Mapping Between Protection Profile for General Purpose Operating Systems, Version 4.3, 27-September-2022 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 generate audit records only supports AU-2 to the extent that the TOE's audit records are included in the set of "organization-defined auditable events" 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)				
FAU_GEN.1	**Audit Data Generation**	AU-2	**Event Logging**	A conformant TOE has the ability to generate audit records for various events.
		AU-3	**Content of Audit Records**	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data.
		AU-12	**Audit Record Generation**	The TOE has the ability to generate audit logs, as well as control which events are logged, satisfying this control.
FCS_CKM.1	**Cryptographic Key Generation**	SC-12	**Cryptographic Key Establishment and Management**	The ability of the TOE to generate asymmetric keys satisfies the key generation portion of this control.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE has the ability to generate asymmetric cryptographic keys that use NSA-approved and FIPS-validated cryptographic algorithms. This control satisfies this SFR with respect to key generation.
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 has the ability to perform key establishment for asymmetric cryptographic keys that use NSA-approved and FIPS-validated cryptographic algorithms. This control satisfies this SFR with respect to key generation.
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/ENCRYPT	**Cryptographic Key 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.
FCS_COP.1/HASH	**Cryptographic Key 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/KEYHMAC	**Cryptographic Key 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_COP.1/SIGN	**Cryptographic Key Operation - Signing**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic signing using NSA-approved and FIPS-validated algorithms.
FCS_RBG_EXT.1	**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.
FCS_STO_EXT.1	**Storage of Sensitive Data**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	A conformant TOE restricts access to repositories containing credential and key data.
		IA-5(1)	**Authenticator Management:** Password-Based Authentication	Cryptographic security of password data allows for proper enforcement of password-based authentication.
		IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	Cryptographic security of PKI data allows for proper enforcement of public key-based authentication.
		SC-13	**Cryptographic Protection**	The ability of a conformant TOE to encrypt data stored in non-volatile memory ensures the integrity and

				authenticity of this data.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A conformant TOE has the ability to implement cryptographic mechanisms to prevent unauthorized disclosure and modification of data.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE has the ability to securely store cryptographic keys.
FDP_ACF_EXT.1	**Access Controls for Protecting User Data**	AC-3	**Access Enforcement**	A conformant TOE has the ability to restrict users from accessing resources owned by other users without permission.
FIA_AFL.1	**Authentication Failure Handling**	AC-7	**Unsuccessful Logon Attempts**	The TOE has the ability to detect when a defined number of unsuccessful authentication attempts occur and take some corrective action.
FIA_UAU.5	**Multiple Authentication Mechanisms**	IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE can implement one or more methods of authentication for users and administrators.
		IA-2(1)	**Identification and Authentication (Organizational Users):** Multi-Factor Authentication to Privileged Accounts	A conformant TOE may provide multi-factor authentication in order to access the TSF using a privileged account.
		IA-2(2)	**Identification and Authentication (Organizational Users):** Multi-Factor Authentication to Non-Privileged Accounts	A conformant TOE may provide multi-factor authentication in order to access the TSF using a non-privileged account.
		IA-2(12)	**Identification and Authentication (Organizational Users):** Acceptance of PIV Credentials	**(selection-dependent)** A conformant TOE may support authentication using a PIN that unlocks an asymmetric key, depending on selections made. This may potentially be derived from a PIV credential.

FIA_X509_EXT.1	**X.509 Certificate Validation**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE has the ability to certificate path and status, which satisfies this control.
		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-** **Service Identification and Authentication**	A conformant TOE supports one of these controls by using X.509 certificates to authenticate remote entities with which the TSF 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.
FMT_MOF_EXT.1	**Management of Security Functions Behavior**	AC-2(5)	**Account Management:** Inactivity Logout	If optional functionality for configuration of screen lock and/or remote connection inactivity timeout, a conformant TOE has the ability to enforce inactivity logout mechanisms.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	This allows a conformant TOE to distinguish between user and administrator roles in terms of the level of system access that is available to each.
		AC-6(1)	**Least Privilege:** Authorize Access to Security Functions	A conformant TOE supports this control by ensuring that security functions cannot be accessed except by authorized administrators.
		AC-6(10	**Least Privilege:** Prohibit Non-Privileged Users from Executing Privileged Functions	A conformant TOE supports this control by limiting the system functions that non-privileged users can perform.
FMT_SMF_EXT.1	**Specification of Management Functions**	AC-2(5)	**Account Management:** Inactivity Logout	If optional functionality for configuration of screen lock and/or remote connection inactivity timeout is selected, a conformant TOE has the ability to enforce inactivity logout mechanisms.

