Protection Profile for Wireless Local Area Network (WLAN) Clients

Information Assurance Directorate

19 December 2011

Version 1.0

Table of Contents

List of Tables

List of Figures

Revision History

Version	Date	Description
1.0	December 2011	Initial release

1 Introduction to the PP

1 This Protection Profile (PP) supports procurements of commercial off-the-shelf (COTS) Wireless Local Area Network (WLAN) Clients for the protection of sensitive but unclassified data on a wireless network. This PP details the policies, assumptions, threats, security objectives, security functional requirements, and security assurance requirements for the WLAN and its supporting environment.

2 The primary intent is to clearly communicate to developers our understanding of the Security Functional Requirements needed to counter the threats that are being addressed by the WLAN Client. The description in the TOE Summary Specification (TSS) of the ST is expected to document the architecture of the product (Target of Evaluation) and the mechanisms used to ensure that critical security transactions are correctly implemented.

1.1 PP Overview of the TOE

3 This document specifies Security Functional Requirements for a WLAN Client. The TOE defined by this PP is the WLAN Client, a component executing on a client machine (often referred to as a "remote access client"). The TOE establishes a secure wireless tunnel between the client device and a WLAN Access System through which all data will traverse. The WLAN Access System ensures that only authorized clients obtain this access through authentication with an Authentication Server. For the purpose of this PP a typical wireless to wired network configuration is discussed. However the intent is not to preclude any other wireless configuration that may exist and meet the requirements in this PP. This PP does not dictate any particular configuration. Instead the PP addresses the security requirements for the client that provides communication between the wireless user and the wired network and its resources. As discussed in the following sections, it is important to stress that the PP covers the functionality of the WLAN client and its administrative capabilities only; it does not levy requirements that will be implemented in the IT environment such as Identification and Authentication, Audit Storage, etc. These capabilities should conform to requirements specified for general purpose operating systems, for example.

4 The WLAN Client supports IEEE 802.1X Port Based Network Access Control. The architectural framework of Port-based access control defines three distinct roles: Supplicant (the TOE), Authenticator (WLAN Access System); and Authentication Server (AS). The WLAN Access System requires successful authentication of the TOE, relying on the AS to authenticate the TOE, before providing network access. The WLAN Access System acts as a pass through device between the TOE and the AS. The WLAN Access System allows the WLAN Client access to the private network only after it has been successfully authenticated by the AS. The TOE and AS must perform mutual machine authentication using X.509 v3 certificates and Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) messages. If either the TOE or AS fail to authenticate, the WLAN Access System ceases to communicate with the WLAN Client. Secure communication tunnels to the private network can only be established if authentication is successful.

1.1.1 Usage and major security features of TOE

5 A WLAN Client allows remote users to use client machines to establish wireless communication with a private network. IP packets passing between the private network and a remote access WLAN Client are encrypted. The WLAN Client protects the data between itself and the private network, providing confidentiality, integrity, and protection of data in transit, even though it traverses a wireless connection.

6 The focus of the Security Functional Requirements in this PP is on the following fundamental aspects of a WLAN Client:

- Authentication of the WLAN Client;
- Authentication of the Authentication Server;
- Cryptographic protection of data in transit; and
- Implementation of services.

7 The WLAN Client establishes an 802.11 tunnel between the client device and the network infrastructure using IEEE 802.1X with EAP-TLS for authentication. It performs mutual authentication to an AS in the private network as part of the EAP-TLS exchange. The EAP-TLS exchange uses machine certificates for mutual authentication. The WLAN Client examines the machine certificate transmitted from the AS, checks its validity, and ensures the certificate is signed by a trusted Certificate Authority (CA). The AS will authenticate the WLAN Client certificate at the same time. When the EAP-TLS exchange completes successfully, the network allows the WLAN Client to finish establishing a secure communication tunnel to the private network. The WLAN Client sets up an encrypted, authenticated channel to the WLAN Access System using a 4 way handshake, as specified in IEEE 802.11. Once the channel is established, all communication between the WLAN Client to the WLAN Access System is encrypted with AES in CCMP mode, as specified in IEEE 802.11.

8 The WLAN Client (Figure 1), as defined by this PP, is a component executing on a remote access client machine. Note the client is depicted as just a small portion of the WLAN client "machine." As such, the TOE must rely heavily on the TOE's operational environment (host platform, network stack, and operating system) for its execution domain and its proper usage. The TOE will rely on the IT environment to address much of the security functionality related to administrative functions.

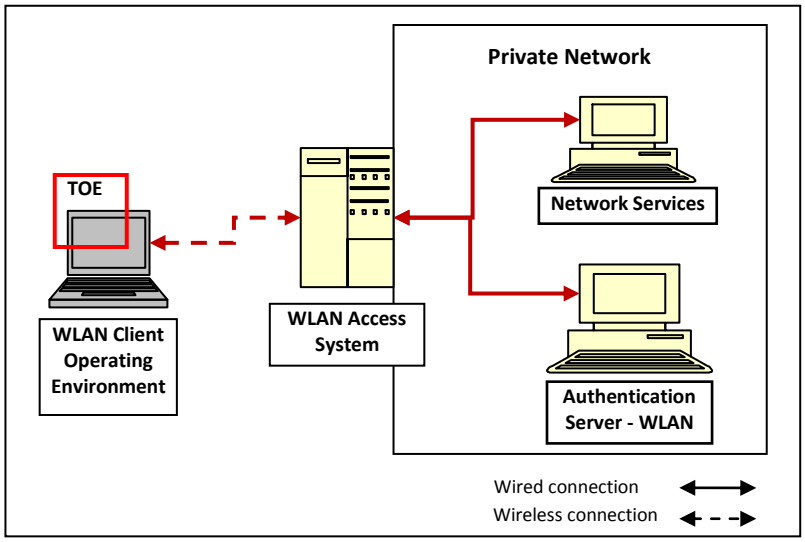

Figure 1: WLAN Client

9 It is assumed that the WLAN Client is implemented properly and contains no critical design mistakes. The security features of the TOE include administration, protocol compliance, cryptographic protection, and audit generation. The WLAN Client relies on the IT environment for its proper execution as well as the following client machine protection mechanisms: audit review, audit storage, identification and

authentication, security management, and session management. The vendor is required to provide configuration guidance (AGD_PRE, AGD_OPE) to correctly install and administer the client machine and the TOE for every operational environment supported.

1.1.2 Cryptography

10 The WLAN Client relies on cryptographic functionality to provide confidentiality, integrity, and protection of data in transit. The WLAN Client is expected to encrypt wireless traffic flowing between two devices that are geographically separated. The WLAN Client serves as an endpoint for a WLAN tunnel and performs a number of cryptographic functions related to establishing and maintaining the tunnel. Through the use of standard protocols and algorithms, the WLAN Client ensures that each message is secure even when traversing the wireless network. The Advanced Encryption Standard (AES) algorithm in CCMP mode is used to protect the data in transit. CCMP mode is based on two block cipher modes in combination - Counter Mode provides confidentiality and the Cipher Block Chaining Message Authentication Code (CBC-MAC) provides integrity of the data.

11 If the cryptography used to authenticate, generate keys, and encrypt information is sufficiently robust and the implementation has no critical design mistakes, an adversary will be unable to exhaust the encryption key space to obtain the wireless data. Compliance with WPA2 as specified in IEEE802.11 and the IEEE802.1X standards, a properly seeded Random Bit Generator (RBG), and secure authentication factors will ensure that access to the transmitted information cannot be obtained with less work than a full exhaust of the key space. Any plaintext secret and private keys or other cryptographic security parameters will be zeroized when no longer in use to prevent disclosure of security critical data.

1.1.3 TOE Administration and the IT Environment

12 The TOE supporting environment is significant. The TOE in almost all cases will be a purely a software solution executing on a general purpose operating system. As such, the TOE must rely heavily on the TOE Operational environment (system hardware, firmware, and operating system) for its execution domain and its proper usage. The vendor is expected to provide sufficient installation and configuration instructions to identify an Operational environment with the necessary features and to provide instructions for how to configure it correctly.

13 The TOE requires that certain management activities (defined in the requirements) be performed by a subset of the authorized users of the TOE. This PP places no requirements on the TOE to provide an identification and authentication capability to restrict these management functions to an administrative role, which implies that there are a number of ways a TOE vendor could be compliant. For example,

1. The TOE contains no notion of an authorized administrator; anyone that can invoke the management utility can configure the TOE. In order to be compliant to the PP in this case, the TOE vendor must provide instructions as part of the AGD_OPE/PRE guidance that detail the procedures an administrator would use to configure the Operational environment such that only a subset of the authorized users of the TOE would be able to execute the management utility. For example, the guidance would describe configuring the access control mechanisms in the Operational environment so that only the administrator-allowed users would be able to execute the management utility. This case reflects the baseline requirements of this PP.
2. The TOE contains a notion of an authorized administrator (or set of administrators), but relies on the Operational environment to perform the identification and authentication functions and then pass some indication to the TOE that can be matched to the internal TOE representation of an authorized administrator. In this case, the ST author will need augment the requirements

(using the templates provided in Appendix C) to specify the capabilities provided by the TOE. The vendor will need to describe any configuration or settings in the Operational environment needed to support the passing of the information to the TOE.

3. The TOE contains its own identification and authentication capability that is used to determine which users of the system housing the hard disk are authorized to use the management functions provided by the TOE. In this case, the ST author will need to use the I&A template information provided in Appendix C in the body of the ST to specify this functionality.

1.1.4 Protocol Compliance

14 The TOEs meeting this PP shall meet the requirements for Wi-Fi Protected Access 2 (WPA2). Specifically the TOE will use Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP), as defined in the WPA2 standard. IEEE 802.1X is used for port-based access control; the client is expected to authenticate with Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) mutual authentication between the wireless client and authentication server. The EAP-TLS protocol is configured to use X.509 v3 certificates as specified in RFC 5216.

2 Security Problem Definition

15 This PP is written to address the situation when an entity desires wireless access to a private network. To allow access to the private network, the entity (machine) must be authenticated before a secure communications channel can be established. The TOE is the entity that seeks to be authenticated and be given access to services offered by the protected network and is the Supplicant in the IEEE 802.1X framework.

16 The proper installation and configuration of the WLAN Client are critical to its correct operation such that proper handling of the TOE by an administrator is also addressed.

17 This chapter identifies the following:

- IT related threats to the organization countered by the WLAN Client;
- Environmental threats requiring controls to provide sufficient protection;
- Organizational security policies for the WLAN Client as appropriate; and
- Significant assumptions about the WLAN Client's operational environment.

2.1 Threats

18 This PP does not include requirements that can protect against an insider threat. Authorized users are not considered hostile or malicious and are trusted to follow appropriate guidance. Only authorized personnel should have access to the client device. Therefore, the primary threat agents addressed by the requirements in this PP are the unauthorized entities that try to gain access to the protected network. An entity is authorized if they can authenticate themselves to the network thus establishing themselves as legitimate users of the network. Because the request for network access by a legitimate entity and passing authentication credentials is done over a wireless network, it is subject to attacks and must be protected from disclosure and modification. A malicious entity could masquerade as a legitimate WLAN Access System, for example, resulting in the compromise of client data and authentication credentials.

19 Use of wireless communications introduces new attack vectors into a network; adversaries can launch wireless attacks without breaching the confines of the protected facility or obtaining access to the client device. Signal jamming and denial of service attacks are common and hard to prevent. Assumptions on the availability of the network are in place to address these threats since they are not covered by the requirements in this PP. However, other mechanisms can be used to protect wireless communication. Improper negotiation of security policies or enforcing weak protocol options to establish a wireless connection is a concern that could result in the disclosure or modification of user and TSF data. While it is impossible to prevent an adversary from "sniffing" wireless traffic, protocol interoperability and mutual agreed upon security policies requiring strong encryption are imperative for establishing wireless LAN protection.

20 Other threat agents include security related information that is not cleared when resources are reallocated; when sensitive values are no longer needed, access to this data must be prevented. The TOE must ensure that residual data is appropriately handled such that security related information is not accessible by other users/processes after it is used. Compromise of TSF data includes authentication

data, session keys, role/user information, security mechanisms, and the data the TOE protects. TOE or TSF data must be protected from inappropriate access and updates.

21 Network attacks, such as that described above against the TOE, are not the sole avenue for gaining unauthorized access and compromising security. Updating products is a common and necessary capability to ensure that changes to the threat environment are addressed; a common attack vector used involves attacking un-patched versions of software containing flaws. Timely application of patches increases the likelihood that the product will be able to maintain and enforce its security policy. However, the updates must be from a trusted source; otherwise, an attacker can write their own "update" that contains malicious code of their choosing, such as a rootkit, bot, or other malware.

