Mapping Between
Protection Profile for General-Purpose Computing Platforms, Version 1.0, 2 February 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 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)				
FMT_CFG_EXT.1	**Secure by Default Configuration**	IA-5	**Authenticator Management**	If the TOE includes a default credential, part (e) of this control is supported because the credential must be changed on first use. This also satisfies part (b) of the control as the 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_MOF.1	**Management of Security Functions Behavior**	AC-3	**Access Enforcement**	A conformant TOE supports this control by limiting the ability to access the TOE's management functions to authorized subjects.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE will restrict access to management functionality to members of a certain role.
		AC-6	**Least Privilege**	A conformant TOE supports least privilege by restricting the users that are able to manage the TSF.
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

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				additional controls may be supported depending on the functionality claimed by the TOE.
FMT_SMR.1	**Security Roles**	AC-2(7)	**Account Management:** Privileged User Accounts	A conformant TOE has the ability to associate users with roles, in support of part (a) of the control.
FPT_JTA_EXT.1	**JTAG/Debug Port Access**	N/A	**N/A**	This SFR restricts access to any JTAG/debug ports on the TOE to an authorized administrator. There is no control that explicitly governs logical access to both inputs and outputs of a physical port.
FPT_PPF_EXT.1	**Protection of Platform Firmware and Critical Data**	SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE has the ability to verify the integrity of updates to itself.
		SI-7(15)	**Software, Firmware, and Information Integrity:** Code Authentication	A conformant TOE will ensure that updates are not installed unless a valid code signing certificate is provided.
FPT_ROT_EXT.1	**Platform Integrity Root**	SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE supports this control by implementing a root of trust for integrity of the TSF such that it is possible to detect if it has been modified.
FPT_ROT_EXT.2	**Platform Integrity Extension**	SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE has the ability to verify the integrity of updates to itself and notify an organizational defined user in the event of a failure.
FPT_STM.1	**Reliable Time Stamps**	AU-8	**Time Stamps**	A conformant TOE can generate and use time stamps addresses the actions defined in this control.
FPT_TUD_EXT.1	**TOE Firmware Update**	CM-14	**Signed Components**	If the TOE supports the ability for its firmware to

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				be updated, it has the ability to authenticate the source of all platform firmware updates using a digital signature algorithm.
		SI-7	**Software, Firmware, and Information Integrity**	If the TOE supports the ability for its firmware to be updated, it has the ability to verify the integrity of updates to itself.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	If the TOE supports the ability for its firmware to be updated, it has the ability to verify the integrity of updates to itself.
Optional Requirements (presented alphabetically)				
FCS_CKM_EXT.5	**Cryptographic Key Derivation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE provides a key generation function through some combination of password-based key derivation and other methods.
FCS_ENT_EXT.1	**Entropy for Tenant Software**	SC-13	**Cryptographic Protection**	A conformant TOE provides entropy source(s) for random number generation which is made accessible to tenant software.
FCS_SLT_EXT.1	**Cryptographic Salt Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE generates salts in support of various key generation and establishment functions.
FCS_STG_EXT.1	**Protected Storage**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	A conformant TOE restricts access to the key storage repository, which supports this control if such a repository is identified by the organization as requiring restricted access.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely store cryptographic keys.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE has the ability to securely store cryptographic keys.
FDP_TEE_EXT.1	**Trusted Execution Environment for Tenant Software**	SC-3	**Security Function Isolation**	A conformant TOE includes a trusted execution environment for the use of tenant software.
		SC-39	**Process Isolation**	A conformant TOE includes a trusted execution environment for the use of tenant software.
		SC-39(1)	**Process Isolation:** Hardware Separation	A conformant TOE includes a trusted execution environment for the use of tenant software.
FIA_TRT_EXT.1	**Authentication Throttling**	AC-7	**Unsuccessful Logon Attempts**	A conformant TOE supports this control by enforcing a delay between unsuccessful authentication attempts.
Objective Requirements (presented alphabetically)				
FPT_ROT_EXT.3	**Hardware Component Integrity**	CM-7(9)	**Least Functionality:** Prohibiting the Use of Unauthorized Hardware	A conformant TOE supports this control by verifying the critical hardware components prior to execution.
		CM-8(3)	**System Component Inventory:** Automated Unauthorized Component Detection	A conformant TOE supports this control by verifying the critical hardware components prior to execution. If an integrity check fails organization roles are identified and appropriate action is taken.
Implementation-Based Requirements (presented alphabetically)				
This PP has no implementation-based requirements.				
Selection-Based 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. The TOE supports the