AC-7	**Unsuccessful Logon Attempts**	A conformant TOE has the ability for an administrator to define a defined number of unsuccessful authentication attempts and take some action when this number is exceeded.
AC-11	**Device Lock**	A compliant TOE supports this control by requiring user re-authentication following a TSF initiated lock or user initiated lock condition.
AC-12	**Session Termination**	A compliant TOE supports this control by automatically terminating a user session by an administrator configured time out session of user activity.
AC-18	**Wireless Access**	If the optional management function of configure WiFi or Bluetooth interface is selected, A conformant TOE will permit an administrator to establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access.
AU-2	**Event Logging**	If the optional management function configure audit rules is selected, a conformant TOE will permit an administrator to identify the types of events that the system is capable of logging.
IA-4	**Identifier Management**	If the optional management function for directory server configuration is selected, a conformant TOE has

				the ability to support identifier management through connection to a centralized directory server.
		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 (f) and (h) of this control.
		SC-7(12)	**Boundary Protection:** Host-Based Protection	If optional management functionality for the configuration of a host-based firewall is selected, a conformant TOE has the ability to apply host-based protection to itself.
		SI-2(5)	**Flaw Remediation:** Automatic Software and Firmware updates	If the optional management functionality enable/disable automatic software updates is selected, a conformant TOE may be configured to carry out automatic updates.
FPT_ACF_EXT.1	**Access Controls**	AC-3(4)	**Access Enforcement:** Discretionary Access Control	The TOE has the ability to enforce DAC through enforcement of an access control policy that allows the owner of an object to deny all other subjects access to that object.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	The TOE has the ability to enforce RBAC because the SFR is defining functionality that is unavailable to all users who belong to a particular role.
		AC-6(10)	**Least Privilege:** Prohibit Non-Privileged Users From Executing Privileged Functions	A conformant TOE prohibits unprivileged users from modifying the security settings.

		AU-9	**Protection of Audit Information**	A conformant TOE supports this control by protecting audit records from unauthorized access.
		IA-5	**Authentication Management**	A conformant TOE supports part (g) of this control by protecting system-wide credential repositories from unauthorized access.
FPT_ASLR_EXT.1	**Address Space Layout Randomization**	SI-16	**Memory Protection**	A conformant TOE has the ability to implement ASLR to prevent unauthorized code execution.
FPT_SBOP_EXT.1	**Stack Buffer Overflow Protection**	SI-16	**Memory Protection**	A conformant TOE has the ability to prevent unauthorized code execution.
FPT_TST_EXT.1	**Boot Integrity**	SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	The TOE has the ability to verify the integrity of the boot chain prior to execution.
		SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE has the ability to implement cryptographic mechanisms to detect unauthorized change.
		SI-7(9)	**Software, Firmware, and Information Integrity:** Verify Boot Process	A conformant TOE has the ability to verify the integrity of the boot process.
FPT_TUD_EXT.1	**Trusted Update**	CM-14	**Signed Components**	A conformant TOE has the ability to require a signed update.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	The TOE has the ability to verify the integrity of updates to itself.
FPT_TUD_EXT.2	**Trusted Update for Application Software**	CM-14	**Signed Components**	A conformant TOE has the ability to require a signed update.
FPT_W^X_EXT.1	**Write XOR Execute Memory Pages**	SI-16	**Memory Protection**	Implementation of this SFR is a method by which a conformant TOE will protect memory from unauthorized code

				execution.
FTP_ITC_EXT.1	**Trusted Channel Communication**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	The use of the cryptographic protocols specified in the SFR implies that the TOE can perform mutual authentication with trusted remote entities.
		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.
FTP_TRP.1	**Trusted Path**	SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE will have the ability to prevent unauthorized disclosure of information and also detect modification to that information.
		SC-11	**Trusted Path**	The TOE establishes a trusted communication path between remote users and itself.
Optional Requirements (presented alphabetically)				
FTA_TAB.1	**Default TOE Access Banners**	AC-8	**System Use Notification**	The TOE displays an advisory warning to the user prior to authentication.
Objective Requirements (presented alphabetically)				
FPT_BLT_EXT.1	**Limitation of Bluetooth Profile Support**	IA-3	**Device Identification and Authentication**	A conformant TOE supports this control by providing a method to limit the devices that are permitted to be authenticated over the Bluetooth interface.
FPT_SRP_EXT.1	**Software Restriction Policies**	CM-5(6)	**Access Restrictions for Change:** Limit Library Privileges	To the extent that a conformant TOE has the ability to implement a whitelisting policy defined by the organization, this SFR satisfies this control.
Implementation-Based Requirements (presented alphabetically)				
This PP has no implementation-based requirements.				
Selection-Based Requirements (presented alphabetically)				
FDP_IFC_EXT.1	**Information Flow Control**	AC-4	**Information Flow Enforcement**	A conformant TOE supports this control by

				enforcing an information flow such that once a VPN connection is made, all subsequent IP traffic must traverse the VPN.
		SC-7(7)	**Boundary Protection:** Split Tunneling for Remote Devices	A conformant TOE supports this control by ensuring that network traffic will not be sent outside of a VPN connection once that connection is established. Per the application note, this is to be understood as a requirement for the VPN client not to split-tunnel.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE supports this control by allowing for the use of a VPN client to protect data in transit from unauthorized modification and disclosure.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE supports this control by allowing for the use of a VPN client that can be used to protect data in transit using IPsec.