22 Once an adversary has access, regardless of the mechanism used to obtain it (network attacks, malicious code, taking advantage of errors in configuration, session hijacking, etc.), the TOE and its data have been compromised. Modification of audit record generation to hide any further nefarious actions taken on the TOE could mask potential problems as well as make it difficult to identify who caused the malicious action. Undetected actions may adversely affect the security of the TOE and may make it difficult to mitigate the problems caused. Note that audit review and storage are handled by the IT environment and are therefore outside the scope of this PP. However, it is assumed that this is done properly and securely to protect the TOE.

23 The following table lists the threats addressed by the WLAN Client and the operational environment. The assumed level of expertise of the attacker for all the threats identified below is unsophisticated.

Table 1: Threats

Threat	Description of Threat
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

2.2 Organizational Security Policies

24 The Organization Security Policies were selected because of their applicability to protect network packets crossing the boundary between a private network and a public network. The policies relating to

procedures are also stated as assumptions. Those policies that do not have a formal reference are expected to be created and formalized subject to the policy description.

Table 2: Organizational Security Policies

Policy	Policy Description
P.COMPATIBILITY	The TOE must meet Request for Comments (RFC) requirements for implemented protocols to facilitate inter-operability- with other network equipment using the same protocols.
P.CONFIGURABILITY	The TOE must provide the capability to configure security-relevant aspects of its operation.

2.3 Assumptions

25 This section of the security problem definition shows the assumptions that are made on the operational environment in order to be able to provide security functionality. If the TOE is placed in an operational environment that does not meet these assumptions, the TOE may no longer be able to provide all of its security functionality. Assumptions can be on the physical environment, personnel and connectivity of the operational environment.

Table 3: TOE Assumptions

Assumption	Description of Assumption
A.NO_TOE_BYPASS	Information cannot flow between the wireless client and the internal wired network without passing through the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

3 Security Objectives

26 The Security Objectives are the requirements for the Target of Evaluation (TOE) and for the Operational Environment derived from the threats, organizational security policies, and the assumptions in Section 2. Section 4 restates the security objectives for the TOE more formally as SFRs. The TOE is evaluated against the SFRs.

3.1 Security Objectives for the TOE

27 Table 4 identifies the Security Objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified. The TOE meets these objectives by satisfying the security functional requirements.

Table 4: Security Objectives for the TOE

Objective	Objective Description
O.AUTH_COMM	The TOE will provide a means to ensure that it is communicating with an authorized Access Point and not some other entity pretending to be an authorized Access Point, and will provide assurance to the Access Point of its identity.
O.CRYPTOGRAPHIC_FUNCTIONS	The TOE shall provide cryptographic functions (i.e., encryption/decryption and digital signature operations) to maintain the confidentiality and allow for detection of modification of data that are transmitted outside the TOE and its host environment.
O.PROTOCOLS	The TOE will ensure that standardized protocols are implemented in the TOE to RFC and/or industry specifications to ensure interoperability.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to allow administrators to be able to configure the TOE.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
O.WIRELESS_ACCESS_POINT_CONNECTION	The TOE will provide the capability to restrict the wireless access points to which is will connect.

3.2 Security Objectives for the Operational Environment

28 The Operational Environment of the TOE implements technical and procedural measures to assist the TOE in correctly providing its security functionality (which is defined by the security objectives for the

TOE). This part-wise solution is called the security objectives for the operational environment and consists of a set of statements describing the goals that the operational environment should achieve.

29 This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means. The assumptions identified in Section 2.3 are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures. Table 5 identifies the security objectives for the environment.

Table 5: Security Objectives for the operational environment

Objective	Objective Description
OE.NO_TOE_BYPASS	Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the operational environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

3.3 Security Objective Rationale

30 This section describes the rationale for the Security Objectives as defined in Section 2. Table 6 illustrates the mapping from Security Objectives to Threats and Policies.

Table 6: Security Objectives to Threats and Policies Mappings

Threat/Policy	Objectives Addressing the Threat and Policies	Rationale
T.TSF_FAILURE Security mechanisms of the TOE may fail, leading to a compromise of the TSF.	O.TSF_SELF_TEST The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.	O. TSF_SELF_TEST counters this threat by ensuring that the TSF runs a suite of self tests to successfully demonstrate the correct operation of the TSF.
T.UNAUTHORIZED_ACCESS A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.	O.AUTH_COMM The TOE will provide a means to ensure that it is communicating with an authorized Access Point and not some other entity pretending to be an authorized Access Point, and will provide assurance to the Access Point of its identity. O.CRYPTOGRAPHIC_FUNCTIONS The TOE shall provide cryptographic functions (i.e., encryption/ decryption and digital signature operations) to maintain the confidentiality and allow for detection of modification of TSF data that is transmitted between physically separated portions of the TOE, or stored outside the TOE. O.TOE_ADMINISTRATION The TOE will provide mechanisms to allow administrators to be able to configure the TOE. O.WIRELESS_ACCESS_POINT_ CONNECTION The TOE will provide the capability to restrict the wireless access points to which it will connect.	O.AUTH_COMM works to mitigate this threat by ensuring that the TOE identifies and authenticates all access points prior to communicating with that access point. The TOE must also be capable of sending its own credentials to access points to ensure mutual authentication prior to communication. O.CRYPTOGRAPHIC_FUNCTIONS contributes to mitigating this threat by providing the underlying cryptographic functionality required by other protection mechanisms. O.TOE_ADMINISTRATION requires the TOE to provide mechanisms to allow the TOE to be configured in a secure manner. O.WIRELESS_ACCESS_POINT_ CONNECTION mitigates the threat by providing mechanisms to restrict the access points to which the TOE can connect.
T.UNAUTHORIZED_UPDATE A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.	O.VERIFIABLE_UPDATES The TOE will provide the capability to ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.	O.VERIFIABLE_UPDATES ensures that the administrator can confirm the update

Threat/Policy	Objectives Addressing the Threat and Policies	Rationale
T.UNDETECTED_ACTIONS Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.	O.SYSTEM_MONITORING The TOE will provide the capability to generate audit data.	O.SYSTEM_MONITORING mitigates this threat by providing the administrator with the capability of configuring the audit mechanism to record actions based on a number of criteria.
T.USER_DATA_REUSE User data may be inadvertently sent to a destination not intended by the original sender.	O.RESIDUAL_INFORMATION_CLEARING The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.	O.RESIDUAL_INFORMATION_CLEARING counters this threat by ensuring that TSF data and user data is not persistent when resources are released by one user/process and allocated to another user/process.
P.COMPATIBILITY The TOE must meet Request for Comments (RFC) requirements for implemented protocols to facilitate inter-operation with other network equipment using the same protocols.	O.PROTOCOLS The TOE will ensure that standardized protocols are implemented in the TOE to RFC and/or Industry specifications to ensure interoperability, that also support communication with a centralized audit server and a RADIUS authentication server.	O.PROTOCOLS satisfies this policy by requiring that standardized protocols are implemented in the TOE to ensure interoperability among IT entities using the same protocols.
P.CONFIGURABILITY The TOE must provide the capability to configure security-relevant aspects of its operation.	O.TOE_ADMINISTRATION The TOE will provide mechanisms to allow administrators to be able to configure the TOE.	O.TOE_ADMINISTRATION satisfies the policy by ensuring that the TOE provides the mechanisms needed to security configure the TOE.

31 Table 7 illustrates the mapping from Security Objectives to Assumptions.

Table 7: Security Objectives to Assumptions Mappings

Assumption	Objectives Addressing the Assumption	Rationale
A.NO_TOE_BYPASS Information cannot flow between the wireless client and the internal wired network without passing through the TOE.	OE.NO_TOE_BYPASS Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.	OE.NO_TOE_BYPASS ensures that all information flow between external and internal networks in different enclaves passes through the TOE.
A.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be	OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the operational	OE.PHYSICAL ensures the TOE, the TSF data, and protected user data is protected from physical attack (e.g., theft, modification, destruction, or eavesdropping). Physical attack

Assumption	Objectives Addressing the Assumption	Rationale
provided by the environment.	environment.	could include unauthorized intruders into the TOE environment, but it does not include physical destructive actions that might be taken by an individual that is authorized to access the TOE environment.
A.TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.	OE.TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.	OE.TRUSTED_ADMIN ensures the administrators are properly trained and the administrative guidance instructs the administrator how to properly configure the environment and TOE to avoid mistakes.

4 Security Requirements and Rationale

32 The Security Requirements are divided into functional requirements and assurance requirements. The SFRs are a formal instantiation of the Security Objectives and are provided with application notes in Section 4.1. They are usually at a more detailed level of abstraction, but they have to be a complete translation (the security objectives must be completely addressed). The CC requires this translation into a standardized language for several reasons:

- To provide an exact description of what is to be evaluated. As security objectives for the TOE are usually formulated in natural language, translation into a standardized language enforces a more exact description of the functionality of the TOE.
- To allow comparison between two STs. As different ST authors may use different terminology in describing their security objectives, the standardized language enforces using the same terminology and concepts. This allows easy comparison.

33 The Security Assurance Requirements (SARs) are typically boilerplate that is inserted and listed separately from the SFRs; the Common Evaluation Methodology (CEM) is then consulted during the evaluation based on the SARs chosen. A more tailored approach is taken in this PP based on the new model for Standard Protection Profiles. While the SARs are still listed for context and completeness in Section 4.3, the activities that an evaluator needs to perform for this TOE with respect to each SFR and SAR are detailed in "Assurance Activities" paragraphs. Assurance Activities are normative descriptions of activities that must take place in order for the evaluation to be complete. Assurance Activities are located in two places in this PP; those that are associated with specific SFRs are located in Section 4.1, while those that are independent of the SFRs are detailed in Section 4.3.

34 For the activities associated directly with SFRs, after each SFR one or more Assurance Activities is listed detailing the activities that need to be performed to achieve the assurance provided for this technology.

35 For the SARs that require activities that are independent of the SFRs, Section 4.3 indicates the additional Assurance Activities that need to be accomplished, along with pointers to the SFRs for which specific Assurance Activities associated with the SAR have been written.

36 Future iterations of the Protection Profile may provide more detailed Assurance Activities based on lessons learned from actual product evaluations.

4.1 Security Functional Requirements

37 This section identifies the SFRs for the TOE that are specific to the security functionality provided by the TOE and distinguishes the WLAN Client from other TOEs. The focus areas of the SFRs are related to audit, cryptography, security management, self-tests, and communication with authorized external IT entities (e.g., WLAN Access System, Authentication Server).

Table 8: TOE Security Functional Requirements

Functional Class	Functional Components
Security Audit (FAU)	FAU_GEN.1 Audit Data Generation
	FAU_SEL.1 Selective Audit
Cryptographic support Class (FCS)	FCS_CKM.1 Cryptographic key generation (Symmetric Keys)
	FCS_CKM.2 Cryptographic Key Distribution (GTK)
	FCS_CKM_EXT.4 Cryptographic Key Zeroization
	FCS_COP.1(1) Cryptographic operation (Data Encryption/Decryption)
	FCS_COP.1(2) Cryptographic operation (Cryptographic Signature)
	FCS_COP.1(3) Cryptographic operation (Cryptographic Hashing)
	FCS_COP.1(4) Cryptographic Operation (Keyed-Hash Message Authentication)
	FCS_COP.1(5) Cryptographic operation (WPA2 Data Encryption/Decryption)
	FCS_EAP-TLS_EXT.1 Extended: Extensible Authentication Protocol-Transport Layer Security
	FCS_RBG_EXT.1 Extended: Cryptographic operation (Random Bit Generation)
User Data Protection Class (FDP)	FDP_RIP.2 Full residual information protection
Identification and Authentication Class (FIA)	FIA_8021X_EXT.1 Extended: 802.1X Port Access Entity (Supplicant) Authentication
	FIA_X509_EXT.1 Extended: X.509 Certificates
Security Management Class (FMT)	FMT_SMF.1 Specification of Management Functions
Protection of the TSF (FPT)	FPT_TST_EXT.1 Extended: TSF Testing
	FPT_TUD_EXT.1 Extended: Trusted Update
TOE Access (FTA)	FTA_ WSE_EXT.1 Extended: Wireless Session Establishment
Trusted Path/Channels (FTP)	FTP_ITC.1 Inter-TSF trusted channel

4.1.1 Class: Security Audit (FAU)

Security audit data generation (FAU_GEN)

FAU_GEN.1	**Audit Data Generation**
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the not specified level of audit; and c) *All* administrative actions; d) [*Specifically defined auditable events listed in Table 9*].