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				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 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-12	**Audit Record 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_SAR.1	**Audit Review**	AU-6(7)	**Audit Record Review, Analysis, and Reporting:**	A conformant TOE will allow designation of

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
			Permitted Actions	permitted actions to their respective roles.
		AU-7	**Audit Record Reduction and Report Generation**	A conformant TOE provides audit review mechanisms to administrators.
FAU_STG.1	**Protected Audit Trail Storage**	AU-9	**Protection of Audit Information**	A conformant TOE has the ability to prevent unauthorized modification and deletion of audit records.
FAU_STG.4	**Prevention of Audit Data Loss**	AU-5	**Response to Audit Logging Process Failures**	A conformant TOE has the ability to react in a specific manner when the allocated audit storage space is full, which supports part (b) of the control.
FAU_STG_EXT.1	**Off-Loading of Audit Data**	AU-4(1)	**Audit Log Storage Capacity:** Transfer to Alternate Storage	A conformant TOE has the ability to transfer generated audit data to an external entity.
		AU-9(2)	**Protection of Audit Information:** Store on Separate Physical Systems or Components	A conformant TOE has the ability to transfer generated audit data to an external entity.
FCS_CKM.1/AK	**Cryptographic Key Generation (Asymmetric Keys)**	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.1/SK	**Cryptographic Key Generation**	SC-12	**Cryptographic Key Establishment and Management**	The ability of the TOE to generate symmetric keys satisfies the key

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
	(Symmetric Encryption Key)			generation portion of this control.
		SC-12(2)	**Cryptographic Key Establishment and Management:** Symmetric Keys	A conformant TOE has the ability to generate symmetric 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 supports the production of asymmetric keys by providing a key establishment function.
FCS_CKM.4	**Cryptographic Key Destruction**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys.
FCS_CKM_EXT.4	**Cryptographic Key and Key Material Destruction Timing**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys.
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/KeyedHash	**Cryptographic Operation (Keyed Hash)**	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/KAT	**Cryptographic Operation (Key Agreement/Transport)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic key agreement or transport.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FCS_COP.1/SigGen	**Cryptographic Operation (Signature Generation)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic signing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1/SigVer	**Cryptographic Operation (Signature Verification)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic signature verification using NSA-approved and FIPS-validated algorithms.
FCS_COP.1/SKC	**Cryptographic Operation (Symmetric Key Cryptography)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform symmetric encryption and decryption using NSA-approved and FIPS-validated algorithms.
FCS_HTTPS_EXT.1	**HTTPS Protocol**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE will support the implementation of PKI-based authentication by validating peer certificates as part of the authentication process.
		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 Protection	The TOE supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FCS_IPSEC_EXT.1	**IPsec Protocol**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE implements peer authentication for IPsec.
		SC-7(5)	**Boundary Protection:** Deny by Default - Allow by Exception	A conformant TOE's IPsec implementation includes a default-deny posture in its SPD.
		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.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_RBG_EXT.1	**Random Bit Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the key generation function of this control through its handling of random bit generation.
FCS_STG_EXT.2	**Key Storage Encryption**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will use a key hierarchy to ensure the secure storage of cryptographic keys.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A conformant TOE will use encryption to ensure the security of stored cryptographic data at rest.
		SC-28(3)	**Protection of Information at Rest:**	A conformant TOE has the ability to securely store cryptographic keys.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
			Cryptographic Keys	
FCS_STG_EXT.3	**Key Integrity Protection**	SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE has the ability to securely store cryptographic keys.
		SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE uses cryptographic methods to ensure the integrity of stored data.
FDP_ITC_EXT.1	**Key/Credential Import**	SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to manage and import cryptographic keys.
		SC-16(1)	**Transmission of Security and Privacy Attributes:** Integrity Verification	A conformant TOE has the ability to verify the integrity of imported keys during transmission.
FIA_AFL_EXT.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_PMG_EXT.1	**Password Management**	IA-5(1)	**Authenticator Management:** Password-Based Authentication	A conformant TOE will have the ability to enforce some minimum password complexity requirements, to those specified in part (h) of this control.
FIA_UAU.5	**Multiple Authentication Mechanisms**	IA-2	**Identification and Authentication**	A conformant TOE will require user identification and authentication before

