Mapping Between

PP-Module for Virtual Private Network (VPN) Clients, Version 2.4, 2022-03-31

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 and 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 specific controls, but typically satisfaction also requires the implementation of operational procedures; furthermore, 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 whether the control is satisfied in the overall system context.
- **Granularity of SFRs versus 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 abstraction. 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 whole system, 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 toward 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; particularly, 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.
- **AC-17.** The primary function of this PP-Module is to facilitate the establishment of IPsec VPN connections. A conformant TOE is therefore deployed to support the enforcement of AC-17 at a general level.
- **PKI certificates.** It does not explicitly state anywhere in the PP-Module that PKI certificates need to be issued as part of the VPN infrastructure, but this is implied since it is virtually impossible to have a VPN infrastructure without some sort of organized PKI. Therefore, a TOE conforming to this PP (and any other PPs that use certificates) is expected to help support SC-17.
- **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.

- **PP-Module.** A TOE that conforms to this PP-Module will also conform to the Protection Profile for General Purpose Operating Systems (GPOS PP), Protection Profile for Mobile Device Fundamentals (MDF PP), Protection Profile for Application Software (App PP), or Protection Profile for Mobile Device Management (MDM PPP) by definition. Therefore, the TOE will satisfy additional security controls not referenced here through its conformance to one of these Base-PPs. This PP-Module refines some of the Base-PP requirements to ensure consistency between the claimed Base-PP and the PP-Module, but this does not affect the security controls that satisfying those requirements is intended to address.

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
Additional Requirements (GPOS PP Base)				
FCS_CKM_EXT.2	**Cryptographic Key Storage**	SC-12	**Cryptographic Key Establishment and Management**	The ability of the TOE to store key data in platform-provided storage supports the key storage portion of this control.
FIA_X509_EXT.3	**Certificate Use and Management**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications, which satisfies this control. Other controls apply if the TOE also uses code signing certificates for software updates (CM-14, SI-7(15)) or integrity verification (SI-7, SI-7(1), SI-7(6)).
FTP_ITC.1	**Inter-TSF Trusted Channel**	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	**Transmission Confidentiality and Integrity**	A conformant TOE can 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 TOE supports a cryptographic method of protecting data in transit.
Additional Requirements (MDF PP Base)				
This PP-Module does not define any additional requirements when the MDF PP is the Base-PP.				
Additional Requirements (App PP Base)				
FCS_CKM_EXT.2	**Cryptographic Key Storage**	IA-5	**Authenticator Management**	A conformant TOE will have the ability to provide secure storage of authenticators depending on the use of the key which would satisfy item (g) of this control.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will help satisfy the key storage portion of this control.

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
FCS_CKM_EXT.4	**Cryptographic Key Destruction**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE can destroy keys based on organizational policy and standards.
Additional Requirements (MDM PP Base)				
This PP-Module does not define any additional requirements when the MDM PP is the Base-PP.				
TOE Security Functional Requirements				
FCS_CKM.1/VPN	**Cryptographic Key Generation (IKE)**	AC-17(2)	**Remote Access:** Protection of Confidentiality and Integrity Using Encryption	A conformant TOE will generate keys that are used for encryption of remote access communications.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE provides a key generation function.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	The specific key generation function provided by the TOE uses asymmetric keys.
FCS_IPSEC_EXT.1	**IPsec**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE implements IPsec as a method of ensuring confidentiality and integrity of data in transit.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE's use of IPsec provides a cryptographic means to protect data in transit.
FDP_RIP.2	**Full Residual Information Protection**	SC-4	**Information in Shared System Resources**	This SFR addresses the control to prevent access to the previous information content of a resource.
FMT_SMF.1/VPN	**Specification of Management Functions (VPN)**	CM-6	**Configuration Settings**	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.