Application Note:

38 *The ST author can include other auditable events directly in the table; they are not limited to the list presented.*

39 *In the case of "a", the audit functions referred to are those provided by the TOE. For example, in the case that the TOE was a stand-alone executable, auditing the startup and the shutdown of the TOE itself would be sufficient to meet the requirements of this clause.*

40 *Many auditable aspects of the SFRs included in this document deal with administrative actions. Item c above requires all administrative actions to be auditable, so no additional specification of the auditability of these actions is present in Table 9. While the TOE itself does not need to provide the ability to perform I&A for an administrator, this requirement implies that the TOE possess the capability to audit the events described by the PP as "administrative actions" (primarily dealing with configuration of the functionality provided by the TOE). It is expected that the OPE guidance detail the steps needed to ensure the audit data generated by the TOE is integrated with the audit capabilities of the underlying IT environment.*

Assurance Activity:

41 *The evaluator shall check the operational guidance and ensure that it lists all of the auditable events and provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the PP is described and that the description of the fields contains the information required in FAU_GEN.1.2, and the additional information specified in Table 9.*

42 *The evaluator shall in particular ensure that the operational guidance is clear in relation to the contents for failed cryptographic events. In Table 9, information detailing the cryptographic mode of operation and a name or identifier for the object being encrypted is required. The evaluator shall ensure that name or identifier is sufficient to allow an administrator reviewing the audit log to determine the context of the cryptographic operation (for example, performed during a key negotiation exchange, performed when encrypting data for transit) as well as the non-TOE endpoint of the connection for cryptographic failures relating to communications with other IT systems.*

43 *The evaluator shall also make a determination of the administrative actions that are relevant in the context of this PP. The TOE may contain functionality that is not evaluated in the context of this PP because the functionality is not specified in an SFR. This functionality may have administrative aspects that are described in the operational guidance. Since such administrative actions will not be performed in an evaluated configuration of the TOE, the evaluator shall examine the operational guidance and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP, which thus form the set of "all administrative actions". The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements.*

44 *The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records in accordance with the assurance activities associated with the functional requirements in this PP. Additionally, the evaluator shall test that each administrative action applicable in the context of this PP is auditable. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries.*

45 *Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly. For example, testing performed to ensure that the administrative guidance*

provided is correct verifies that AGD_OPE.1 is satisfied and should address the invocation of the administrative actions that are needed to verify the audit records are generated as expected.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*information specified in column three of the table below*].

Application Note:

46 *As with the previous component, the ST author should update Table 9 with any additional information generated. "Subject identity" in the context of this requirement could either be the administrator's user id or the affected network interface, for example.*

Assurance Activity:

47 *This activity should be accomplished in conjunction with the testing of FAU_GEN.1.1.*

Table 9: Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	None.
FCS_CKM.1	Failure of the key generation activity.	None.
FCS_CKM.2	Failure of the key distribution activity.	None.
FCS_CKM_EXT.4	Failure of the key zeroization process.	Identity of object or entity being cleared.
FCS_COP.1(1)	Failure of encryption or decryption.	Cryptographic mode of operation, name/identifier of object being encrypted/decrypted.
FCS_COP.1(2)	Failure of cryptographic signature.	Cryptographic mode of operation, name/identifier of object being signed/verified.
FCS_COP.1(3)	Failure of hashing function.	Cryptographic mode of operation, name/identifier of object being hashed.
FCS_COP.1(4)	Failure in Cryptographic Hashing for Non-Data Integrity.	Cryptographic mode of operation, name/identifier of object being hashed.
FCS_COP.1(5)	Failure of WPA2 encryption or decryption.	Cryptographic mode of operation, name/identifier of object being encrypted/decrypted, non-TOE endpoint of connection (IP address).

Requirement	Auditable Events	Additional Audit Record Contents
FCS_EAP-TLS_EXT.1	Protocol failures. Authentication Failure.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_RBG_EXT.1	Failure of the randomization process.	None.
FDP_RIP.2	None.	
FIA_8021X_EXT.1	Attempts to access to the 802.1X controlled port.	Provided client identity (IP address).
FIA_X509_EXT.1	None.	
FMT_SMF.1	None.	
FPT_TST_EXT.1	Execution of this set of TSF self-tests. Detected integrity violations.	For integrity violations, the TSF code file that caused the integrity violation.
FPT_TUD_EXT.1	Initiation of the update. Any failure to verify the integrity of the update.	No additional information.
FTA_WSE_EXT.1	All attempts to connect to access points.	Identity of access point being connected to.
FTP_ITC.1	All attempts to establish a trusted channel. Detection of modification of channel data.	Identification of the non-TOE endpoint of the channel.

Security Audit Event Selection (FAU_SEL)

FAU_SEL.1 **Selective Audit**

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) event type;
b) success of auditable security events;
c) failure of auditable security events; and
d) [assignment: other attributes].

Application Note:

48 *The intent of this requirement is to identify all criteria that can be selected to trigger an audit event. For the ST author, the assignment is used to list any additional criteria or "none". The auditable event types are listed in Table 9.*

Assurance Activity:

49 *The evaluator shall review the administrative guidance to ensure that the guidance itemizes all event types, as well as describes all attributes that are to be selectable in accordance with the requirement, to include those attributes listed in the assignment. The administrative guidance shall also contain*

instructions on how to set the pre-selection, as well as explain the syntax (if present) for multi-value pre-selection. The administrative guidance shall also identify those audit records that are always recorded, regardless of the selection criteria currently being enforced.

50 *The evaluator shall also perform the following tests:*

- *Test 1: For each attribute listed in the requirement, the evaluator shall devise a test to show that selecting the attribute causes only audit events with that attribute (or those that are always recorded, as identified in the administrative guidance) to be recorded.*
- *Test 2 [conditional]: If the TSF supports specification of more complex audit pre-selection criteria (e.g., multiple attributes, logical expressions using attributes) then the evaluator shall devise tests showing that this capability is correctly implemented. The evaluator shall also, in the test plan, provide a short narrative justifying the set of tests as representative and sufficient to exercise the capability.*

4.1.2 Class: Cryptographic Support (FCS)

51 The cryptographic requirements are also structured to require the use of the Wi-Fi certification requirements for WPA2 enterprise, based on the IEEE 802.11 standard. The Wi-Fi Alliance WPA2 Enterprise certification program tests devices for data communications interoperability at ISO OSI layers 1 and 2, and mandates the use of the Advanced Encryption Standard (AES)-Counter with Cipher Block Chaining (Counter with CBC)-Message Authentication Code (MAC) algorithm (known collectively as AES-CCMP) for secure connections.

Cryptographic Key Management (FCS_CKM)

FCS_CKM.1	**Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)**
FCS_CKM.1.1	**Refinement:** The TSF shall **derive symmetric** cryptographic keys in accordance with a specified cryptographic key **derivation** algorithm **[PRF-384] with** specified cryptographic key size **[128 bits] using a Random Bit Generator as specified in FCS_RBG_EXT.1 and with an administratively-configured cryptoperiod with a granularity no greater than an hour** that meet the following: **[802.11-2007].**

Application Note:

52 *This requirement applies only to the keys that are generated/derived for the communications between the access point and the client once the client has been authenticated. It refers to the derivation of the PTK from the PMK, which is done using a random value generated by the RBG specified in this PP, the HMAC function using SHA-1 as specified in this PP, as well as other information. This is specified in 802.11-2007 primarily in chapter 8.*

53 ***Assurance Activity:***

The cryptographic primitives will be verified through assurance activities specified later in this PP. The evaluator shall verify that the TSS describes how the primitives defined and implemented by this PP are

used by the TOE in establishing and maintaining secure connectivity to the wireless clients. The TSS shall also provide a description of the developer's method(s) of assuring that their implementation conforms to the cryptographic standards; this includes not only testing done by the developing organization, but also any third-party testing that is performed. The evaluator shall ensure that the description of the testing methodology is of sufficient detail to determine the extent to which the details of the protocol specifics are tested. The evaluator shall check the administrative guidance to ensure that it describes the method by which the cryptoperiod for the session keys can be configured, and that the granularity of the specification is no more than an hour. The evaluation team shall also perform the following test:

- *Test 1: Following the administrative guidance, the evaluator shall configure the cryptoperiod of the session key. The evaluator shall successfully connect the TOE to the access point, and maintain the connection for a length of time greater than the cryptoperiod. The evaluator shall determine that after the configured cryptoperiod, a re-negotiation is initiated to establish a new session key.*

FCS_CKM.2	**Cryptographic Key Distribution (GTK)**
FCS_CKM.2.1	**Refinement:** The TSF shall distribute **Group Temporal Key** in accordance with a specified cryptographic key distribution method: [AES Key Wrap in an EAPOL-Key frame] that meets the following: [RFC 3394 for AES Key Wrap, 802.11-2007 for the packet format and timing considerations] **and does not expose the cryptographic keys**.

Application Note:

54 *This requirement applies to the Group Temporal Key (GTK) that is received by the TOE for use in decrypting broadcast and multicast messages from the Access Point to which it's connected. 802.11-2007 specifies the format for the transfer as well as the fact that it must be wrapped by the AES Key Wrap method specified in RFC 3394; the TOE must be capable of unwrapping such keys.*

Assurance Activity:

55 *The evaluator shall check the TSS to ensure that it describes how the GTK is unwrapped prior to being installed for use on the TOE using the AES implementation specified in this PP. The evaluator shall also perform the following tests:*

- *Test 1: The evaluator shall successfully connect the TOE to the access point. As the TOE is connected, the evaluator shall observe that the GTK is not transmitted in the clear between the TOE and the Access Point.*
- *Test 2: The evaluator shall cause a broadcast message to be sent by the Access Point to which the TOE is connected. The evaluator shall ensure the message is encrypted and cannot be read in transit, and that the TOE is able to decrypt and read the message sent.*

FCS_CKM_EXT.4	**Cryptographic Key Zeroization**
FCS_CKM_EXT.4.1	**Refinement:** The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

Application Note:

56 *Any security related information (such as keys, authentication data, and passwords) must be zeroized when no longer in use to prevent the disclosure or modification of security critical data.*

57 *The zeroization indicated above applies to each intermediate storage area for plaintext key/CSP (i.e., any storage, such as memory buffers, that is included in the path of such data) upon the transfer of the key/CSP to another location.*

58 *Since the TOE does not necessarily include the host IT environment, the extent of this capability is necessarily somewhat limited. For the purposes of this requirement, it is sufficient for the TOE to invoke the correct underlying functions of the host to perform the zeroization--it does not imply that the TOE has to include a kernel-mode memory driver to ensure the data are zeroized.*

Assurance Activity:

59 *The evaluator shall check to ensure the TSS describes each of the secret keys (keys used for symmetric encryption), private keys, and CSPs used to generate key; when they are zeroized (for example, immediately after use, on system shutdown, etc.); and the type of zeroization procedure that is performed (overwrite with zeros, overwrite three times with random pattern, etc.). If different types of memory are used to store the materials to be protected, the evaluator shall check to ensure that the TSS describes the zeroization procedure in terms of the memory in which the data are stored (for example, "secret keys stored on flash are zeroized by overwriting once with zeros, while secret keys stored on the internal hard drive are zeroized by overwriting three times with a random pattern that is changed before each write"). If a read-back is done to verify the zeroization, this shall be described as well.*

Cryptographic Operation (FCS_COP)

FCS_COP.1(1)	**Cryptographic Operation (Data Encryption/Decryption)**
FCS_COP.1.1(1)	**Refinement:** The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES operating in* [**assignment: *one or more modes***]] and cryptographic key sizes 128-bits, 256-bits, and [**selection: 192 bits, no other key sizes**] that meets the following: • **FIPS PUB 197, "Advanced Encryption Standard (AES)"** • **[Selection: NIST SP 800-38A, NIST SP 800-38B, NIST SP 800-38C, NIST SP 800-38D, NIST SP 800-38E]**

Application Note:

60 *For the assignment, the ST author should choose the mode or modes in which AES operates. For the first selection, the ST author should choose the key sizes that are supported by this functionality. For the second selection, the ST author should choose the standards that describe the modes specified in the assignment.*

61 *Note that this requirement does not apply to wireless traffic encryption. Requirement FCS_COP.1(5) defines the mode, key size and standards that are used for wireless WPA2 encryption/decryption.*

Assurance Activity:

62 *The evaluator shall use tests appropriate to the modes selected in the above requirement from "The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)", "The XTS-AES Validation System (XTSVS)", The CMAC Validation System (CMACVS)", "The Counter with Cipher Block Chaining-Message Authentication Code (CCM) Validation System (CCMVS)", and "The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS)" (these documents are available from http://csrc.nist.gov/groups/STM/cavp/index.html) as a guide in testing the requirement above. This will require that the evaluator have a trusted reference implementation of the algorithms that can produce test vectors that are verifiable during the test.*

FCS_COP.1(2) **Cryptographic Operation (Cryptographic Signature)**

FCS_COP.1.1(2)

Refinement: The TSF shall perform **cryptographic signature services** in accordance with a ***[selection:***

(1) Digital Signature Algorithm (DSA) with a key size (modulus) of 2048 bits or greater,

(2) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater, or

(3) Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater]

