Mapping Between
Protection Profile for Application Software, Version 1.4, 7 October 2021
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.
- **Granularity of SFRs vs controls.** It is important to remember that the Security Functional Requirements (SFRs) and the Security and Privacy Controls (Controls) are at completely different levels of abstractions. SFRs can be very low level, specifying internal characteristics and behaviors of given functions. Even when broader, SFRs are restricted to a specific product. Controls, on the other hand, are very high level, specifying both technical behavior and processes for the system writ large, broadly across the large number of devices, components and products that make up the system and achieve the overall mission. A low-level SFR may contribute in some small way towards the satisfaction of a control, but it rarely satisfies the control in isolation and should not be interpreted as doing so. More often, the combination of SFRs that define the security functionality of a product may serve to support just a single control, and looking at the finer level of detail may not be as useful, such as the low-level details of protocol implementations. When looking at these mappings, it is important to remember the differences in levels of abstraction; in particular, it is important not to read more into an SFR to Control mapping than a contribution of some level of support.
- **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(1) to the extent that the data 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.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
Mandatory Requirements (presented alphabetically)				
FCS_CKM_EXT.1	**Cryptographic Key Generation Services**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to provide a key generation function.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE has the ability to generate asymmetric cryptographic keys. This SFR addresses the control with respect to key generation.
FCS_RBG_EXT.1	**Random Bit Generation Services**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to use of an appropriate DRBG ensures that generated keys provide an appropriate level of security.
FCS_STO_EXT.1	**Storage of Credentials**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	A conformant TOE restricts access to a credential repository, which supports this control if such a repository is identified by the organization as requiring restricted access.
		IA-5	**Authenticator Management**	A conformant TOE has the ability to protect authenticator content from unauthorized modification or disclosure as specified in part (g) of the control.
FDP_DAR_EXT.1	**Encryption of Sensitive Application Data**	SC-28	**Protection of Information at Rest**	A conformant TOE has the ability to place sensitive application data in protected storage, either within its own boundary or in the Operational Environment.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	**(selection-dependent)** A conformant TOE has the ability to store sensitive application data in protected storage. This may involve cryptographic protection of this data, depending on selections made.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FDP_DEC_EXT.1	**Access to Platform Resources**	AC-3(12)	**Access Enforcement:** Assert and Enforce Application Access	A conformant TOE supports this control by identifying the system resources it requires the use of. Parts (a) or (c) of this control are supported, depending on whether access is requested during initial installation or runtime.
		AC-6	**Least Privilege**	A conformant TOE has the ability to provide the minimum level of access to system resources required to implement its functionality.
FDP_NET_EXT.1	**Network Communications**	AC-3	**Access Enforcement**	A conformant TOE has the ability to access network resources for which it is authorized.
		AC-3(12)	**Access Enforcement:** Assert and Enforce Application Access	A conformant TOE supports this control by identifying the network resources it requires the use of. Parts (a) or (c) of this control are supported, depending on whether access is requested during initial installation or runtime.
FMT_CFG_EXT.1	**Secure by Default Configuration**	AC-3	**Access Enforcement**	A conformant TOE supports this control through its default implementation of file permissions that protect the application binaries and data from unauthorized access.
		AC-6	**Least Privilege**	A conformant TOE is implemented such that its default file system permissions restrict its access to only the subjects that need to interact with it.
		IA-5	**Authenticator Management**	If the TOE includes a default credential, part (e) of this control is satisfied because the credential must be changed on first use. This also satisfies part (b) of the control as the

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				changed credential is an 'initial authenticator.' Note however that there are no PP requirements for the composition of authenticators, so part (b) is only satisfied if the administrator follows organizational guidance when specifying this.
FMT_MEC_EXT.1	**Supported Configuration Mechanism**	N/A	N/A	This SFR defines the ability of the TOE to be deployed in an environment where an OS platform is used in accordance with vendor guidance. This means that the TOE can exist in an organization that satisfies CM-2 but the presence of the TOE does not assist in the enforcement or satisfaction of the control.
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.
FPR_ANO_EXT.1	**User Consent for Transmission of Personally Identifiable Information**	AC-3	**Access Enforcement**	A conformant TOE has the ability to provide access enforcement by ensuring that only the authorized transmission of personally identifiable information will be performed.
		PT-4	**Consent**	A conformant TOE requires user approval before the transmission of Personally

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				Identifiable Information over a network.
FPT_AEX_EXT.1	**Anti-Exploitation Capabilities**	SI-16	**Memory Protection**	A conformant TOE has the ability to provide measures to ensure that the underlying platform's memory is protected against unauthorized code execution. The extent to which the control is satisfied depends on both the organizational safeguards that are used to mitigate this and the specific countermeasures that are used by the TOE.
FPT_API_EXT.1	**Use of Supported Services and API's**	SA-15(5)	**Development Process, Standards, and Tools:** Attack Surface Reduction	The TOE developer is required to use only documented platform APIs, which reduces the attack surface of the TSF to known components.
FPT_LIB_EXT.1	**Use of Third Party Libraries**	CM-2	**Baseline Configuration**	A conformant TOE packages third party libraries as part of the current baseline configuration.
		SA-15(5)	**Development Process, Standards, and Tools:** Attack Surface Reduction	A conformant TOE supports the enforcement of this control because enumerating the third party libraries used by the TOE reduces the attack surface of the TSF to known components.
FPT_IDV_EXT.1	**Software Identification and Versions**	CM-2	**Baseline Configuration**	A conformant TOE is uniquely identified through its version information in support of establishing a baseline configuration for information system assets. Note that if the TOE claims use of SWID tags in this SFR, it also supports the enforcement of CM-2(2).
		CM-8	**System Component Inventory**	A conformant TOE's use of version information supports the enforcement of this control by providing a means to uniquely

