Mapping Between

Protection Profile for USB Flash Drives, Version 1.0, 2011-12-01

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 or PP-Configuration 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 satisfies SC-28 for the data stored on it. Use of the TOE is only one small part of the organization's implementation of SC-28 as a whole.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
TOE Security Functional Requirements				
FCS_CKM.1(1)	**Cryptographic Key Generation (DEK)**	SC-12	**Cryptographic Key Establishment and Management**	The ability of the TOE to generate symmetric keys satisfies the key generation portion of this control.
		SC-12(2)	**Cryptographic Key Establishment and Management:** Symmetric Keys	A conformant TOE ensures that generated asymmetric keys provide an appropriate level of security.
FCS_CKM.1(2)	**Cryptographic Key Generation (KEK)**	SC-12	**Cryptographic Key Establishment and Management**	The ability of the TOE to derive key encryption keys satisfies the key generation portion of this control.
FCS_CKM.1(3)	**Cryptographic Key Generation (Password Conditioning)**	IA-5	**Authenticator Management**	A conformant TOE protects the authenticator content from unauthorized

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				disclosure and modification as identified in item (g).
		IA-5(1)	**Authenticator Management:** Password-Based Authentication	A conformant TOE will have the ability to enforce some minimum password complexity requirements, although they are not identical to CNSS or DoD parameter values or to those specified in part (a) of this control.
		SC-13	**Cryptographic Protection**	A conformant TOE supports this control by using a password as a mechanism to unlock a data encryption key. Note however that the extent to which this control is supported depends on whether the organization's implementation of the control aligns with the TOE's behavior with respect to the data that is protected and the cryptographic mechanisms used to protect that data.
FCS_CKM.2	**Cryptographic Key Distribution (Trusted Update)**	SC-12	**Cryptographic Key Establishment and Management**	The ability of the TOE to generate symmetric keys satisfies the key distribution portion of this control.
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(2)	**Cryptographic Operation (Signature Verification)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic signing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(3)	**Cryptographic Operation (Cryptographic Hashing)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic hashing using NSA-approved and FIPS-validated algorithms.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
FCS_COP.1(4)	**Cryptographic Operation (Key Masking)**	SC-13	**Cryptographic Protection**	A conformant TOE supports this control by implementing a mechanism by which a KEK is used to mask a DEK.
FCS_RBG_EXT.1	**Extended: Cryptographic Operation (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.
FDP_DSK_EXT.1	**Extended: Protection of Data on USB Flash Drive**	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.
FIA_AUT_EXT.1	**Extended: USB Flash Drive User Authorization**	AC-3	**Access Enforcement**	A conformant TOE will enforce access control on stored data at rest.
FMT_MTD.1	**Management of TSF Data (for reading of all symmetric keys)**	AC-3	**Access Enforcement**	A conformant TOE will ensure that there is no external mechanism to access key data stored on the TOE.
FMT_SMF.1	**Specification of Management Functions**	IA-5	**Authenticator Management**	A conformant TOE supports this control through management of the password authorization factor (function c).
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports this control through management of the key data associated with the TOE (functions a and b). Note that the scope of the control's applicability is to the TOE itself as no integration with a larger key management system is expected. This control mapping also does not consider any selections made for function d, which may cover other controls.
FPT_SFP_EXT.1	**Extended: TSF System File Protection**	CM-14	**Signed Components**	A conformant TOE supports this control by ensuring that software will not be

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				installed unless it has a valid digital signature.
FPT_TUD_EXT.1	**Extended: USB Flash Device Trusted Update**	CM-14	**Signed Components**	A conformant TOE supports this control by ensuring that software will not be installed unless it has a valid digital signature per FPT_TUD_EXT.1.3. FPT_TUD_EXT.1.1 and 1.2 do not directly relate to any security controls.
FPT_TST_EXT.1	**Extended: TSF Testing**	SI-6	**Security and Privacy Function Verification**	A conformant TOE will run automatic tests to ensure correct operation of its own functionality.
Additional Requirements				
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(X2)	**Cryptographic Operation (Cryptographic Hashing)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic hashing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1	**Cryptographic Operation (Keyed Cryptographic Hashing)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform keyed cryptographic hashing using NSA-approved and FIPS-validated algorithms.
FCS_CKM.1(3)	**Cryptographic Key Generation (Passphrase Conditioning)**	IA-5	**Authenticator Management**	A conformant TOE protects the authenticator content from unauthorized disclosure and modification as identified in item (g).
		IA-5(1)	**Authenticator Management:** Password-Based Authentication	A conformant TOE will have the ability to enforce some minimum password complexity requirements, although they are not identical to CNSS or DoD requirements or to those specified in part (a) of this control.
		SC-13	**Cryptographic Protection**	A conformant TOE supports this control by using a password as a mechanism

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				to unlock a data encryption key. Note however that the extent to which this control is supported depends on whether the organization's implementation of the control aligns with the TOE's behavior with respect to the data that is protected and the cryptographic mechanisms used to protect that data.
FCS_CKM_EXT.1(X1)	**Cryptographic key generation (Host Split Authorization Factor)**	AC-3	**Access Enforcement**	A conformant TOE supports this control by implementing a mechanism to generate a split authorization factor, which enforces access to protected data by requiring the user to have possession of an authorization factor that is stored outside of the TOE.
FCS_CKM_EXT.1(X2)	**Cryptographic key generation (TOE Stored Submasks)**	AC-3	**Access Enforcement**	A conformant TOE supports this control by protecting a generated submask from unauthorized access using a PIN, which enforces access to protected data by requiring the user to have possession of an authorization factor that is stored outside of the TOE.
FIA_AFL_EXT.1	**Authorization Failure Handling**	AC-7	**Unsuccessful Logon Attempts**	A conformant TOE supports this control by taking an action to render its data unreadable when an excessive number of failed authentication attempts occur. Note that in order to apply to the control this behavior must be consistent with the actions the organization specifies in part (b) of the control.
Optional Requirements				
No optional requirements defined.				
Selection-Based Requirements				
No selection-based requirements defined.				

Common Criteria Version 3.x SFR	NIST SP 800-53 Revision 5 Control Supports	Comments and Observations
Objective Requirements		
No objective requirements defined.		