Application Note: As the preferred approach for cryptographic signature, elliptic curves will be required in future publications of this PP.

that meets the following:

Case: Digital Signature Algorithm

- **[selection: FIPS PUB 186-3, "Digital Signature Standard"]**

Case: RSA Digital Signature Algorithm

- **[selection: FIPS PUB 186-3, "Digital Signature Standard"]**

Case: Elliptic Curve Digital Signature Algorithm

- **[selection: FIPS PUB 186-3, "Digital Signature Standard "]**
- **The TSF shall implement "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-3, "Digital Signature Standard").**

Application Note:

63 *The ST Author should choose the algorithm implemented to perform digital signatures; if more than one algorithm is available, this requirement should be iterated to specify the functionality. For the algorithm chosen, the ST author should make the appropriate assignments/selections to specify the parameters that are implemented for that algorithm.*

64 *For elliptic curve-based schemes, the key size refers to the log_2 of the order of the base point. As the preferred approach for digital signatures, ECDSA will be required in future publications of this PP.*

Assurance Activity:

65 *The evaluator shall use the signature generation and signature verification portions of "The Digital Signature Algorithm Validation System" (DSA2VS), "The Elliptic Curve Digital Signature Algorithm Validation System" (ECDSA2VS), and "The RSA Validation System" (RSA2VS) as a guide in testing the requirement above. The Validation System used shall comply with the conformance standard identified in the ST (i.e. FIPS PUB 186-3). This will require that the evaluator have a trusted reference implementation of the algorithms that can produce test vectors that are verifiable during the test.*

FCS_COP.1(3)	**Cryptographic Operation (Cryptographic Hashing)**
FCS_COP.1.1(3)	**Refinement:** The TSF shall perform [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm [**selection: SHA-1, SHA-256, SHA-384] and message digest sizes** [**selection: 160, 256, 384**] **bits** that meet the following: *FIPS Pub 180-3, "Secure Hash Standard."*

Application Note:

66 *The selection of the hashing algorithm must correspond to the selection of the message digest size; for example, if SHA-1 is chosen, then the only valid message digest size selection would be 160 bits.*

Assurance Activity:

67 *The evaluator shall use "The Secure Hash Algorithm Validation System (SHAVS)" as a guide in testing the requirement above. This will require that the evaluator have a trusted reference implementation of the algorithms that can produce test vectors that are verifiable during the test.*

FCS_COP.1(4)	**Cryptographic Operation (Keyed-Hash Message Authentication)**
FCS_COP.1.1(4)	**Refinement:** The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-** [selection: SHA-1, SHA-256, SHA-384],-key size **[assignment: key size (in bits) used in HMAC], and message digest size of** [selection: 160, 256, 384] **bits** that meet the following: **FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code", and FIPS PUB 180-3, "Secure Hash Standard"**.

Application Note:

68 *The selection of the hashing algorithm must correspond to the selection of the message digest size; for example, if HMAC-SHA-256 is chosen, then the only valid message digest size selection would be 256 bits.*

69 *The message digest size above corresponds to the underlying hash algorithm used. Note that truncating the output of the HMAC following the hash calculation is an appropriate step in a variety of applications.*

This does not invalidate compliance with this requirement, however, the ST should state that truncation is performed, the size of the final output, and the standard to which this truncation complies.

Assurance Activity:

70 *The evaluator shall use "The Keyed-Hash Message Authentication Code (HMAC) Validation System (HMACVS)" as a guide in testing the requirement above. This will require that the evaluator have a trusted reference implementation of the algorithms that can produce test vectors that are verifiable during the test.*

FCS_COP.1(5)	**Cryptographic Operation (WPA2 Data Encryption/Decryption)**
FCS_COP.1.1(5)	**Refinement:** The TSF shall perform **encryption and decryption in accordance with the specified cryptographic algorithm AES CCMP and cryptographic key size of 128 bits** that meet the following: **FIPS PUB 197, NIST SP 800-38C and IEEE 802.11-2007**.

Application Note:

71 *Note that to comply with IEEE 802.11-2007, AES CCMP (which uses AES in CCM as specified in SP 800-38C) with cryptographic key size of 128 bits must be implemented. In the future, as this standard is updated and new cryptographic modes are reviewed and approved by NIST, this requirement may include requirements for additional/new cryptographic modes and key sizes.*

Assurance Activity:

72 *The evaluator shall use tests from "The Counter with Cipher Block Chaining-Message Authentication Code (CCM) Validation System (CCMVS)" as a guide in testing the requirement above. This will require that the evaluator have a trusted reference implementation of the algorithms that can produce test vectors that are verifiable during the test.*

73 *Additionally, the evaluator shall use tests from the IEEE 802.11-02/362r6 document "Proposed Test vectors for IEEE 802.11 TGi", dated September 10, 2002, Section 2.1 AES-CCMP Encapsulation Example and Section 2.2 Additional AES CCMP Test Vectors to further verify the IEEE 802.11-2007 implementation of AES-CCMP.*

Extended: Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) (FCS_EAP-TLS_EXT)

FCS_EAP-TLS_EXT.1	**Extended: Extensible Authentication Protocol-Transport Layer Security**

FCS_EAP-TLS_EXT.1.1 The TSF shall implement the EAP-TLS protocol as specified in RFC 5216 supporting the following ciphersuites:

- Mandatory Ciphersuites in accordance with RFC 3268:

  TLS_RSA_WITH_AES_128_CBC_SHA
  TLS_RSA_WITH_AES_256_CBC_SHA
  TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  TLS_DHE_RSA_WITH_AES_256_CBC_SHA

- Optional Ciphersuites:

  [selection:
  None
  TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
  TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
  TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246
  TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
  TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
  TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
  TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5430
  TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5430
  ].

FCS_EAP-TLS_EXT.1.2 The TOE shall generate random values used in the EAP-TLS exchange using the RBG specified in FCS_RBG_EXT.1.

FCS_EAP-TLS_EXT.1.3 The TSF shall use X503 v3 certificates as specified in FIA_X509_EXT.1.

FCS_EAP-TLS_EXT.1.4 The TSF shall verify that the server certificate presented includes the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extended KeyUsage field.

FCS_EAP-TLS_EXT.1.5 The TSF shall allow an authorized administrator to configure the list of CAs that are allowed to sign authentication server certificates that are accepted by the TOE.

FCS_EAP-TLS_EXT.1.6 The TSF shall allow an authorized administrator to configure the list of algorithm suites that may be proposed and accepted during the EAP-TLS exchanges.

Application Note:

74 *The ciphersuites to be used in the evaluated configuration are limited by this requirement. The ST author should select the optional ciphersuites that are supported; if there are no ciphersuites supported other than the mandatory suites, then "None" should be selected. It is acceptable to limit the ciphersuites that can be used in an evaluated configuration administratively.*

The Suite B algorithms listed above (RFC 5430) are the preferred algorithms for implementation.

75 *While FCS_EAP-TLS_EXT.1.4 requires that the TOE perform certain checks on the certificate presented by the authentication server, there are corresponding checks that the authentication server will have to perform on the certificate presented by the client; namely that the extendedKeyUsage field of the client certificate includes "Client Authentication" and that the key agreement bit (for the Diffie-Hellman ciphersuites) or the key encipherment bit (for RSA ciphersuites) be set. Certificates obtained for use by the TOE will have to conform to these requirements in order to be used in the enterprise.*

Assurance Activity:

76 *In order to show that the TSF implements the RFCs correctly, the evaluator shall ensure that the TSS contains the following information:*

- *For each section of each applicable RFC listed for the FCS_EAP_TLS_EXT.1 elements, for all statements that are not "MUST" (for example, "MAY", "SHOULD", "SHOULD NOT", etc.), if the TOE implements such options it shall be described in the TSS. If the included functionality is indicated as "SHOULD NOT" or "MUST NOT" in the standard, the TSS shall provide a rationale for why this will not adversely affect the security policy implemented by the TOE;*
- *For each section of each RFC, any omission of functionality related to "SHOULD" statements shall be described;*

77 *Any TOE-specific extensions, processing that is not included in the standard, or alternative implementations allowed by the standard that may impact the security requirements the TOE is to enforce shall be described.*

78 *The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics (e.g., extensions supported, client authentication supported) are specified, and the ciphersuites supported are specified as well. The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component. The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).*

79 *The evaluator shall check that the OPE guidance contains instructions for the administrator to configure the list of Certificate Authorities that are allowed to sign certificates used by the authentication server that will be accepted by the TOE in the EAP-TLS exchange, and instructions on how to specify the algorithm suites that will be proposed and accepted by the TOE during the EAP-TLS exchange.*

80 *The evaluator shall also perform the following tests:*

- *Test 1: The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an EAP session. It is sufficient to observe (on the wire) the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).*
- *Test 2: The following test is repeated for each supported certificate signing algorithm supported. The evaluator shall attempt to establish the connection using a server with a authentication server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field.*
- *Test 3: Following the guidance provided by the OPE/PRE guidance, a CA will be configured as "acceptable" for authentication server certificates and then the evaluator will start a wireless connection and verify that the wireless client is able to successfully connect. The evaluator will then configure the system such that an otherwise valid certificate is signed by a CA that is not allowed by the TOE. Attempts to authenticate to an authorization server presenting such a certificate should result in the connection being refused.*
- *Test 4: The evaluator shall follow the administrative guidance to configure the list of protocols to be proposed during EAP-TLS negotiations that is limited to only those specified by the first element of this component. The evaluator shall initiate a connection with an access point and ensure that only those protocols configured are proposed. If the initial list is not a subset of the total set of protocol proposed by the client, the evaluator shall repeat the test specifying a subset of the protocols used in the initial test.*

Extended: Cryptographic Operation (Random Bit Generation) (FCS_RBG_EXT)

FCS_RBG_EXT.1	**Extended: Cryptographic operation (Random Bit Generation)**
FCS_RBG_EXT.1.1	The TSF shall perform all random bit generation (RBG) services in accordance with [selection, choose one of: NIST Special Publication 800-90 using [selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES), Dual_EC_DRBG (any)]; FIPS Pub 140-2 Annex C; X9.31 Appendix 2.4 using AES] seeded by an entropy source that accumulates entropy from [selection: choose one of: one or more independent hardware-based noise sources, one or more independent software-based noise sources, a combination of hardware-based and software-based noise sources.].
FCS_RBG_EXT.1.2	The deterministic RBG shall be seeded with a minimum of [selection, choose one of: 128 bits, 256 bits] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

Application Note:

81 *NIST Special Pub 800-90, Appendix C describes the minimum entropy measurement that will probably be required in future versions of FIPS-140. If possible this should be used immediately and will be required in future versions of this PP.*

82 *For the first selection in FCS_RBG_EXT.1.1, the ST author should select the standard to which the RBG services comply (either 800-90 or 140-2 Annex C). For the second selection, the ST author indicates how the client collects entropy for the RBG.*

83 *SP 800-90 contains four different methods of generating random numbers; each of these, in turn, depends on underlying cryptographic primitives (hash functions/ciphers). The ST author will select the function used (if 800-90 is selected), and include the specific underlying cryptographic primitives used in the requirement or in the TSS. While any of the identified hash functions (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) are allowed for Hash_DRBG or HMAC_DRBG, only AES-based implementations for CT_DRBG are allowed. While any of the curves defined in 800-90 are allowed for Dual_EC_DRBG, the ST author not only must include the curve chosen, but also the hash algorithm used.*

84 *Note that for FIPS Pub 140-2 Annex C, currently only the method described in NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, Section 3 is valid. If the key length for the AES implementation used here is different than that used to encrypt the user data, then FCS_COP.1 may have to be adjusted or iterated to reflect the different key length. For the selection in FCS_RBG_EXT.1.2, the ST author selects the minimum number of bits of entropy that is used to seed the RBG.*

85 *The ST author also ensures that any underlying functions are included in the baseline requirements for the TOE.*

86 *In the future, most of the requirements described in A Method for Entropy Source Testing: Requirements and Test Suite Description will be required by this PP. The follow Assurance Activities currently reflect only that subset of activities that are required.*

Assurance Activity:

87 *The evaluator shall review the TSS section to determine the version number of the product containing the RBG(s) used in the TOE. The evaluator shall also confirm that the TSS describes the noise source or sources from which entropy is gathered. The evaluator will further verify that all of the underlying functions and parameters used in the RBG are listed in the TSS.*

88 *The evaluator shall verify that the TSS contains a description of the RBG model, including the method for obtaining entropy input, as well as identifying the entropy source(s) used, how entropy is produced/gathered from each source, and how much entropy is produced by each entropy source. The evaluator shall also ensure that the TSS describes the entropy source health tests, a rationale for why the health tests are sufficient to determine the health of the entropy sources, and known modes of entropy source failure. Finally, the evaluator shall ensure that the TSS contains a description of the RBG outputs in terms of the independence of the output and variance with time and/or environmental conditions.*

