ensures that ephemeral storage of decrypted sensitive data cannot be used as a mechanism to disclose that data to an unintended recipient.
FIA_AUT_EXT.1	**Subject Authorization**	IA-2	**Identification and Authentication**	A conformant TOE implements or relies on one or more methods of

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
			(Organizational Users)	authorizing users based on validation of an authorization factor.
FMT_SMF.1(2)	**Specification of File Encryption 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 Keys 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.
		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.
Optional Requirements				
FCS_CKM_EXT.5	**File Authentication Key (FAK) Support**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will ensure that any FAKs are generated and protected in an appropriate manner.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE will ensure that any FAKs 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_COP_EXT.1	**FAK Encryption/Decryption Support**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will ensure that FAKs are not stored in plaintext.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE supports this control by virtue of the fact that the control requires protected storage for cryptographic keys. This SFR requires the TOE to implement a cryptographic method to protect the confidentiality of stored keys, or to implement key derivation such that keys are not stored at all and this control is satisfied by default.
FDP_AUT_EXT.1	**Authentication of Selected User Data**	SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE implements a method to verify data integrity through data authentication.
FDP_AUT_EXT.2	**Data Authentication Using cryptographic Keyed-Hash Functions**	SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE uses cryptographic mechanisms to validate data integrity through data authentication.
FDP_AUT_EXT.3	**Data Authentication Using Asymmetric Signing and Verification**	SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE uses cryptographic mechanisms to validate data integrity through data authentication.
FDP_PM_EXT.1	**Protection of Data in Power Managed States**	AC-3	**Access Enforcement**	A conformant TOE will ensure that encrypted data at rest is not decrypted unless a valid authorization factor is provided.
		SC-4	**Information in Shared System Resources**	A conformant TOE ensures that plaintext sensitive data is destroyed on a power state transition so that this cannot be used as a mechanism to disclose that

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				data to an unintended recipient.
		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. This includes ensuring that engaging a power state or lock state transition on the TOE platform cannot be used as a way to prevent the engaging of these protection mechanisms.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A conformant TOE will encrypt data at rest using AES.
FDP_PRT_EXT.3	**Protection of Third-Party Data**	SC-28	**Protection of Information at Rest**	A conformant TOE will enforce its data at rest protection mechanisms against temporary files.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A conformant TOE will encrypt data at rest using AES.
FIA_FCT_EXT.1	**Multi-User Authorization**	SC-4	**Information in Shared System Resources**	A conformant TOE will ensure that user-specific data is protected at the user level so that multiple users on the same system cannot access data that does not belong to them.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will ensure that user-specific data at rest is protected such that only the authorized user may access it.
		SC-28	**Protection of Information at Rest**	A conformant TOE will protect data at rest using unique keys for individual users.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A conformant TOE will encrypt data at rest using AES.
		SC-50	**Software-Enforced Separation and Policy Enforcement**	A conformant TOE will enforce domain separation by ensuring that a multi-user system protects data in such a manner that only the authorized user for that particular data may access it.
FIA_FCT_EXT.2	**Authorized Key Sharing**	AC-3	**Access Enforcement**	A conformant TOE has a mechanism that allows a user to grant another user access to their protected data.
Selection-Based Requirements				
FCS_CKM_EXT.3	**Key Encrypting Key (KEK) Support**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely generate or import keys.
FCS_CKM_EXT.6	**Cryptographic Password/Passphrase Conditioning**	IA-5	**Authenticator Management**	A conformant TOE requires passwords to meet specific length and composition restrictions, which may address part (h) of the control depending on what the organization's requirements for password complexity rules are.
		SC-13	**Cryptographic Protection**	A conformant TOE will condition password data using a NIST-approved method.
		SC-28	**Protection of Information at Rest**	A conformant TOE uses salts to increase password complexity.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A conformant TOE uses key derivation rather than persistent storage to maintain password data.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control**		**Comments and Observations**
FCS_COP.1(5)	**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(6)	**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(7)	**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 Function**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform key derivation using NSA-approved and FIPS-validated algorithms.
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.
FCS_VAL_EXT.2	**Validation Remediation**	AC-7	**Unsuccessful Logon Attempts**	A conformant TOE performs some protective action if a user has a sufficiently large number of consecutive failed authorization attempts due to presenting an invalid authorization factor.
Objective Requirements				
This PP-Module has no objective requirements.				