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
FPT_TST_EXT.1	**TSF Self-Test**	SI-6	**Security and Privacy Function Verification**	A conformant TOE can verify the correct operation of its cryptographic functionality.
		SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE can verify the integrity of the TOE's software components that can be considered a subset of the actions available for selection and assignment in the SFR.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE can verify its own integrity prior to execution.
Optional Requirements				
FIA_BMA_EXT.1	**Biometric Activation**	AC-14	**Permitted Actions without Identification or Authentication**	A conformant TOE supports this control to the extent that the actions it requires authentication for are in alignment with the security plan for the system.
		IA-2(1)	**Identification and Authentication (Organizational Users):** Multi-Factor Authentication to Privileged Accounts	A conformant TOE supports this control by requiring multi-factor authentication to authorize a connection attempt.
FPF_MFA_EXT.1	**Multifactor Authentication Filtering**	AC-14	**Permitted Actions without Identification or Authentication**	A conformant TOE supports this control to the extent that the actions it requires authentication for are in alignment with the security plan for the system.
		IA-2(1)	**Identification and Authentication (Organizational Users):** Multi-Factor Authentication to Privileged Accounts	A conformant TOE supports this control by requiring multi-factor authentication to authorize a connection attempt.
Objective Requirements				

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
FAU_GEN.1/VPN	**Audit Data Generation**	AU-2	**Event Logging**	A conformant TOE can generate audit records for various events. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-3	**Content of Audit Records**	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-3(1)	**Content of Audit Records:** Additional Audit Information	A conformant TOE will generate audit information for some auditable events beyond what is mandated in AU-3. This may or may not be sufficient to satisfy this control based on the additional audit information required by the organization. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-12	**Audit Record Generation**	A conformant TOE can generate audit logs. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				control and if the TOE's audit log is part of the overall system's auditing.
FAU_SEL.1/VPN	**Selective Audit**	AU-12	**Audit Record Generation**	A conformant TOE can support part (b) of this control by providing a mechanism to determine the set of auditable events that result in the generation of audit records.
Implementation-Based Requirements				
FDP_VPN_EXT.1	**Split Tunnel Prevention**	SC-7(7)	**Boundary Protection:** Split Tunneling for Remote Devices	A conformant TOE can ensure that split tunneling is prevented by directing all network traffic to flow through an established VPN connection.
Selection-Based Requirements				
FCS_EAP_EXT.1	**EAP-TLS**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE can 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 TOE's use of EAP-TLS supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	A conformant TOE supports this control if the control's assignment defines the cryptography implemented by the TSF as appropriate for the information system.
FIA_HOTP_EXT.1	**HMAC-Based One-Time Password Pre-Shared Keys**	IA-5	**Authenticator Management**	A conformant TOE uses hash-based pre-shared keys as a type of authenticator and will ensure their strength and confidentiality, which supports parts (c) and (h) of this control.
FIA_PSK_EXT.1	**Pre-Shared Key Composition**	N/A	**N/A**	This SFR does not support any security controls on its own; it only functions as a

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				stub to allow the TOE vendor to specify the context in which the TOE uses pre-shared keys and the types of pre-shared keys it uses.
FIA_PSK_EXT.2	**Generated Pre-Shared Keys**	IA-5	**Authenticator Management**	A conformant TOE uses generated pre-shared keys as a type of authenticator and will ensure their strength and confidentiality, which supports parts (c) and (h) of this control.
FIA_PSK_EXT.3	**Password-Based Pre-Shared Keys**	IA-5	**Authenticator Management**	A conformant TOE uses password-based pre-shared keys as a type of authenticator and will ensure their strength and confidentiality, which supports parts (c) and (h) of this control.
FIA_PSK_EXT.4	**HMAC-Based One-Time Password Pre-Shared Keys Support**	N/A	**N/A**	This SFR does not support any security controls on its own; it only functions as a stub to allow the TOE vendor to specify the TOE's support for HMAC-based pre-shared keys and whether the TSF verifies these keys itself or interfaces with an external authentication server to do so.
FIA_PSK_EXT.5	**Time-Based One-Time Password Pre-Shared Keys Support**	N/A	**N/A**	This SFR does not support any security controls on its own; it only functions as a stub to allow the TOE vendor to specify the TOE's support for time-based pre-shared keys and whether the TSF verifies these keys itself or interfaces with an external authentication server to do so.
FIA_TOTP_EXT.1	**Time-Based One-Time Password Pre-Shared Keys**	IA-5	**Authenticator Management**	A conformant TOE uses time-based pre-shared keys as a type of authenticator

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				and will ensure their strength and confidentiality, which supports parts (c) and (h) of this control. Note also that time-based pre-shared keys implicitly support part (f) of this control since they are only valid for a given period.