89 *Regardless of the standard to which the RBG is claiming conformance, the evaluator performs the following test:*

- *Test 1: The evaluator shall determine an entropy estimate for each entropy source by using the Entropy Source Test Suite. The evaluator shall ensure that the TSS includes an entropy estimate that is the minimum of all results obtained from all entropy sources.*

90 *The evaluator shall also perform the following tests, depending on the standard to which the RBG conforms.*

Implementations Conforming to FIPS 140-2, Annex C

91 *The reference for the tests contained in this section is The Random Number Generator Validation System (RNGVS) [RNGVS]. The evaluators shall conduct the following two tests. Note that the "expected values" are produced by a reference implementation of the algorithm that is known to be correct. Proof of correctness is left to each Scheme.*

92 *The evaluators shall perform a Variable Seed Test. The evaluators shall provide a set of 128 (Seed, DT) pairs to the TSF RBG function, each 128 bits. The evaluators shall also provide a key (of the length appropriate to the AES algorithm) that is constant for all 128 (Seed, DT) pairs. The DT value is incremented by 1 for each set. The seed values shall have no repeats within the set. The evaluators ensure that the values returned by the TSF match the expected values.*

93 *The evaluators shall perform a Monte Carlo Test. For this test, they supply an initial Seed and DT value to the TSF RBG function; each of these is 128 bits. The evaluators shall also provide a key (of the length appropriate to the AES algorithm) that is constant throughout the test. The evaluators then invoke the TSF RBG 10,000 times, with the DT value being incremented by 1 on each iteration, and the new seed for the subsequent iteration produced as specified in NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, Section 3. The evaluators ensure that the 10,000th value produced matches the expected value.*

Implementations Conforming to NIST Special Publication 800-90

94 *The evaluator shall perform 15 trials for the RNG implementation. If the RNG is configurable, the evaluator shall perform 15 trials for each configuration. The evaluator shall also confirm that the operational guidance contains appropriate instructions for configuring the RNG functionality.*

95 *If the RNG has prediction resistance enabled, each trial consists of (1) instantiate drbg, (2) generate the first block of random bits (3) generate a second block of random bits (4) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. "Generate one block of random bits" means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP 800-90).*

96 *If the RNG does not have prediction resistance, each trial consists of (1) instantiate drbg, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final value is additional input to the second generate call.*

97 *The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator.*

***Entropy input:** the length of the entropy input value must equal the seed length.*

Nonce: *If a nonce is supported (CTR_DRBG with no df does not use a nonce), the nonce bit length is one-half the seed length.*
Personalization string: *The length of the personalization string must be <= seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is support, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied.*
Additional input: *the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.*

4.1.3 Class: User Data Protection (FDP)

Residual Information Protection (FDP_RIP)

FDP_RIP.2	**Full Residual Information Protection**
FDP_RIP.2.1	The TSF shall enforce that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to*, *deallocation of the resource from*] all objects.

Application Note:

98 *This requirement ensures, for example, that protocol data units (PDUs) are not padded with residual information such as cryptographic key material. The ST author uses the selection to specify when previous information is made unavailable.*

Assurance Activity:

99 *"Resources" in the context of this requirement are network packets being sent through (as opposed to "to", as is the case when a security administrator connects to the TOE) the TOE. The concern is that once a network packet is sent, the buffer or memory area used by the packet still contains data from that packet, and that if that buffer is re-used, those data might remain and make their way into a new packet. The evaluator shall check to ensure that the TSS describes packet processing to the extent that they can determine that no data will be reused when processing network packets. The evaluator shall ensure that this description at a minimum describes how the previous data are zeroized/overwritten, and at what point in the buffer processing this occurs.*

4.1.4 Class: Identification and Authentication (FIA)

100 The baseline requirements for the TOE are fairly limited with respect to I&A, since no formal administrative or general purpose users are defined. The extent of the I&A required to be performed by the TOE relates to the process of becoming connected to the protected network through the Wireless Access System. Additionally, some of the requirements that might normally be considered part of the I&A process are specified in other sections of this PP, particularly those related to cryptographic protocols used for the wireless communications (WPA2). This was done to keep requirements on those protocols grouped together for understandability as well as for ease of authoring and applying

assurance activities. Therefore, the requirements in this section cover the remaining two aspects of the I&A capabilities the TOE must support:

- **802.1X-2010 Authentication.** The 802.1X-2010 standard (and associated RFCS) specifies authentication of a machine for the purposes of accessing a network. This method is used as a precursor to wireless operations using the 802.11-2007 standard. While 802.1X contains requirements for several different parties that participate in 802.1X exchanges, the requirements below are targeted at the TOE's role as a "supplicant" per 802.1X.
- **Credentials.** The protocols and mechanisms specified in this and other sections of the PP rely on certificates for use in the EAP-TLS exchange in performing the 802.1X authentication.

Extended: 802.1X Port Access Control Authentication (FIA_8021X_EXT)

FIA_8021X_EXT.1	**Extended: 802.1X Port Access Entity (Supplicant) Authentication**
FIA_8021X_EXT.1.1	The TSF shall conform to IEEE Standard 802.1X for a Port Access Entity (PAE) in the "Supplicant" role.

Application Note:

101 *This requirement covers the TOE's role as the supplicant in an 802.1X authentication exchange. If the exchange is completed successfully, the TOE will derive the PMK as a result of the EAP-TLS (or other appropriate EAP exchange) and perform the 4-way handshake with the wireless access system (authenticator) to begin 802.11 communications.*

102 *As indicated previously, there are at least two communication paths present during the exchange; one with the wireless access system and one with the authentication server that uses the wireless access system as a relay. The TOE establishes an EAP over LAN (EAPOL) connection with the wireless access system as specified in 802.1X-2010. The TOE and authentication server establish an EAP-TLS session (RFC 5216).*

103 *The point of performing 802.1X authentication is to gain access to the network (assuming the authentication was successful and that all 802.11 negotiations are performed successfully); in the terminology of 802.1X, this means the TOE will gain access to the "controlled port" maintained by the wireless access system.*

Assurance Activity:

104 *In order to show that the TSF implements the 802.1X-2010 standard correctly, the evaluator shall ensure that the TSS contains the following information:*

- *the sections (clauses) of the standard that the TOE implements;*
- *For each identified section, any options allowed by the standards are specified; and*
- *For each identified section, any non-conformance is identified and described, including a justification for the non-conformance.*

105 *The evaluator shall also perform the following tests:*

- *Test 1: The evaluator shall demonstrate that the TOE has no access to the test network. After successfully authenticating with an authentication server through a wireless access system, the evaluator shall demonstrate that the TOE does have access to the test network.*

- *Test 2: The evaluator shall demonstrate that the TOE has no access to the test network. The evaluator shall attempt to authenticate using an invalid client certificate, such that the EAP-TLS negotiation fails. This should result in the TOE still being unable to access the test network.*

- *Test 3: The evaluator shall demonstrate that the TOE has no access to the test network. The evaluator shall attempt to authenticate using an invalid authentication server certificate, such that the EAP-TLS negotiation fails. This should result in the TOE still being unable to access the test network.*

X509 Certificates (FIA_X509_EXT)

FIA_X509_EXT.1	**Extended: X.509 Certificates**
FIA_X509_EXT.1.1	The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for EAP-TLS exchanges.

Application Note:

106 *It should be noted that RFC 5280 defines certificate validation and certification path validation requirements that must be implemented by the TOE as per this requirement.*

Assurance Activity:

107 *In order to show that the TSF supports the use of X.509v3 certificates according to the RFC 5280, the evaluator shall ensure that the TSS describes the following information:*

- *For each section of RFC 5280, any statement that is not "MUST" (for example, "MAY", "SHOULD", "SHOULD NOT", etc.) shall be described so that the reader can determine whether the TOE implements that specific part of the standard;*
- *For each section of RFC 5280, any non-conformance to "SHOULD" statements shall be described;*
- *Any TOE-specific extensions or processing that is not included in the standard that may impact the security requirements the TOE is to enforce shall be described.*

108 *Additionally, the evaluator shall devise tests that show that the TOE processes certificates that conform to the implementation described in the TSS; are able to form a certification path as specified in the standard and in the TSS; and are able to validate certificates as specified in the standard (certification path validation including CRL processing). This testing shall be described in the team test plan.*

109 *It should be noted that future versions of this PP will have more explicit testing requirements for a TOE's certificate handling capability. Additionally, protocol-specific certificate handling testing will need to be performed and can be combined with the testing required by this assurance activity.*

110 *The evaluator shall check the administrative guidance to ensure that it describes how the TOE chooses which certificates to use, and any necessary instructions for configuring the operating environment so that the TOE can use the certificates.*

111 *The evaluator shall perform the following tests for each function in the system that requires the use of certificates:*

- *Test 1: The evaluator shall demonstrate that using a certificate without a valid certification path results in the function failing. Using the administrative guidance, the evaluator shall then load a certificate or certificates needed to validate the certificate to be used in the function, and demonstrate that the function succeeds. The evaluator then shall delete one of the certificates, and show that the function fails.*

4.1.5 Class: Security Management (FMT)

112 As indicated in Section 1 of this PP, the TOE is not required to maintain a separate management role. They are, however, required to provide functionality to configure certain aspects of TOE operation that should not be available to the general user population. If the TOE does provide some degree of administrative control, then the appropriate requirements from Appendix C should be used in the ST.

Specification of Management Functions (FMT_SMF)

FMT_SMF.1	**Specification of Management Functions**

FMT_SMF.1.1	The TSF shall be capable of performing the following management functions:
	• **Specify the CAs from which the TOE will accept authentication server certificates,**
	• **specify the FQDN of acceptable authentication server certificates,**
	• **enable/disable certificate revocation list checking,**
	• **configure the cryptoperiod for the established session keys. The unit of measure for configuring the cryptoperiod shall be no greater than an hour,**
	• **disable ad hoc wireless client-to-client connection capability,**
	• **disable wireless network bridging capability,**
	• **disable roaming capability,**
	• **specify the algorithm suites that may be proposed and accepted during the EAP-TLS exchanges,**
	• **specify wireless networks that are acceptable for the TOE to connect,**
	• **ability to disable/enable IEEE 802.1X pre-authentication,**
	• **ability to disable/enable and configure PMK caching:**
	  ○ **set the amount of time (in minutes) PMK entries are cached,**
	  ○ **set the maximum number of PMK entries that can be cached,**
	• **ability to update the TOE, and to verify the updates,**
	• **ability to configure all security management functions identified in other sections of this PP,**
	• **[assignment: any additional management functions].**

Application Note:

113 *For installation, the WLAN Client relies on the IT environment to authenticate the administrator to the client machine.*

114 *For the function configure the cryptoperiod for the established session keys, the unit of measure for configuring the cryptoperiod shall be no greater than an hour. For example: units of measure in seconds, minutes and hours are acceptable and units of measure in days or greater are not acceptable.*

115 ***Assurance Activity:***

116 *The evaluator shall check to make sure that every management function mandated by the PP is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function. The evaluator shall test the TOE's ability to provide the management functions by configuring the TOE and testing each option listed in the requirement above.*

117 *Note that the testing here may be accomplished in conjunction with the testing of other requirements, such as FCS_EAP-TLS_EXT and FTA_WSE_EXT.*

4.1.6 Class: Protection of the TSF (FPT)

Extended: TSF Self Test (FPT_TST_EXT)

FPT_TST_EXT.1	**Extended: TSF Self Test**
FPT_TST_EXT.1.1	The TSF shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.
FPT_TST_EXT.1.2	The TSF shall provide the capability to verify the integrity of stored TSF executable code when it is loaded for execution through the use of the TSF-provided cryptographic services.

Application Note:

118 *While the TOE is typically a software package running in the IT Environment, it is still capable of performing the self-test activities required above. It should be understood, however, that there is a significant dependency on the host environment in assessing the assurance provided by the tests mentioned above (meaning that if the host environment is compromised, the self tests will not be meaningful).*

Assurance Activity:

119 *The evaluator shall examine the TSS to ensure that it details the self tests that are run by the TSF on start-up; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.*

120 *The evaluator shall examine the TSS to ensure that it describes how to verify the integrity of stored TSF executable code when it is loaded for execution. The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the integrity of stored TSF executable code*

has not been compromised. The evaluator also ensures that the TSS (or the operational guidance) describes the actions that take place for successful (e.g. hash verified) and unsuccessful (e.g., hash not verified) cases. The evaluator shall perform the following tests:

- *Test 1: The evaluator performs the integrity check on a known good TSF executable and verifies that the check is successful.*
- *Test 2: The evaluator modifies the TSF executable, performs the integrity check on the modified TSF executable and verifies that the check fails.*

Extended: Trusted Update (FPT_TUD_EXT.1)

FPT_TUD_EXT.1	**Extended: Trusted Update**
FPT_TUD_EXT.1.1	The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.
FPT_TUD_EXT.1.2	The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.
FPT_TUD_EXT.1.3	The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [selection: published hash, no other functions] prior to installing those updates.

