Mapping Between
Extended Package for Software File Encryption, Version 1.0, 10-November-2014
and
NIST SP 800-53 Revision 4

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 4, 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.
- **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 to the extent that the data being protected by the TSF 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.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 4 Control**		**Comments and Observations**
Security Functional Requirements for the Software File Encryption Application (TOE)				
FCS_CKM_EXT.2	**Cryptographic Key Generation (FEK)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to perform key generation in support of key establishment activities.
		SC-12(2)	**Cryptographic Key Establishment and Management:** Symmetric Keys	A conformant TOE has the ability to generate symmetric cryptographic keys that use NSA-approved and FIPS-validated

				cryptographic algorithms, satisfying the key generation portion of this control.
FDP_PRT_EXT.1	**Protection of Selected User Data**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform symmetric encryption and decryption using NSA-approved and FIPS-validated algorithms.
		SC-28	**Protection of Information at Rest**	A conformant TOE provides a mechanism for securing data at rest.
		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 STIGs or other organizational requirements. Specific additional controls may be supported depending on the functionality claimed by the TOE; the security control assessor must review what has been selected in the Security Target and determine what additional support is provided, if any.

FPT_FEK_EXT.1	**File Encryption Key (FEK) Support**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to either prevent the storage of cryptographic keys or to store them only in a secure manner.
FPT_KYP_EXT.1	**Protection of Key and Key Material**	IA-5	**Authenticator Management**	A conformant TOE provides the ability to protect any key data used as an authenticator against unauthorized identification or disclosure.
		SC-12	**Cryptographic Protection**	A conformant TOE will ensure that secret key and keying material data are not stored in plaintext except in specific cases where appropriate.
Security Functional Requirements for the Software File Encryption Application of Client Platform				
FCS_CKM_EXT.4	**Cryptographic Key Destruction**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys.
FCS_COP.1(1)	**Cryptographic Operation:** Data Encryption	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform symmetric encryption and decryption using NSA-approved and FIPS-validated algorithms.
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_IV_EXT.1	**Initialization Vector Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will generate initialization vectors in support of key lifecycle activities.
		SC-13	**Cryptographic Protection**	A conformant TOE has the ability to generate IVs in a manner that facilitates proper key generation.
FCS_KYC_EXT.1	**Key Chaining and Key Storage**	SC-13	**Cryptographic Protection**	If the TSF provides the mechanism for securing

				keys stored in a key chain, it will implement NSA-approved and FIPS-validated cryptography in order to satisfy this function.
FIA_AUT_EXT.1	**User Authorization**	IA-5	**Authenticator Management**	A conformant TOE will define authenticators that are associated with users and used to access encrypted data belonging to those users.
		IA-5(1)	**Authenticator Management:** Password-Based Authentication	Depending on the type of authentication factor required by the TOE, the control for password-based authentication may be satisfied.
FDP_PRT_EXT.1	**Protection of Selected User Data**	SC-4	**Information in Shared Resource**s	A conformant TOE will ensure that residual sensitive file information does not persist in memory after use.
Optional Requirements				
FDP_PRT_EXT.2	**Protection of Selected User Data**	AC-3	**Access Enforcement**	A conformant TOE will ensure that logical access to encrypted data is granted only to the user(s) that are authorized to decrypt it.
		SC-4	**Information in Shared Resources**	A conformant TOE will ensure that residual sensitive file information does not persist in memory after use.
FDP_PM_EXT.1	**Protection of Data in Power Managed States**	IA-11	**Re-Authentication**	Depending on the power states supported by the TSF, a conformant TOE may require re-authentication to occur following a transition to a power-on state before access to

				encrypted data is granted.
		SC-4	**Information in Shared Resources**	A conformant TOE will ensure that residual sensitive file information is not made available during or after a transition to a powered-down state.
		SC-28	**Protection of Information at Rest**	A conformant TOE will protect information at rest when in a power managed state.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	The mechanism by which a conformant TOE protects data at rest in a power managed state is through the use of encryption.
FDP_AUT_EXT.2	**Data Authentication Using Cryptographic, Keyed-Hash Functions**	SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE will perform data authentication in order to ensure the integrity of encrypted data.
		SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE will use cryptographic methods in order to verify the integrity of encrypted data.
		SC-13	**Cryptographic Protection**	The TOE uses NSA-approved and FIPS-validated cryptographic functionality in order to perform data authentication.
FDP_AUT_EXT.1	**Authentication of Selected User Data**	SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE will perform data authentication in order to ensure the integrity of encrypted data.
		SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE will use cryptographic methods in order to verify the integrity of encrypted data.
		SC-13	**Cryptographic Protection**	The TOE uses NSA-approved and FIPS-

				validated cryptographic functionality in order to perform data authentication.
FCS_COP.1(6)	**Cryptographic Operation:** FAK Encryption/Decryption Support	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform key wrapping using NSA-approved and FIPS-validated algorithms.
FCS_CKM_EXT.5	**Cryptographic Key Management:** File Authentication Key (FAK) Support	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will have the ability to generate file authentication keys and to ensure that these keys are either not stored or stored in a secure manner.
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.
FDP_AUT_EXT.3	**Data Authentication Using Asymmetric Signing and Verification**	SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE will perform data authentication in order to ensure the integrity of encrypted data.
		SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE will use cryptographic methods in order to verify the integrity of encrypted data.
		SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform key wrapping using NSA-approved and FIPS-validated algorithms.
Selection-based Requirements				
FCS_CKM.1(A)	**Cryptographic Key Generation:** Password/Passphrase Conditioning	SC-12	**Cryptographic Protection**	A conformant TOE has the ability to perform password conditioning using NSA-approved and FIPS-validated algorithms.

FCS_CKM.1(1)	**Cryptographic Key Generation:** For Asymmetric Keys	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will perform key generation as part of the process for enabling secure storage of a FEK.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	The specific method of generating ephemeral keys used as part of secure storage of a FEK is an asymmetric key generation algorithm.
FCS_CKM_EXT.1	**Cryptographic Key Management:** Key Encrypting Key (KEK) Support	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to support the use of key encryption keys as a method for ensuring the secure storage of generated keys.
FCS_COP.1(4)	**Cryptographic Operation:** Keyed-Hash Message Authentication	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform keyed-hash message authentication using NSA-approved and FIPS-validated
FIA_FCT_EXT.1(1)	**User Authorization with External Entity Authorization Factors**	AC-3	**Access Enforcement**	A conformant TOE has the ability to require an external authentication factor to be provided before data can be decrypted.
		IA-5(11)	**Authenticator Management:** Hardware Token-Based Authentication	A conformant TOE has the ability to rely on a hardware token (such as a smart card) to provide an external authentication factor.

FIA_FCT_EXT.1(2)	**User Authentication with Password/Passphrase Authorization Factors**	AC-3	**Access Enforcement**	A conformant TOE has the ability to require a password authentication factor to be provided before data can be decrypted.