Mapping Between

Protection Profile Module for Virtual Private Network (VPN) Clients, Version 2.1, 05-October-2017

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.
- **PKI certificates.** It does not explicitly state anywhere in the PP 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.
- **Supported controls.** In general, the TOE's ability to satisfy a given control will frequently depend on how the parameters are completed in the control and the level of congruence between that completion and how the SFRs are completed in the ST.

Common Criteria Version 3.x SFR		**Supports Enforcement of NIST SP 800-53 Revision 4 Control**		**Comments and Observations**
GPOS PP Requirements				
FCS_CKM.1(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's ensures that generated asymmetric keys provide an appropriate level of security.
FCS_CKM.2(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's ensures that generated asymmetric keys provide an appropriate level of security.
FCS_COP.1(1)	**Cryptographic Operation (Data 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_CKM.1/VPN	**Cryptographic Key Generation (IKE)**	AC-17(2)	**Remote Access:** Protection of Confidentiality / 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_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:** PKI-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications satisfying this control.
		SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE will use cryptographic methods in order to verify the integrity of certificate revocation.
		SI-7(15)	**Software, Firmware, and Information Integrity:** Code Authentication	A conformant TOE will ensure that code is not executed unless a valid code signing certificate is provided.
		CM-5(3)	**Access Restrictions for Change:** Signed Components	FCS_CKM_EXT.3.1 requires a hash or signature to validate trusted updates using certificates. The control requires the use of a signature, so this may or may not be met depending on the selection made in the SFR.
FTP_ITC.1	**Inter-TSF Trusted Chanel**	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 has 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 or Alternate Physical Protection	The TOE supports a cryptographic method of protecting data in transit.
MDF PP Requirements				
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's ensures that generated asymmetric keys provide an appropriate level of security.
FCS_CKM.2(1)	**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 supports the production of asymmetric keys by providing a key establishment function.
FCS_COP.1(1)	**Cryptographic Operation**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform symmetric encryption and decryption using NSA-approved and FIPS-validated algorithms.

FIA_X509_EXT.2	**X.509 Certificate Authentication**	CM-5(3)	**Access Restrictions for Change:** Signed Components	FIA_X509_EXT.2.1 requires the certificate to be digitally signed prior to installation of updates. A conformant TOE may support this control by requiring the use of X.509 certificates for update integrity verification, depending on selections made.
		IA-5(2)	**Authenticator Management:** PKI-Based Authentication	A conformant TOE will validate certificate responses providing certificate integrity, satisfying part (a) of this control.
		SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE will use cryptographic methods in order to verify the integrity of the certificate path.
		SI-7(15)	**Software, Firmware, and Information Integrity:** Code Authentication	A conformant TOE may use X.509 certificates to authenticate software updates to the TOE, depending on selections made.
FTP_ITC_EXT.1	**Trusted Channel Communication**	AC-18(1)	**Wireless Access**	A conformant TOE requires a trusted channel in order to establish wireless communications.
		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 has 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 or Alternate Physical Protection	The TOE supports a cryptographic method of protecting data in transit.
FCS_CKM.1/VPN	**Cryptographic Key Generation**: IKE	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.
App PP Security Functional Requirements				
FCS_CKM.1(1)	**Cryptographic Asymmetric Key Generation**	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	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 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_EXT.1	**Cryptographic Key Generation Services**	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 may have the ability to generate asymmetric cryptographic keys. This SFR addresses the control with respect to key generation.
FCS_COP.1(1)	**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.
FIA_X509_EXT.2	**X.509 Certificate Authentication**	IA-5(2)	**Authenticator Management:** PKI-Based Authentication	A conformant TOE will validate certificate responses, satisfying part (a) of this control.

FTP_DIT_EXT.1	**Protection of Data in Transit**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE ensures the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic or Alternate Physical 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.
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 (h) of this control.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will help satisfy the key storage portion of this control.
FCS_CKM_EXT.4	**Cryptographic Key Destruction**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to destroy keys based on organizational policy and standards.
TOE Security Functional Requirements				
FCS_IPSEC_EXT.1	**IPsec Protocol**	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 Integrity:** Cryptographic or Alternate Physical 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 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**	N/A	N/A	There are no controls specifically pertain to providing management functions for VPN functionality.
FPT_TST_EXT.1	**TSF Self Test**	SI-6	**Security Function Verification**	A conformant TOE has the ability to verify the correct operation of its cryptographic functionality.
		SI-7	**Software, Firmware and Information Integrity**	A conformant TOE has the ability to 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 has the ability to verify the integrity of the boot chain prior to execution.
Optional Requirements				
N/A		N/A		
Selection-Based Requirements				

FIA_PSK_EXT.1	**Pre-Shared Key Composition**	IA-5	**Authenticator Management**	A conformant TOE uses pre-shared keys as a type of authenticator and will ensure their strength and confidentiality, which supports parts c and h of the control.
Objective Requirements				
FAU_GEN.1	**Audit Data Generation**	AU-2	**Auditable Events**	A conformant TOE has the ability to 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 Generation**	A conformant TOE has the ability to generate audit logs. 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.
FAU_SEL.1	**Selective Audit**	AU-12	**Audit Generation**	A conformant TOE has the ability to 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.
FDP_IFC_EXT.1	**Subset Information Control**	SC-7(7)	**Boundary Protection:** Prevent Split Tunneling for Remote Devices	A conformant TOE has the ability to ensure that split tunneling is prevented by directing all network traffic to flow through an established VPN connection.