Application Note:

121 *The digital signature mechanism referenced in the third element is the one specified in FCS_COP.1(2). The published hash referenced is generated by one of the functions specified in FCS_COP.1(3).*

Assurance Activity:

122 *Updates to the TOE are signed by an authorized source and may also have a hash associated with them, or are signed by an authorized source. If digital signatures are used, the definition of an authorized source is contained in the TSS, along with a description of how the certificates used by the update verification mechanism are contained on the device. The evaluator ensures this information is contained in the TSS. The evaluator also ensures that the TSS (or the operational guidance) describes how the candidate updates are obtained; the processing associated with verifying the digital signature or calculating the hash of the updates; and the actions that take place for successful (hash or signature was verified) and unsuccessful (hash or signature could not be verified) cases. The evaluator shall perform the following tests:*

- *Test 1: The evaluator performs the version verification activity to determine the current version of the product. The evaluator obtains a legitimate update using procedures described in the operational guidance and verifies that it is successfully installed on the TOE. Then, the evaluator performs a subset of other assurance activity tests to demonstrate that the update functions as expected. After the update, the evaluator performs the version verification activity again to verify the version correctly corresponds to that of the update.*

- *Test 2: The evaluator performs the version verification activity to determine the current version of the product. The evaluator obtains or produces an illegitimate update, and attempts to install it on the TOE. The evaluator verifies that the TOE rejects the update.*

4.1.7 Class: TOE Access (FTA)

Extended: Wireless Session Establishment (FTA_WSE_EXT)

FTA_WSE_EXT.1	Extended: Wireless Session Establishment
FTA_WSE_EXT.1.1	The TSF shall only attempt connections to wireless networks specified as acceptable networks based on [assignment: *attribute(s) used to identify the list of acceptable networks*] as configured by an authorized administrator.

Application Note:

123 *The intent of this requirement is to allow the administrator to limit the access points to which the TOE is allowed to connect. The assignment is used by the ST author to specify the attributes (e.g., IP Address, SSID, etc.) that can be used by the administrator to specify the acceptable access points.*

Assurance Activity:

124 *The evaluator shall examine the TSS to determine that all of the attributes that can be used to specify acceptable networks (access points) are specifically defined. The evaluator shall examine the operational guidance to determine that it contains guidance for configuring each of the attributes identified in the TSS. The evaluator shall also perform the following test for each attribute:*

- *Test 1: The evaluator configures the TOE to allow a connection with a specific access point. The evaluator also configures the test environment such that the allowed access point and an access point that is not allowed are both "visible" to the TOE. The evaluator shall demonstrate that they can successfully establish a session with the allowed access point. The evaluator will then attempt to establish a session with the disallowed access point, and observe that the access attempt fails.*

4.1.8 Class: Trusted Path/Channels (FTP)

Trusted Channel (FTP_ITC)

FTP_ITC.1	Inter-TSF trusted channel
FTP_ITC.1.1	**Refinement:** The TSF shall **use 802.11-2007, 802.1X, and EAP-TLS** to provide a **trusted** communication channel between itself and **a wireless access point** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data **from disclosure and detection of modification of the channel data**.

FTP_ITC.1.2	The TSF shall permit *the TSF* to initiate communication via the trusted channel.
FTP_ ITC.1.3	The TSF shall initiate communication via the trusted channel *prior to any other communication through the connected network*.

Application Note:

125 *The intent of the above requirement is to use the cryptographic protocols identified in the requirement to protect communications between the TOE and the Access Point.*

126 *The requirement implies that not only are communications protected when they are initially established, but also on resumption after an outage. It may be the case that some part of the TOE setup involves manually setting up tunnels to protect other communication, and if after an outage the TOE attempts to re-establish the communication automatically with (the necessary) manual intervention, there may be a window created where an attacker might be able to gain critical information or compromise a connection.*

Assurance Activity:

127 *The evaluator shall examine the TSS to determine that it describes the details of the TOE connecting to an access point in terms of the cryptographic protocols specified in the requirement, along with TOE-specific options or procedures that might not be reflected in the specification. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST. The evaluator shall confirm that the operational guidance contains instructions for establishing the connection to the access point, and that it contains recovery instructions should a connection be unintentionally broken. The evaluator shall also perform the following tests:*

- *Test 1: The evaluators shall ensure that the TOE is able to initiate communications with an access point using the protocols specified in the requirement, setting up the connections as described in the operational guidance and ensuring that communication is successful.*
- *Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.*
- *Test 4: The evaluator shall ensure, for each communication channel with an authorized IT entity, modification of the channel data is detected by the TOE.*
- *Test 5: The evaluators shall physically interrupt the connection from the TOE to the access point (e.g., moving the TOE host out of range of the access point, turning the access point off). The evaluators shall ensure that subsequent communications are appropriately protected, at a minimum in the case of any attempts to automatically resume the connection or connect to a new access point.*

128 *Further assurance activities are associated with the specific protocols.*

4.2 Rationale for Security Functional Requirements

129 This section describes the rationale for the TOE Security Functional Requirements as defined in Section 4.1. Table 10 illustrates the mapping from Security Functional Requirements to Security Objectives with a corresponding rationale that the objective is addressed by the requirement.

130 The Security Target (ST) provided by the vendor also contains a security requirements rationale, consisting of two sections:

- a tracing that shows which SFRs address which security objectives for the TOE;
- a set of justifications that shows that all security objectives for the TOE are effectively addressed by the SFRs. (per CC part 1, Section B7)

Table 10: Rationale for TOE Security Functional Requirements

Objective	Requirement Addressing the Objective	Rationale
O.AUTH_COMM The TOE will provide a means to ensure that it is communicating with an authorized Access Point and not some other entity pretending to be an authorized Access Point, and will provide assurance to the Access Point of its identity.	FCS_CKM.1 FCS_COP.1(2) FCS_EAP-TLS_EXT.1 FIA_8021X_EXT.1 FIA_X509_EXT.1 FTP_ITC.1	FTP_ITC.1 (and the supporting requirements FCS_CKM.1, FCS_COP.1(2), FCS_EAP-TLS_EXT.1, FIA_8021X_EXT.1, and FIA_X509_EXT.1) require the TOE provide a mechanism that creates a distinct communication channel between the TOE and both remote administrators and trusted IT entities that protects the data that traverse this channel from disclosure or modification. This is done cryptographically using the protocols specified by the requirements; these protocols provide the assured mutual identification of the endpoints and protection of the channel data.
O.CRYPTOGRAPHIC_FUNCTIONS The TOE shall provide cryptographic functions (i.e., encryption/decryption and digital signature operations) to maintain the confidentiality and allow for detection of modification of data that are transmitted outside the TOE and its host environment.	FCS_CKM.1 FCS_CKM.2 FCS_CKM_EXT.4 FCS_COP.1(1) FCS_COP.1(2) FCS_COP.1(3) FCS_COP.1(4) FCS_COP.1(5) FCS_RBG_EXT.1 FIA_X509_EXT.1	FCS_CKM.1 generate symmetric key. These keys are used by the AES encryption/decryption functionality specified in FCS_COP.1(5). FCS_CKM.2 assures that the distribution method of cryptographic keys for wireless client communications are in accordance with a standard and do not get exposed. FCS_CKM_EXT.4 provides the functionality for ensuring key and key material is zeroized. Since the TOE will in most cases be a software entity running on the host, the extent of this requirement is to make sure that the software invokes appropriate functions to clear the data; the host will

		ultimately be responsible for making sure the data are clear. FCS_COP.1(1) specifies that AES be used to perform encryption and decryption operations for the various protocols specified in the PP. FCS_COP.1(2) requires a digital signature capability be implemented in the TOE for trusted updates and certificate operations associated with the protocols used to protect the traffic. FCS_COP.1(3) and FCS_COP.1(4) require that the TSF provide hashing services using an implementation of the Secure Hash Algorithm algorithms for data integrity verification and non-data integrity operations. FIA_X509_EXT.1 requires that the certificates used to support many of the cryptographic operations previously mentioned conform to an appropriate standard. FCS_RBG_EXT.1 requires that a robust random bit generation capability be present.
O.PROTOCOLS The TOE will ensure that standardized protocols are implemented in the TOE to RFC and/or Industry specifications to ensure interoperability.	FCS_EAP-TLS_EXT.1 FIA_8021X_EXT.1 FTP_ITC.1	FCS_EAL-TLS_EXT.1, FIA_8021X_EXT.1, and FTP_ITC.1 (for 802.11-2007) all reference the standards (and indicate any restrictions on those standards) applicable to the protocol they require to be implemented.
O.RESIDUAL_INFORMATION_CLEARING The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.	FCS_CKM_EXT.4 FDP_RIP.2	FCS_CKM_EXT.4 ensures the destruction of any cryptographic keys when no longer needed. FDP_RIP.2 is used to ensure the contents of resources are not available to subjects other than those explicitly granted access to the data. For this TOE it is critical that the memory used to build network packets is either cleared or that some buffer management scheme be employed to prevent the contents of a packet being disclosed in a subsequent packet (e.g., if padding is used in the construction of a packet, it must not contain another user's data or TSF data).

O.SYSTEM_MONITORING The TOE will provide the capability to generate audit data.	FAU_GEN.1 FAU_SEL.1	FAU_GEN.1 defines the set of events that the TOE must be capable of recording, while FAU_SEL.1 allows the administrator to configure which auditable events will be recorded in the audit trail.
O.TOE_ADMINISTRATION The TOE will provide mechanisms to allow administrators to be able to configure the TOE.	FAU_SEL.1 FMT_SMF.1	FAU_SEL.1 requires the capability to configure the auditable events to be recorded, while FMT_SMF.1 provides configuration requirements for other parts of the TOE. As mentioned in the introduction, the TOE is not required to provide an administrative role, but the TOE in combination with the IT Environment must be capable of restricting these functions to a subset of the general users of the host machine.
O.TSF_SELF_TEST The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.	FPT_TST_EXT.1	FPT_TST_EXT.1 requires the TOE to provide a suite of self tests to assure the correct operation of the TSF, and to detect integrity problems in its stored executable.
O.VERIFIABLE_UPDATES The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.	FCS_COP.1(2) FCS_COP.1.(3) FPT_TUD_EXT.1	FCS_COP.1(2) and FCS_COP.1(3) specify digital signature algorithms and hash functions used in verification of updates. FPT_TUD_EXT.1 provides a way to determine the version of firmware running, initiate an update, and verify the firmware/software updates to the TOE prior to installation.
O.WIRELESS_ACCESS_POINT_CONNECTION The TOE will provide the capability to restrict the wireless access points to which is will connect.	FTA_WSE_EXT.1	FTA_WSE_EXT.1 provides the capability to control access to wireless access points based on the identity of the access point.

4.3 Security Assurance Requirements

131 The Security Objectives for the TOE in Section 3 were constructed to address threats identified in Section 2.1 and the Organizational Security Policies cited in Section 2.2. The Security Functional Requirements (SFRs) in Section 4.1 are a formal instantiation of the Security Objectives.

132 As indicated in the introduction to Section 4, while this section contains the complete set of SARs from the CC, the Assurance Activities to be performed by an evaluator are detailed in Section 4.1 as well as in this section.

133 For each family, "Developer Notes" are provided on the developer action elements to clarify what, if any, additional documentation/activity needs to be provided by the developer. For the content/presentation and evaluator activity elements, additional assurance activities (to those already contained in Section 4.1) are described as a whole for the family, rather than for each element. Additionally, the assurance activities described in this section are complementary to those specified in Section 4.1.

134 The TOE security assurance requirements, summarized in Table 11, identify the management and evaluative activities required to address the threats and policies identified in Section 2 of this PP. Section 4.4 provides a succinct justification for choosing this set of assurance requirements for this PP.

Table 11: TOE Security Assurance Requirements

Assurance Class	Assurance Components	Assurance Components Description
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Tests	ATE_IND.1	Independent testing - conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability analysis
Life Cycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage

4.3.1 Class ADV: Development

135 For TOEs conforming to this PP, the information about the TOE is contained in the guidance documentation available to the end user as well as the TOE Summary Specification (TSS) portion of the ST. While it is not required that the TOE developer write the TSS, the TOE developer must concur with the description of the product that is contained in the TSS as it relates to the functional requirements. The Assurance Activities contained in Section 4.1 should provide the ST authors with sufficient information to determine the appropriate content for the TSS section.

