Mapping Between

Extended Package for Wireless Local Area Network (WLAN) Clients, Version 1.0, 08-February-2016

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.
- **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.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 4 Control Supports**		**Comments and Observations**
FAU_GEN.1/ WLAN Note: this SFR definition merely adds new auditable events to the existing SFR that is defined by the Base-PP.	**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.
FCS_CKM.1/WLAN	**Cryptographic Key Generation:** Symmetric Keys for WPA2 Connections	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE provides a key generation function in support of the key lifecycle process.
		SC-12(2)	**Cryptographic Key Establishment and Management:** Symmetric Keys	The TOE will implement the key generation function using symmetric keys.
FCS_CKM.2/ WLAN	**Cryptographic Key Distribution:** GTK	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will decrypt and use GTKs in a manner that does not subject them to unauthorized disclosure.
FCS_TLSC_EXT.1/ WLAN	**Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)**	AC-18(1)	**Wireless Access:** Authentication and Encryption	A conformant TOE encrypts wireless communications using TLS encryption.
		IA-5(2)	**Authenticator Management:** PKI-Based Authentication	A conformant TOE provides the ability to configure the authorized CAs that can be used, which supports the "accepted trust anchor" portion of the control.
		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's use of SSH supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	A conformant TOE's implementation used to establish TLS communications supports this control if

				the control's assignment defines the cryptography implemented by the TSF as appropriate for the information system.
FIA_PAE_EXT.1	**Port Access Entity Authentication**	AC-18	**Wireless Access**	A conformant TOE supports the authentication aspect of this control by performing user authentication.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE supports the implementation of this control by identifying and authenticating users prior to establishing a wireless connection.
FIA_X509_EXT.2/WLAN	**X.509 Certificate Authentication:** EAP-TLS	AC-18(1)	**Wireless Access:** Authentication and Encryption	A conformant TOE supports the authentication aspect of this control by requiring X.509 certificate authentication.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE will support this control by requiring users to present X.509 certificates in order to authenticate themselves prior to establishing EAP-TLS communications.
FMT_SMF_EXT.1/ WLAN	**Specification of Management Functions:** Wireless LAN	AC-18	**Wireless Access**	A conformant TOE provides the ability to configure the security policy for wireless network communications, which supports this control by providing an interface to limit connectivity to authorized networks.

		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 STIGs or other organizational requirements. Specific additional controls may be supported depending on the functionality claimed by the TOE; the security control assessor must review what has been selected in the Security Target and determine what additional support is provided, if any.
FPT_TST_EXT.1/WLAN	**TSF Cryptographic Functionality Testing:** Wireless LAN	SI-6	**Security Function Verification**	A conformant TOE has the ability to shut down or restart in the event of a self-test failure.
		SI-7(1)	**Software, Firmware and Information Integrity:** Integrity Checks	The TOE has the ability to verify the integrity of TOE executable code.
		SI-7(6)	**Software, Firmware and Information Integrity:** Cryptographically-Validated Integrity	A conformant TOE has the ability to implement cryptographic mechanisms to detect unauthorized change.
FTA_WSE_EXT.1	**Wireless Network Access**	AC-18	**Wireless Access**	A conformant TOE provides the ability to ensure that only connections to authorized wireless

				networks can be performed.
FTP_ITC_EXT.1/WLAN	**Trusted Channel Communication:** Wireless LAN	AC-18(1)	**Wireless Access:** Authentication and Encryption	A conformant TOE uses 802.1X for authentication and EAP-TLS to encrypt wireless data in transit.
Security Functional Requirements – OS PP Base				
FCS_CKM_EXT.3	**Cryptographic Key Destruction**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to destroy keys when appropriate in order to conform to organizational policy and standards.
Security Functional Requirements – MDF PP Base				
FCS_CKM_EXT.4	**Key Destruction**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to destroy keys when appropriate in order to conform to organizational policy and standards.
Optional Requirements				
FIA_X509_EXT.4	**Certificate Storage and Management**	AC-18(1)	**Wireless Access:** Authentication and Encryption	A conformant TOE can store certificates which are used in support of enforcing authentication on wireless access.
		IA-5	**Authenticator Management**	A conformant TOE has the ability to store certificates in a way that prevents from unauthorized modification or disclosure.
		IA-5(2)	**Authenticator Management:** PKI-Based Authentication	A conformant TOE supports part (b) of this sub-control by limiting access to certificate (private key) data.
Selection-based Requirements				

FCS_TLSC_EXT.2/ WLAN	**TLS Client Protocol**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to limit the elliptic curves that can be used for key establishment.
Objective Requirements				
N/A	**N/A**	**N/A**	**N/A**	**N/A**