Mapping Between

Protection Profile Module for File Encryption Enterprise Management, Version 1.0, 30 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 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 various organizational assets that the TOE is capable of managing.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
Modified Requirements				
FTP_DIT_EXT.1	**Protection of Data in Transit**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE supports the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The use of the protocols specified in the SFR ensures the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
Mandatory Requirements				
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_COP.1(5)	**Cryptographic Operation (Key Wrapping)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform key transport 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 encryption 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 transport using NSA-approved and FIPS-validated algorithms.
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_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.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
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_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.1(1)	**Validation (Server Administrator)**	AC-3	**Access Enforcement**	A conformant TOE will ensure that access to management functions is not granted unless a valid authorization factor is provided.
		AC-14	**Permitted Actions without Identification or Authorization**	A conformant TOE will ensure that management functions cannot be accessed without presentation of a valid authorization factor.
FCS_VAL_EXT.1(2)	**Validation (User)**	AC-3	**Access Enforcement**	A conformant TOE will ensure that access to user key material is not granted unless a valid authorization factor is provided.
		AC-14	**Permitted Actions without Identification or Authorization**	A conformant TOE will ensure that user key material cannot be accessed without presentation of a valid authorization factor.
FCS_VAL_EXT.2(2)	**Validation Remediation (User)**	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.
FIA_AUT_EXT.1	**Subject Authorization**	IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE implements or relies on one or more methods of authorizing users based on validation of an authorization factor.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FIA_REC_EXT.1	**Recovery Support**	N/A	**N/A**	NIST SP 800-53 revision 5 does not define any controls that relate specifically to the use of recovery credentials.
FIA_UAU.1	**Timing of Authentication**	AC-14	**Permitted Actions without Identification or Authorization**	A conformant TOE will ensure that management functions cannot be accessed without presentation of a valid authorization factor.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE has the ability to require that certain functions require successful authentication to access.
FIA_UID.1	**Timing of Identification**	AC-14	**Permitted Actions without Identification or Authorization**	A conformant TOE will ensure that management functions cannot be accessed without presentation of a valid authorization factor.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE has the ability to require that certain functions require successful authentication to access.
FMT_MOF.1	**Server Management of Security Functions Behavior**	AC-3	**Access Enforcement**	A conformant TOE will not permit configuration of cryptographic functionality unless proper authorization is provided.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE will restrict access to management functionality to members of a certain role.
		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting the users that are able to configure cryptographic functionality.
		AC-6(1)	**Least Privilege:** Authorize Access to Security Functions	A conformant TOE associates authorizations to use its security functions

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				with users who belong to authorized roles.
FMT_MTD.1	**Management of TSF Data**	AC-3	**Access Enforcement**	A conformant TOE will not permit manipulation of its stored data unless proper authorization is provided.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE will restrict access to management functionality to members of a certain role.
		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting the users that are able to manage TSF data.
		AC-6(1)	**Least Privilege:** Authorize Access to Security Functions	A conformant TOE associates authorizations to use its security functions with users who belong to authorized roles.
FMT_SMF.1(2)	**Specification of Management Functions (Management Server)**	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.
FMT_SMR.2	**Restrictions on Security Roles**	AC-2(7)	**Account Management:** Privileged User Accounts	A conformant TOE has the ability to associate users with roles, in support of part (a) of the control.
FPT_ITT.1	**Basic Internal TSF Data Transfer Protection**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE will support this control by providing a protected communication channel between remote

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				distributed TOE components.
		SC-8(1)	**Transmission Confidentiality and Integrity**: Cryptographic Protection	A conformant TOE will use cryptographic methods to protect data in transit between different parts of 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.
FPT_KYP_EXT.2	**Attribution of Key and Key Material**	AC-16(4)	**Security and Privacy Attributes:** Association of Attributes by Authorized Individuals	A conformant TOE associates key chains with individual users and potentially other attributes such as a specific device that the protected key can be used for. This is defined administratively or as part of a user-initiated registration process.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE will have the ability to prevent unauthorized disclosure of information and detect modification to that information.
Optional Requirements				
This PP-Module has no optional requirements.				
Selection-Based Requirements				
FCS_CKM_EXT.6		IA-5	**Authenticator Management**	A conformant TOE requires passwords to meet specific

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
	Cryptographic Password/Passphrase Conditioning			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.
FCS_VAL_EXT.2(1)	**Validation Remediation (Server Administrator)**	AC-7	**Unsuccessful Logon Attempts**	A conformant TOE performs some protective action if an administrator has a sufficiently large number of consecutive failed authorization attempts due to presenting an invalid authorization factor.
FIA_CHR_EXT.1	**Challenge/Response Recovery Credential**	N/A	**N/A**	NIST SP 800-53 revision 5 does not define any controls that relate specifically to the use of challenge/response as a method of generating recovery credentials.
FTP_TRP.1	**Trusted Path**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A conformant TOE may support the enforcement of this control if the protocol(s) used to establish trusted communications uses mutual authentication.
		SC-8(1)	**Transmission Confidentiality and Integrity:**	A conformant TOE will have the ability to prevent unauthorized disclosure of information and detect

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
			Cryptographic Protection	modification to that information.
		SC-11	**Trusted Path**	The TOE establishes a trusted communication path between remote users and itself.
Objective Requirements				
This PP-Module has no objective requirements.				