4.3.1.1 ADV_FSP.1 Basic functional specification

136 The functional specification describes the TOE Security Function Interfaces (TSFIs). It is not necessary to have a formal or complete specification of these interfaces. Additionally, because TOEs conforming to this PP will necessarily have interfaces to the operational environment that are not directly invokable by TOE users (to include administrative users), there is little point specifying that such interfaces be described in and of themselves since only indirect testing of such interfaces may be possible. The activities for this family for this PP should focus on understanding the interfaces presented in the TSS in response to the functional requirement, and the interfaces presented in the AGD documentation. No

additional “functional specification” document should be necessary to satisfy the assurance activities specified.

137 In understanding the interfaces to the TOE, it is important to consider that the threat that is to be countered is that the attacker gains unauthorized access to the wired network through a wireless connection. The TOE interface which supports communication between the wireless client and the wired network is a critical interface that requires protection such that only authenticated users are allowed access and an encrypted tunnel is established. In addition to the wireless client interface, the administrative interface (how the TOE is configured) also needs to be described.

138 The interfaces that need to be evaluated are characterized through the information needed to perform the assurance activities listed, rather than as an independent, abstract list.

Developer action elements:

ADV_FSP.1.1D	The developer shall provide a functional specification.
ADV_FSP.1.2D	The developer shall provide a tracing from the functional specification to the SFRs.
Developer Note:	As indicated in the introduction to this section, the functional specification is comprised of the information contained in the AGD_OPR and AGD_PRE documentation, coupled with the information provided in the TSS of the ST. The assurance activities in the functional requirements point to evidence that should exist in the documentation and TSS section; since these are directly associated with the SFRs, the tracing in element ADV_FSP.1.2D is implicitly already done and no additional documentation is necessary.

Content and presentation elements:

ADV_FSP.1.1C	The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.2C	The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.3C	The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.
ADV_FSP.1.4C	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_ FSP.1.1E	The evaluator *shall confirm* that the information provided meets all

requirements for content and presentation of evidence.

ADV_ FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

Assurance Activity:

139 *There are no specific assurance activities associated with these SARs. The functional specification documentation is provided to support the evaluation activities described in Section 4.1, and other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other assurance activities being performed; if the evaluator is unable to perform an activity because there is insufficient interface information, then an adequate functional specification has not been provided.*

4.3.2 Class AGD: Guidance Documents

140 The guidance documents will be provided with the developer's security target. Guidance must include a description of the administrative model, and how the administrator verifies that the operational environment (the system that hosts the WLAN Client) can fulfill its role for the security functionality. The documentation should be in an informal style and readable by an administrator.

141 Guidance must be provided for every operational environment that the product supports as claimed in the ST. This guidance includes

- instructions to successfully install the TOE in that environment; and
- instructions to manage the security of the TOE as a product and as a component of the larger operational environment; and
- instructions to provide a protected administrative capability through the use of either TOE capabilities, environmental capabilities, or a combination of the two.

142 Guidance pertaining to particular security functionality is also provided; requirements on such guidance are contained in the assurance activities specified in Section 4.1

4.3.2.1 AGD_OPE.1 Operational User Guidance

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

Developer Note: Rather than repeat information here, the developer should review the assurance activities for this component to ascertain the specifics of the guidance that the evaluators will be checking for. This will provide the necessary information for the preparation of acceptable guidance.

Content and presentation elements:

AGD_OPE.1.1C	The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C	The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C	The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4C	The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5C	The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6C	The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7C	The operational user guidance shall be clear and reasonable.
	Evaluator action elements:
AGD_OPE.1.1E	The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

Assurance Activity:

143 During operation, the activities to be described in the guidance fall into two broad categories; those that are performed by a (non-administrative) user, and those that are performed by an administrator. It should be noted that most procedures needed for non-administrative users are referenced in the assurance activities in Section 4.1.

144 With respect to the administrative functions, while several have also been described in Section 4.1, additional information is required as follows.

145 The operational guidance shall at a minimum list the processes running (or that could run) on the TOE in its evaluated configuration during its operation that are capable of processing data received on the network interfaces (there are likely more than one of these, and this is not limited to the process that "listens" on the network interface). It is acceptable to list all processes running (or that could run) on the TOE in its evaluated configuration instead of attempting to determine just those that process the network data. For each process listed, the administrative guidance will contain a short (e.g., one- or two-line) description of the process' function, and the privilege with which the service runs. "Privilege"

includes the hardware privilege level (e.g., ring 0, ring 1), any software privileges specifically associated with the process, and the privileges associated with the user role the process runs as or under.

146 The operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.

147 The documentation must describe the process for verifying updates to the TOE, either by checking the hash or by verifying a digital signature. The evaluator shall verify that this process includes the following steps:

- For hashes, a description of where the hash for a given update can be obtained. For digital signatures, instructions for obtaining the certificate that will be used by the FCS_COP.1(2) mechanism to ensure that a signed update has been received from the certificate owner. This may be supplied with the product initially, or may be obtained by some other means.

- Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory).

- Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes generation of the hash/digital signature.

4.3.2.2 AGD_PRE.1 Preparative procedures

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Developer Note: As with the operational guidance, the developer should look to the assurance activities to determine the required content with respect to preparative procedures.

Content and presentation elements:

AGD_ PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_ PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

AGD_ PRE.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

AGD_ PRE.1.2E The evaluator *shall apply* the preparative procedures to confirm that the TOE can be prepared securely for operation.

Assurance Activity:

148 As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms and components (that is, combination of hardware and operating system) claimed for the TOE in the ST.

149 The evaluator shall check to ensure that the following guidance is provided:

- As indicated in the introductory material, administration of the TOE is performed by one or more administrators that are a subset of the group of all users of the TOE. While it must be the case that the overall system (TOE plus Operational Environment) provide this capability, the responsibility for the implementation of the functionality can vary from totally the Operational Environment's responsibility to totally the TOE's responsibility. At a high level, the guidance must contain the appropriate instructions so that the Operational Environment is configured so that it provides the portion of the capability for which it is responsible. If the TOE provides no mechanism to allow separation of administrative users from the population of users, then the instructions, for instance, would cover the OS configuration of the OS I&A mechanisms to provide a unique (OS-based) identity for users, and further guidance would instruct the installer on the configuration of the DAC mechanisms of the OS using the TOE administrative identity (or identities) so that only TOE administrators would have access to the administrative executables. If the TOE provides some or all of this functionality, then the appropriate requirements are included in the ST from Appendix C, and the assurance activities associated with those requirements provide details on the guidance necessary for both the TOE and Operational Environment.

The evaluators shall also perform the following tests:

- Test 1 [Conditional]: If the separation of administrative users from all TOE users is performed exclusively through the configuration of the Operational Environment, the evaluators will, for each configuration claimed in the ST, ensure that after configuring the system according to the administrative guidance, non-administrative users are unable to access TOE administrative functions.

4.3.3 Class ATE: Tests

150 Testing is specified for functional aspects of the system as well as aspects that take advantage of design or implementation weaknesses. The former is done through the ATE_IND family, while the latter is through the AVA_VAN family. At the assurance level specified in this PP, testing is based on advertised functionality and interfaces with dependency on the availability of design information. One of the primary outputs of the evaluation process is the test report as specified in the following requirements.

4.3.3.1 ATE_IND.1 Independent testing - Conformance

151 Testing is performed to confirm the functionality described in the TSS as well as the administrative (including configuration and operation) documentation provided. The focus of the testing is to confirm that the requirements specified in Section 4.1 are being met, although some additional testing is

specified for SARs in Section 4.3. The Assurance Activities identify the minimum testing activities associated with these components. The evaluator produces a test report documenting the plan for and results of testing, as well as coverage arguments focused on the platform/TOE combinations that are claiming conformance to this PP.

Developer action elements:

ATE_IND.1.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.1.1C The TOE shall be suitable for testing.

Evaluator action elements:

ATE_IND.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2E The evaluator *shall test* a subset of the TSF to confirm that the TSF operates as specified.

Assurance Activity:

152 The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the body of this PP's Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluators must document in the test plan that each applicable testing requirement in the ST is covered.

153 The Test Plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platform and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary.

154 The test plan describes the composition of each platform to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluators are expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) is provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform.

155 The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.

4.3.4 Class AVA: Vulnerability assessment

156 For the first generation of this protection profile, the evaluation lab is expected to survey open sources to discover what vulnerabilities have been discovered in these types of products. In most cases, these vulnerabilities will require sophistication beyond that of a basic attacker. Until penetration tools are created and uniformly distributed to the evaluation labs, evaluators will not be expected to test for these vulnerabilities in the TOE. The labs will be expected to comment on the likelihood of these vulnerabilities given the documentation provided by the vendor. This information will be used in the development of penetration testing tools and for the development of future protection profiles.

4.3.4.1 AVA_VAN.1 Vulnerability survey

	Developer action elements:
AVA_VAN.1.1D	The developer shall provide the TOE for testing.
	Content and presentation elements:
AVA_VAN.1.1C	The TOE shall be suitable for testing.
	Evaluator action elements:
AVA_VAN.1.1E	The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.1.2E	The evaluator *shall perform* a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.1.3E	The evaluator *shall conduct* penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

Assurance Activity:

157 As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in WLAN Client products in general, as well as those that pertain to the particular TOE . The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. For example, if the vulnerability can be detected by pressing a key combination on boot-up, for example, a test would be suitable at the assurance level of this PP. If

exploiting the vulnerability requires an electron microscope and a tank of liquid nitrogen, for instance, then a test would not be suitable and an appropriate justification would be formulated.

4.3.5 Class ALC: Life-cycle support

158 At the assurance level provided for TOEs conformant to this PP, life-cycle support is limited to end-user-visible aspects of the life-cycle, rather than an examination of the TOE vendor's development and configuration management process. This is not meant to diminish the critical role that a developer's practices play in contributing to the overall trustworthiness of a product; rather, it's a reflection on the information to be made available for evaluation at this assurance level.

4.3.5.1 ALC_CMC.1 Labeling of the TOE

159 This component is targeted at identifying the TOE such that it can be distinguished from other products or version from the same vendor and can be easily specified when being procured by an end user.

Developer action elements:

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements:

ALC_CMC.1.1C The TOE shall be labeled with its unique reference.

Evaluator action elements:

ALC_CMC.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

Assurance Activity:

160 The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.

4.3.5.2 ALC_CMS.1 TOE CM coverage

161 Given the scope of the TOE and its associated evaluation evidence requirements, this component's assurance activities are covered by the assurance activities listed for ALC_CMC.1.

Developer action elements:

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

Evaluator action elements:

ALC_CMS.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

Assurance Activity:

162 The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.

4.4 Rationale for Security Assurance Requirements

163 The rationale for choosing these security assurance requirements is that this is the first Standard Protection Profile for this technology. The first Protection Profile is used to ascertain best development practices. If vulnerabilities are found in these types of products, then more stringent security assurance requirements will be mandated based on actual vendor practices.

Appendix A: Supporting Tables, References, and Acronyms

[1] Common Criteria for Information Technology Security Evaluation (CC) Version 3.1, R3 July 2009

[2] Draft Consistency Instruction Manual, for Basic Robustness Environments, Release 4.0, CC version 3.1, 2008

[3] Federal Information Processing Standard Publication (FIPS-PUB) 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, May 25, 2001 (CHANGE NOTICES (12-03-2002)

[4] Federal Information Processing Standard Publication (FIPS-PUB) 180-3, Secure Hash Standard, October 2008

[5] Federal Information Processing Standard Publication (FIPS-PUB) 186-3, Digital Signature Standard (DSS), June 2009

[6] Federal Information Processing Standard Publication (FIPS-PUB) 197, Specification for the Advanced Encryption Standard (AES), November 26, 2001

[7] NIST Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004

[8] NIST Special Publication 800-57, Recommendation for Key Management, March 2007

[9] NIST Special Publication 800-63, Electronic Authentication Guideline, April 2006

[10] NIST Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised) , March 2007

[11] NSA Glossary of Terms Used in Security and Intrusion Detection, Greg Stocksdale, NSA Information Systems Security Organization, April 1998. Need to update to CNSS 4009

[12] RFC 2865 Remote Authentication Dial In User Service (RADIUS), June 2000

[13] RFC 2868 RADIUS Attributes for Tunnel Protocol Support, June 2000

[14] RFC 3575 IANA Considerations for RADIUS, July 2003

[15] RFC 3579 RADIUS (Remote Authentication Dial In User Service Support For Extensible Authentication Protocol (EAP), September 2003

[16] RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, September 2003

[17] RFC 5216 The EAP-TLS Authentication Protocol, March 2008

[18] WPA2 Standard

AES	Advanced Encryption Standard
AF	Authorization factor
AS	Authentication Server
CAVS	Cryptographic Algorithm Validation System
CC	Common Criteria
CCTL	Common Criteria Testing Laboratory
CM	Configuration management
COTS	Commercial Off-The-Shelf
CMVP	Cryptographic Module Validation Program
DRBG	Deterministic Random Bit Generator
DoD	Department of Defense
EAL	Evaluation Assurance Level
ES	Encryption Subsystem
FIPS	Federal Information Processing Standards
ISSE	Information System Security Engineers
IT	Information Technology
OSP	Organization Security Policy
PP	Protection Profile
PUB	Publication
RBG	Random Bit Generator
SAR	Security Assurance Requirements
SF	Security Function
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification

Appendix B: NIST SP 800-53/CNSS 1253 Mapping

Several of the NIST SP 800-53/CNSS 1253 controls are either fully or partially addressed by compliant TOEs. This section outlines the requirements that are addressed, and can be used by certification personnel to determine what, if any, additional testing is required when the TOE is incorporated into its operational configuration.