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
			(Organizational Users)	permitting access to the TSF.
		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.
		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.
FIA_UAU.7	**Protected Authentication Feedback**	IA-6	**Authentication Feedback**	The TOE is required to provide obscured feedback to the user while authentication is in progress.
FIA_UIA_EXT.1	**Administrator Identification and Authentication**	AC-3	**Access Enforcement**	A conformant TOE will implement an access control policy that
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE has the ability to require that certain functions require successful authentication to access.
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.
		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

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				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**	CM-14	**Signed Components**	**(selection-dependent)** A conformant TOE may support this control by requiring the use of X.509 certificates for update integrity verification, depending on selections made.
		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**	**(selection-dependent)** A conformant TOE may

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
			Authentication: Cryptographic Bidirectional Authentication	support this control if the TSF uses X.509 authentication for a trusted channel that requires client authentication, such as mutually-authenticated TLS.
		SI-7(15)	**Software, Firmware, and Information Integrity:** Code Authentication	**(selection-dependent)** A conformant TOE may use X.509 certificates to authenticate software updates to the TOE, depending on selections made.
FPT_JTA_EXT.2	**JTAG/Debug Port Disablement**	SI-16	**Memory Protection**	A conformant TOE supports this control by preventing unauthorized access to system memory through a JTAG interface.
FPT_PHP.1	**Passive Detection of Physical Attack**	PE-3(5)	**Physical Access Control:** Tamper Protection	A conformant TOE detects physical tampering that might compromise the TSF.
		SR-9	**Tamper Resistance and Detection**	A conformant TOE detects physical tampering that might compromise the TSF.
FPT_PHP.2	**Notification of Physical Attack**	SI-4(5)	**System Monitoring:** System Generated Alerts	A conformant TOE notifies organizational defined roles in the event of detection of physical tampering.
		SR-9	**Tamper Resistance and Detection**	A conformant TOE detects physical tampering that might compromise the TSF.
FPT_PHP.3	**Resistance to Physical Attack**	PE-3(5)	**Physical Access Control:** Tamper Protection	A conformant TOE detects physical tampering that might compromise the TSF.
		SR-9	**Tamper Resistance and Detection**	A conformant TOE detects physical tampering that might compromise the TSF.
FPT_RVR_EXT.1	**Platform Firmware Recovery**	CM-2(3)	**Baseline Configuration:** Retention of Previous Configurations	A conformant TOE may retain previous firmware versions that can be used to revert to the prior firmware image in the

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				event of a boot firmware failure.
		SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE has the ability to verify the integrity of updates to itself.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE has the ability to verify the integrity of updates to itself.
FPT_TUD_EXT.2	**Platform Firmware Authenticated Update Mechanism**	CM-14	**Signed Components**	A conformant TOE has the ability to authenticate the source of all platform firmware updates using a digital signature algorithm.
		SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE has the ability to verify the integrity of updates to itself.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE has the ability to verify the integrity of updates to itself.
		SI-7(5)	**Software, Firmware, and Information Integrity:** Automated Response to Integrity Violations	A conformant TOE may ability to halt the installation and notify an authorized user in the event of a platform firmware integrity detection.
FPT_TUD_EXT.3	**Platform Firmware Delayed-Authentication Update Mechanism**	CM-14	**Signed Components**	A conformant TOE has the ability to authenticate the source of all platform firmware updates using a digital signature algorithm.
		SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE has the ability to verify the integrity of updates to itself.
		SI-7(1)	**Software, Firmware, and Information**	A conformant TOE has the ability to verify the integrity of updates to itself.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
			Integrity: Integrity Checks	
		SI-7(5)	**Software, Firmware, and Information Integrity:** Automated Response to Integrity Violations	A conformant TOE may ability to halt the installation and notify an authorized user in the event of a platform firmware integrity detection.
FPT_TUD_EXT.4	**Secure Local Platform Firmware Update Mechanism**	N/A	**N/A**	This SFR restricts TSF updates to local interfaces only. There is no control that explicitly limits the logical functionality of a system based on the physical interface used to access it.
FTP_ITC_EXT.1	**Trusted Channel Communication**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	Depending on the cryptographic protocols used to implement the claimed SFR, a conformant TOE may be able to 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 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_ITE_EXT.1	**Encrypted Data Communications**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A conformant TOE supports this control by requiring a remote entity to be authenticated through the use of a shared secret.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
		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 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_ITP_EXT.1	**Physically Protected Channel**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE implements functionality to protect data in transit.
FTP_TRP.1	**Trusted Path**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	Depending on the cryptographic protocols used to implement the claimed SFR, a conformant TOE may be able to perform mutual authentication with trusted remote entities.
		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.