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				identify it in an information system component inventory.
FPT_TUD_EXT.1	**Integrity for Installation and Update**	CM-14	**Signed Components**	A conformant TOE requires that TOE updates include integrity measures through the use of a digital signature.
		SI-2	**Flaw Remediation**	To prevent the software from being out of date and vulnerable to flaws, a conformant TOE has the ability to update its components through the underlying OS platform.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE has the ability to verify the integrity of updates to it.
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.
Optional Requirements (presented alphabetically)				
FCS_CKM.1/SK	**Cryptographic Symmetric Key Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE establishes and manages cryptographic keys for required cryptography employed within the application.
		SC-12(2)	**Cryptographic Key Establishment and Management:** Symmetric Keys	A conformant TOE has the ability to produce symmetric keys in accordance with organization-defined requirements.
Objective Requirements (presented alphabetically)				

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FPT_API_EXT.2	**Use of Supported Services and APIs**	SA-15(5)	**Development Process, Standards, and Tools:** Attack Surface Reduction	A conformant TOE is required to parse only certain types of data, which reduces the attack surface of the TSF to fewer input data methods.
Implementation-Based Requirements (presented alphabetically)				
This PP has no implementation-based requirements.				
Selection-Based Requirements (presented alphabetically)				
FCS_CKM.1/AK	**Cryptographic Asymmetric Key Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to perform key generation functions.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE has the ability to generate asymmetric cryptographic keys. This SFR addresses the control with respect to key generation.
FCS_CKM.1/PBKDF	**Password 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 protects stored passwords using an approved salted key derivation function as identified in item (d).
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to perform Password-based Key Derivation Functions.
FCS_CKM.2	**Cryptographic Key Establishment**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports this control by providing a key establishment function.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE ensures that generated asymmetric keys provide an appropriate level of security.
FCS_COP.1/SKC	**Cryptographic Operation – Encryption / Decryption**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform symmetric encryption and decryption 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/Hash	**Cryptographic Operation – 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/Sig	**Cryptographic Operation – Signing**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic signing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1/KeyedHash	**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 algorithms.
FCS_HTTPS_EXT.1/Client	**HTTPS Protocol**	SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE provides the ability to implement HTTPS using TLS to ensure the confidentiality and integrity of data in transit.
FCS_HTTPS_EXT.1/Server	**HTTPS Protocol**	SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE provides the ability to implement HTTPS using TLS to ensure the confidentiality and integrity of data in transit.
FCS_HTTPS_EXT.2	**HTTPS Protocol with Mutual Authentication**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A conformant TOE supports this control by implementing cryptographic mutual authentication for the HTTPS channel.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE provides the ability to implement HTTPS using TLS to ensure the confidentiality and integrity of data in transit.
FCS_RBG_EXT.2	**Random Bit Generation from Application**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to generate keys using pseudorandom inputs in accordance with organization-defined requirements.
		SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform deterministic random bit generation using NSA-

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				approved and FIPS-validated algorithms.
FIA_X509_EXT.1	**X.509 Certificate Validation**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE has the ability to validate certificate path and status, which satisfies this control.
		SC-23	**Session Authenticity**	Depending on the TOE's use of trusted communications channels, it may use X.509 certificate validation in support of session authentication.
		SC-23(5)	**Session Authenticity:** Allowed Certificate Authorities	A conformant TOE supports this control because the SFR requires the certificate path to terminate with a trusted certificate. This means that the TSF has the capability to reject a certificate based on its issuer not being trusted. This allows the TOE to conform to an organizational policy to accept only those certificates that are signed by a trusted issuer, as long as those issuers are designated in the system as trust anchors.
FIA_X509_EXT.2	**X.509 Certificate Authentication**	IA-2	**Identification and Authentication (Organizational Users)**	**(selection-dependent)** A conformant TOE may support this control if it acts as a server for communications that use bidirectional authentication and the client is authenticated using an X.509 certificate that represents a user, such as through a physical USB authentication token.
		IA-3 -or- IA-9	**Device Identification and Authentication** **-or-**	A conformant TOE supports one of these controls by using X.509 certificates to authenticate remote entities with which the TSF

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
			Service Identification and Authentication	attempts to connect to via a trusted protocol. Which control is supported depends on whether the presented certificate represents a device or a service running on a particular device (e.g. in a case where a single device has different certificates used for different services).
		IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	**(selection-dependent)** A conformant TOE may support this control if the TSF uses X.509 authentication for a trusted channel that requires client authentication, such as mutually-authenticated TLS.
FPT_TUD_EXT.2	**Integrity for Installation and Update**	SI-2(6)	**Flaw Remediation:** Removal of Previous Versions of Software and Firmware	A conformant TOE removes previous versions of software or firmware components after updates have been installed.
		SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE is distributed using the format of the platform-supported package manager.