# Mapping Between

# Network Device Collaborative Protection Profile (NDcPP) Extended Package MACsec Ethernet Encryption, Version 1.2, 2016-05-10

# 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.
- **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. This therefore 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).** Perhaps it is needless to say, but 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 on its TLS proxy interfaces 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.
- **Extended Package.** A TOE that conforms to this extended package 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. The additional requirements added by the extended package This extended package refines some of the NDcPP requirements to ensure consistency between the PP and the extended package, but this does not affect the security controls that satisfying those requirements is intended to address.

| Common Criteria Version 3.x SFR | | NIST SP 800-53 Revision 5 Control Supports | | Comments and Observations |
|---|---|---|---|---|
| **TOE Security Functional Requirements** | | | | |
| 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 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 | 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 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. |

| Common Criteria Version 3.x SFR | | NIST SP 800-53 Revision 5 Control Supports | | Comments and Observations |
|---|---|---|---|---|
| | | 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_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 occurs and take some corrective action. |
| FIA_PSK_EXT.1 | **Extended: 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. |
| 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(2)/SelfTest | **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** | AU-2 | **Event Logging** | A conformant TOE supports this control by ensuring that replay attempts are logged. |

| Common Criteria Version 3.x SFR | | NIST SP 800-53 Revision 5 Control Supports | | Comments and Observations |
|---|---|---|---|---|
| | | SC-23 | **Session Authenticity** | A conformant TOE supports this control by detecting attempted reuse of MACsec data to illicitly impersonate a valid session. |
| **Optional Requirements** | | | | |
| FIA_AFL_EXT.1 | **Extended: 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_RPL_EXT.1 | **Extended: Replay Detection for XPN** | SC-23 | **Session Authenticity** | A conformant TOE supports this control by using extended packet numbering as a mechanism to detect replayed traffic. |
| **Selection-Based Requirements** | | | | |
| FMT_SNMP_EXT.1 | **SNMP Management** | IA-5(1) | **Authenticator Management:** Password-Based Authentication | A conformant TOE will have the ability to enforce some minimum 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 will have the ability to 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. |

| Common Criteria Version 3.x SFR | | NIST SP 800-53 Revision 5 Control Supports | | Comments and Observations |
|---|---|---|---|---|
| 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_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. |
| **Objective Requirements** | | | | |
| This EP has no objective requirements. | | | | |