Application Note: In this version, only a simple mapping is provided. In future versions, additional narrative will be included that will provide further information for the certification team. This additional information will include details regarding the SFR to control mapping discussing what degree of compliance is provided by the TOE (e.g., fully satisfies the control, partially satisfies the control). In addition, a comprehensive review of the specified assurance activities, and those evaluation activities that occur as part of satisfying the SARs will be summarized to provide the certification team information regarding how compliance was determined (e.g., document review, vendor assertion, degree of testing/verification). This information will indicate to the certification team what, if any, additional activities they need to perform to determine the degree of compliance to specified controls.

Since the ST will make choices as far as selections, and will be filling in assignments, a final story cannot necessarily be made until the ST is complete and evaluated. Therefore, this information should be included in the ST in addition to the PP. Additionally, there may be some necessary interpretation (e.g.,"modification") to the activities performed by the evaluator based on a specific implementation. The scheme could have the oversight personnel (e.g., Validators) fill in this type of information, or could have this done by the evaluator as part of the assurance activities. The verification activities are a critical piece of information that must be provided so the certification team can determine what, if anything, they need to do in addition to the work of the evaluation team.

Identifier	Name	Applicable SFRs
AC-3	Access Enforcement	FMT_SMF.1
AU-2	Auditable Events	FAU_GEN.1
AU-2(4)		FAU_GEN.1
AU-3	Content of Audit Records	FAU_GEN.1
AU-3(1)		FAU_GEN.1
AU-7	Audit Reduction and Report Generation	FAU_SEL.1
AU-10	Non-Repudiation	FCS_COP.1(2)
AU-12	Audit Generation	FAU_GEN.1
CM-5	Access Restrictions for Change	FPT_TUD_EXT.1
IA-3	Device Identification and Authentication	FCS_EAP-TLS_EXT.1, FIA_8021X_EXT.1, FTP_ITC
IA-5	Authenticator Management	FIA_X509_EXT.1
SC-4	Information in Shared Resources	FDP_RIP.2
SC-8	Transmission Integrity	FTP_ITC.1
SC-9	Transmission Confidentiality	FTP_ITC.1
SC-12	Cryptographic Key Establishment and Management	FCS_CKM.1, FCS_CKM.2, FCS_CKM_EXT.4
SC-13	Use of Cryptography	FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_COP.1(5), FCS_RBG_EXT.1
SI-6	Security Functionality Verification	FPT_TST_EXT.1

Appendix C: Additional Requirements

164 *For this draft of the PP, this appendix contains additional components without supporting threats, objectives, rationale, or (in some cases) assurance activities. In tandem with the first review cycle, this supporting information will be developed and incorporated into the next release of the PP. Comments on the information contained in this section (both on whether the requirements contained are applicable to the potential conformant TOEs as well as requirements that are not contained in this appendix that are widely applicable to WLAN Client products) are welcome and solicited.*

165 As indicated in the introduction to this PP, there are several capabilities that a TOE may implement and still be conformant to this PP. These capabilities are not required, creating a dependency on the IT environment (for instance, identification and authentication of administrators of the TOE). However, if a TOE does implement such capabilities, the ST will take the following information and include it in their ST. Requirements not contained in this appendix may be included in the ST, but are subject to review and acceptance by the National Scheme overseeing the evaluation before a conformance claim to this PP can be made.

C.1 Class: Security Audit (FAU)

166 If audit review and/or storage are supported by the TOE the following audit requirements must be included in the ST, as appropriate.

Audit Review (FAU_SAR.1)

FAU_SAR.1	**Audit Review**
FAU_SAR.1.1	The TSF shall provide **Authorized Administrators** with the capability to read **all audit data** from the audit records.
FAU_SAR.1.2	**Refinement:** The TSF shall provide the audit records in a manner suitable for the ~~user~~ **Authorized Administrators** to interpret the information.

Restricted Audit Review (FAU_SAR.2)

FAU_SAR.2	**Restricted Audit Review**
FAU_SAR.2.1	**Refinement:** The TSF shall prohibit all users read access to the audit records **in the audit trail, except Authorized Administrators.**

FAU_STG_EXT.4	**Prevention of Audit Data Loss**
FAU_STG_EXT.4.1	The TSF shall provide the Authorized Administrator the capability to select one or more of the following actions: a) prevent auditable events, except those taken by the Authorized Administrator, and

b) overwrite the oldest stored audit records

to be taken if the audit trail is full.

Application Note:

167 *The TOE provides the Authorized Administrator the option of preventing audit data loss by preventing auditable events from occurring. The Authorized Administrator actions under these circumstances are not required to be audited. The TOE also provides the Authorized Administrator the option of overwriting "old" audit records rather than preventing auditable events, which may protect against a denial-of-service attack.*

C.2 Class: Identification and Authentication (FIA)

168 In the case that the TOE provides administrative capability, there are a number of requirements that can be applied to specify the capability, including remote administration, local administration, and protection of the administrative session. For this version of the PP, it is acceptable to use the administrative requirements from the Wireless Access System Protection Profile to specify such a capability for the client.

169 In the case that the TOE provides the capability to store and manage certificates used during the exchanges, the following requirement can be included in the ST.

X509 Certificates (FIA_X509_EXT)

FIA_X509_EXT.2	**Extended: X.509 Certificate Storage and Management**
FIA_X509_EXT.2.2	The TSF shall store and protect certificate(s) from unauthorized deletion and modification.
FIA_X509_EXT.2.3	The TSF shall provide the capability for Authorized Administrators to load X.509v3 certificates into the TOE for use by the security functions specified in this PP.

Application Note:

170 *FIA_X509_EXT.1.2 applies to certificates that are used and processed by the TSF. Certificates that are used and process by other components in the Operational Environment (e.g., the RADIUS server) are not intended to be covered by this element.*

Assurance Activity:

171 *The TSS shall describe all certificate stores implemented that contain certificates used to meet the requirements of this PP. This description shall contain information pertaining to how certificates are loaded into the store, and how the store is protected from unauthorized access.*

172 *The evaluator shall perform the following tests for each function in the system that requires the use of certificates:*

- *Test 1: The evaluator shall demonstrate that using a certificate without a valid certification path results in the function failing. The evaluator shall then load a certificate or certificates needed to validate the certificate to be used in the function, and demonstrate that the function succeeds. The evaluator then shall delete one of the certificates, and show that the function fails.*

C.3 Audit Requirements

173 Depending on the specific requirements selected by the ST author from this appendix, the ST author should include the appropriate auditable events in the corresponding table in the ST for the requirements selected.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_SAR.1	None.	
FAU_SAR.2	Attempts to read the audit records.	None.
FAU_STG_EXT.4	Audit trail reaching capacity.	None.
FIA_X509_EXT.2	Attempts to load certificates. Attempts to revoke certificates.	None.

Appendix D: Document Conventions

174 Except for replacing United Kingdom spelling with American spelling, the notation, formatting, and conventions used in this PP are consistent with version 3.1 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the PP reader.

175 The notation, formatting, and conventions used in this PP are largely consistent with those used in version 3.1 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the PP user. The CC allows several operations to be performed on functional and assurance requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in Appendix C4 of Part 1 of the CC 3.1. Each of these operations is used in this PP.

Refinement Convention

176 The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by the word "Refinement" in **bold text** after the element number and the additional text in the requirement in bold text.

Selection Convention

177 The **selection** operation is used to select one or more options provided by the CC in stating a requirement (see appendix C.4.3 Part 1, CC 3.1). Selections that have been made by the PP authors show the selection in **bold** characters, the brackets and the word "selection" removed. Selections to be filled in by the ST author are shown in square brackets with an indication that a selection is to be made, [selection:].

Assignment Convention

178 The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password (see appendix C.4.2 Part 1, CC 3.1). Showing the value in **bold** characters denotes assignments that have been made by the PP authors, the brackets and the word "assignment" are removed. Assignments to be filled in by the ST author are shown in square brackets with an indication that an assignment is to be made [assignment:].

Iteration Convention

179 The **iteration** operation is used when a component is repeated with varying operations (see appendix C.4.1 Part 1, CC 3.1). The iteration number (iteration_number) is show in parenthesis following the component identifier.

180 The iteration operation may be performed on every component. The PP/ST author performs an iteration operation by including multiple requirements based on the same component. Each iteration of a component shall be different from all other iterations of that component, which is realized by completing assignments and selections in a different way, or by applying refinements to it in a different way.

Extended Requirement Convention

181 Extended requirements are permitted if the CC does not offer suitable requirements to meet the authors' needs. Extended requirements must be identified and are required to use the CC

class/family/component model in articulating the requirements. Extended requirements will be indicated with the "EXT" inserted within the component.

Application Notes

182 Application notes contain additional supporting information that is considered relevant or useful for the construction of security targets for conformant TOEs, as well as general information for developers, evaluators, and ISSEs. Application notes also contain advice relating to the permitted operations of the component.

Assurance Activities

183 Assurance activities serve as a Common Evaluation Methodology for the functional requirements levied on the TOE to mitigate the threat. The activities include instructions for evaluators to analyze specific aspects of the TOE as documented in the TSS, thus levying implicit requirements on the ST author to include this information in the TSS section. In this version of the PP these activities are directly associated with the functional and assurance components, although future versions may move these requirements to a separate appendix or document.

Appendix E: Glossary of Terms

Access Point – provides the network interface that enables wireless client hosts access to a wired network. Once authenticated as trusted nodes on the wired infrastructure, the APs provide the encryption service on the wireless network between the wireless client and the RF interface of the AP.

Administrator – a user that has administrative privilege to configure the TOE.

Authentication Server – an authentication server on the wired network which receives authentication credentials from wireless clients for authenticating.

Authentication Credentials – the information the system uses to verify that the user or administrator is authorized to access the TOE or network. Credentials can be as simple as username and password or stronger certificates.

Critical Security Parameter (CSP) – security related information, e.g. secret and private cryptographic keys, and authentication data such as passwords and PINs, whose disclosure or modification can compromise the security of a cryptographic module.

Entropy Source – this cryptographic function provides a seed for a random number generator by accumulating the outputs from one or more noise sources. The functionality includes a measure of the minimum work required to guess a given output and tests to ensure that the noise sources are operating properly.

Extensible Authentication Protocol (EAP) – an authentication framework used in wireless networks. The TOE supports EAP-TLS. EAP-TLS uses PKI to authenticate both the authentication server and the wireless client.

FIPS-approved cryptographic function – a security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either: 1) specified in a Federal Information Processing Standard (FIPS), or 2) adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS.

IEEE 802.1X - IEEE standard for port-based network access control that defines an authentication mechanism to devices (wireless clients) to attach to a wired network. The main components needed to support IEEE 802.1X is the supplicant (wireless client), authenticator (the TOE), and authentication server.

IT Environment – hardware and software that are outside the TOE boundary that the support the TOE functionality and security policy.

Operational Environment – the environment in which the TOE is operated.

SAR (Security Assurance Requirements) – describes the development and evaluation methodologies for the developer and the lab to demonstrate compliance with the Security Functional Requirements. The SAR should describe specific tests for the developers and the evaluators.

SFR (Security Functional Requirement) – describes security functions that must be met by the TOE. The SFR's are tailored for the specific technology.

ST (Security Target) – describes and identifies the security properties of the TOE.

TOE (Target of Evaluation) – refers to a product or set of products that include hardware, software, and guidance that are to be evaluated against the requirements in this PP.

TOE Security Functionality (TSF) – a set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP) – a set of rules that regulate how assets are managed, protected and distributed within a TOE.

TOE Summary Specification (TSS) – a description of how the TOE satisfies all of the SFRs.

Unauthorized User – a user who has not been authorized by the administrator to use the TOE.

Appendix F: PP Identification

Tile:	Protection Profile for Wireless Local Area Network (WLAN) Clients
Version:	1.0
Sponsor:	National Information Assurance Partnership (NIAP)
CC Version:	Common Criteria for Information Technology Security Evaluation (CC) Version 3.1, R3 July 2009
Keywords:	Authentication Server , WLAN Client, WLAN Access System, EAP, EAP-TLS, IEEE 802.11, IEEE 802.1X