Mapping Between

PP-Module for MACsec Ethernet Encryption, Version 1.0, 2023-03-02

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 or 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 certain controls, but typically satisfaction also requires the implementation of operational procedures. Further, given that systems are typically the product of the 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 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; in particular, it is important not to read more into an SFR to control mapping than a contribution of some level of support.
- **SC-8 and SC-13.** The primary purpose of a MACsec product is to establish a point-to-point Layer 2 connection that uses MACsec for protection of data in transit. Therefore, this supports the enforcement of SC-8 at a high level, and SC-8(1) and SC-13 more specifically because the data protection mechanism uses encryption to ensure confidentiality. Individual SFRs may relate to other security controls to ensure the secure implementation of the functions that are performed in support of this, but the reader should be aware that SC-8 and relevant sub-controls are the behaviors that MACsec is intended to address.
- **SA-4(7).** Generally, satisfaction of any NIAP PP or PP-Configuration 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 implement trusted communications for MACsec, supports SC-8 and related controls for those interfaces only; it cannot enforce protection of data in transit for non-TLS protocols that are outside of its own boundary.

- **PP-Module.** A TOE that conforms to this PP-Module will also conform to the collaborative Protection Profile for Network Devices (NDcPP) by definition. Therefore, the TOE will satisfy additional security controls not referenced here through its conformance to that PP. This PP-Module refines some of the NDcPP requirements to ensure consistency between the 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
Mandatory Requirements (presented alphabetically)				
FAU_GEN.1/MACSEC	**Audit Data Generation (MACsec)**	AU-2	**Event Logging**	A conformant TOE can 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 can generate audit logs, as well as control which events are logged, satisfying this control.
FCS_COP.1/CMAC	**Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)**	SC-13	**Cryptographic Protection**	A conformant TOE can perform AES-CMAC using NSA-approved and FIPS-validated algorithms.
FCS_COP.1/MACSEC	**Cryptographic Operation (MACsec AES Data Encryption and Decryption)**	SC-13	**Cryptographic Protection**	A conformant TOE can perform AES functionality for MACsec using NSA-approved and FIPS-validated algorithms.
FCS_MACSEC_EXT.1	**MACsec**	IA-3	**Device Identification and Authentication**	A conformant TOE supports this control by using a remote peer's MAC address as a device identifier when establishing a MACsec connection.
		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	A conformant TOE supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	A conformant 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

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				organizational requirements.
FCS_MACSEC_EXT.2	**MACsec Integrity and Confidentiality**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE provides integrity protection for transmitted data.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE implements a cryptographic mechanism to ensure the integrity of data in transit.
		SC-13	**Cryptographic Protection**	A conformant TOE implements a cryptographic mechanism to ensure the integrity of data in transit.
FCS_MACSEC_EXT.3	**MACsec Randomness**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE uses a suitable mechanism to generate unique cryptographic keys.
FCS_MACSEC_EXT.4	**MACsec Key Usage**	IA-3	**Device Identification and Authentication**	A conformant TOE supports this control by implementing a mechanism to authenticate MACsec peers.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE implements a lifetime mechanism for generated keys as well as appropriate mechanisms for key distribution.
FCS_MKA_EXT.1	**MACsec Key Agreement**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports this control by implementing a defined mechanism for key agreement.
FIA_PSK_EXT.1	**Pre-Shared Key Composition**	IA-3	**Device Identification and Authentication**	A conformant TOE supports this control by using a pre-shared key to authenticate a remote MACsec peer.
FMT_SMF.1/MACSEC	**Specification of Management Functions (MACsec)**	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

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				configure its behavior in accordance with organizational requirements. Specific additional controls may be supported depending on the functionality claimed by the TOE.
FPT_CAK_EXT.1	**Protection of CAK Data**	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.
		IA-5	**Authenticator Management**	A conformant TOE protects CAK data (considered to be authentication data due to its role in identifying itself to a peer device) from unauthorized disclosure, in support of part (g) of this control.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the enforcement of this control by protecting stored cryptographic data.
FPT_FLS.1	**Failure with Preservation of Secure State**	SC-24	**Fail in Known State**	A conformant TOE supports this control by failing in a known state when any of the failures identified in the SFR occur.
FPT_RPL.1	**Replay Detection**	SC-23	**Session Authenticity**	A conformant TOE supports this control by detecting attempted reuse of MACsec data to illicitly impersonate a valid session.
FTP_ITC.1/MACSEC	**Inter-TSF Trusted Channel (MACsec Communications)**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A conformant TOE supports the enforcement of this control because MACsec requires the use of mutual authentication.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE can ensure the confidentiality and integrity of information transmitted between the

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				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.
Optional Requirements (presented alphabetically)				
FIA_AFL_EXT.1	**Authentication Attempt Limiting**	AC-7	**Unsuccessful Logon Attempts**	A conformant TOE supports this control in a limited manner by enforcing rate limiting on authentication attempts once a certain number of invalid attempts have been made. This qualifies as an "other organization-defined action" in part (b) of the control because the SFR requires the TSF to implement this function using a static algorithm rather than an "organization-defined delay algorithm" specified in the control.
FPT_DDP_EXT.1	**Data Delay Protection**	SC-23	**Session Authenticity**	A conformant TOE supports this control by using data delay protection as a mechanism to detect replayed traffic.
FPT_RPL_EXT.1	**Replay Protection for XPN**	SC-23	**Session Authenticity**	A conformant TOE supports this control by using extended packet numbering as a mechanism to detect replayed traffic.
FTP_TRP.1/MACSEC	**Trusted Path (MACsec Administration)**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A conformant TOE may support the enforcement of this control if the protocols used to establish trusted communications uses mutual authentication.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE can prevent unauthorized disclosure of information and detect modification to that information.

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		SC-11	**Trusted Path**	The TOE establishes a trusted communication path between remote users and itself.
Objective Requirements (presented alphabetically)				
This PP-Module has no objective requirements.				
Implementation-Based Requirements (presented alphabetically)				
This PP-Module has no implementation-based requirements.				
Selection-Based Requirements (presented alphabetically)				
FCS_DEVID_EXT.1	**Secure Device Identifiers**	IA-3	**Device Identification and Authentication**	A conformant TOE supports this control by implementing DevIDs as a mechanism used to identify and authenticate MACsec peers.
		IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE implicitly supports this control because 802.1AR DevIDs are based on X.509 certificates.
FCS_EAP-TLS_EXT.1	**EAP-TLS Protocol**	IA-3	**Device Identification and Authentication**	A conformant TOE supports this control by implementing EAP-TLS using DevIDs as a device authentication for MACsec.
FCS_SNMP_EXT.1	**SNMP Protocol**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A conformant TOE may support the enforcement of this control if the SNMP protocol implementation used to establish trusted communications uses mutual authentication.
		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.
FMT_SNMP_EXT.1	**SNMP Management**	IA-5(1)	**Authenticator Management:**	A conformant TOE can enforce some minimum

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			Password-Based Authentication	password complexity requirements for SNMP authentication, although they are not identical to CNSS or DoD requirements or to those specified in part (a) of this control.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE can prevent unauthorized disclosure of information and detect modification to that information.
		SC-11	**Trusted Path**	The TOE establishes a trusted communication path between remote users and itself.