Protection Profile for Wireless Local Area Network (WLAN) Access Systems

Information Assurance Directorate

01 December 2011

Version 1.0

Table of Contents

List of Tables

Revision History

Version	Date	Description
1.0	01 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) Access Systems 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 Access System. 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 Access System. The WLAN Access System provides secure wireless access to a wired network by controlling the link between the wireless client and that wired network. The TOE may be implemented by one or more physical components.

1.1.1 Usage and major security features of TOE

4 The WLAN Access System contributes to a secure wireless access solution for providing secure communication between a user (wireless client) and a wired network (e.g., enterprise network) by providing centralized management functions, policy control, and cryptographic services to support administration, authentication, encryption, and the protection and handling of data in transit. The WLAN Access System requires the wireless client to perform 802.1X authentication, relying on an authentication server to authenticate the client, before providing network access. The WLAN Access System acts as a pass through device between the wireless client and authentication server. Secure communication tunnels are formed only if authentication is successful. Following successful authentication, the WLAN Access System derives a session key with each wireless client. All subsequent communication between the WLAN Access System and the wireless client is encrypted. The WLAN Access System decrypts traffic that originates from an authenticated wireless client and passes the traffic into the backend network. Likewise, the WLAN Access System encrypts traffic sent from the backend network to the authenticated wireless client. The WLAN Access System supports multiple simultaneous wireless connections and is capable of establishing and terminating multiple cryptographic tunnels to and from those peers.

5 Conformant TOEs will meet the Expanded Service Set (ESS) requirements in the 802.11 standard using 802.1X authentication; there are no requirements and subsequently no verified claims relating to Independent Basic Service Set (IBSS) operations, or ESS operations using a pre-shared key.

6 The TOE maintains an administrative role. Administrators must be authenticated before they can manage the TOE. The WLAN Access System supports both a remote authentication mechanism and a local authentication mechanism to perform administrator login. The remote administrator can access the WLAN Access System remotely through a secure connection implemented by SSH or TLS/HTTPS, for example. The ability to configure the TOE from the wireless side is disabled by default.

7 If the WLAN Access System is implemented by two or more physical components, a secure channel between TOE components is provided to protect control/configuration data exchanged between the components. Similarly, IT entities in the operational environment (RADIUS Server, Audit Server) will also communicate with the TOE over a secure channel. All of the IT entities (TOE components and those

external to the TOE) will be authenticated through the use of either shared secrets or X.509v3 machine certificates for authentication.

8 It is assumed that all components of the WLAN Access System are implemented properly and contain no critical design mistakes. The vendor is required to provide configuration guidance (AGD_PRE, AGD_OPR) to correctly install and administer the TOE for every operational environment supported.

1.1.2 Encryption

9 The WLAN Access System is expected to encrypt wireless traffic flowing between two devices that are geographically separated. The WLAN Access System serves as an endpoint for a WLAN tunnel and performs a number of cryptographic functions related to establishing and maintaining the tunnel. 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.

10 In addition to the protection of wireless traffic, the WLAN Access System must provide the capability for secure communications for remote administrator sessions as well as protect RADIUS packets between itself and an external authentication server. These measures help prevent unauthorized access from internal and external interfaces through use of peer authentication, data confidentiality and integrity, and protocol compliance.

1.1.3 Administration

11 The WLAN Access System must provide an administrator role to install, configure, and maintain the TOE. The TOE will provide both remote and local authenticated access to perform administrative duties. Although this PP requires one administrative role, the ST author can include additional administrative roles to further separate administrative functions to distinct administrative roles (e.g., cryptographic administrator, audit administrator). In this case, the ST author will need to refine the FMT_SMR requirement and update applicable security management requirements to restrict functionality to the appropriate administrator role.

12 Authorized administrators will correctly follow any required configuration guidance. The TOE shall be capable of providing the following administrative functions:

- Specify a maximum number of successive failed authentication attempts that will be permitted by a remote administrator;
- Modifying the behavior of cryptographic functions;
- Configuring communications with an external authentication server, an NTP server, and an audit server; and
- Enable, disable, and configure audit collection.

1.1.4 Protocol Compliance

13 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 WLAN Access System will implement the RADIUS protocol (RFC 2865) as well for communication with an authentication server with additional support for passing the EAP packets (2869).

14 The TOEs meeting this PP will also implement and conform to the Internet Engineering Task Force (IETF) Internet Protocol Security (IPsec) Encapsulating Security Payload (ESP) protocol to further protect the RADIUS communications with an authentication server. IPsec, SSH, or TLS/HTTPS are also used to ensure secure communication with a remote administrator.

1.1.5 Available non-TOE Hardware/Software/Firmware

15 The TOE supporting environment is significant because the WLAN Access System is contributing to an 802.1X WLAN solution. 802.1X defines a framework for providing authenticated access to WLAN networks. In 802.1X terminology, the WLAN Access System is the authenticator and acts as a relay for EAP-TLS messages being exchanged between the wireless client and the authentication server. The wireless client and RADIUS authentication server are not part of the TOE and considered part of the TOE's operational environment. The TOE can be implemented by one or more components all of which comprise the TOE.

16 The TOE also relies on a non-TOE audit server for storage and review of audit records. Although the TOE generates audit records, the storage of these audit records and the ability to allow the administrator to review these audit records is provided by the operational environment.

2 Security Problem Definition

17 This Protection Profile (PP) is written to address the situation when network packets cross the boundary between a wired private network and a wireless client. To protect the data in-transit from disclosure and modification, a WLAN Access System is created to establish secure communications. The WLAN Access System provides one end of the secure cryptographic tunnel and performs encryption and decryption of network packets in accordance with a WLAN Access System security policy negotiated with its authenticated wireless client.

18 The proper installation, configuration, and administration of the WLAN Access System are critical to its correct operation such that proper handling of the TOE by an administrator is also addressed.

19 This chapter identifies the following:

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

2.1 Threats

20 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 access system. Signal jamming and denial of service attacks are common and hard to prevent. The WLAN Access System supports multiple simultaneous wireless connections and is capable of establishing and terminating multiple cryptographic tunnels to and from those peers. These measures, along with requirements on protocol compliance and quotas on resource utilization, help mitigate denial of service (DoS) attacks and prevent resource exhaustion.

21 This PP also does not include requirements that can protect against an insider threat; this includes the compromise of an authorized endpoint (e.g., an authorized client device, or authorized IT entity/peer). Authorized users are not considered hostile or malicious and are trusted to follow appropriate guidance. Only authorized personnel should have access to equipment, administrative consoles, and the device. Therefore, the primary threat agents are the unauthorized entities that try to gain access to the protected network. Because the request for network access by a legitimate entity and authentication credentials can originate from a non-secure area, it is subject to network attacks and must be protected from disclosure and modification. A malicious entity could try to steal authentication credentials and pretend to be a legitimate user, for example, by sniffing the packets exchanged between the TOE and a legitimate WLAN client.

22 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.

23 Likewise, remote users trying to gain administrator access to the TOE itself (versus the network protected by the TOE) defines another threat agent. As a non-general purpose system, the TOE only allows administrators direct access to the TOE to allow for installation, configuration, and maintenance. Because the TOE supports remote administration, the TOE is subject to network attacks that manipulate

the data entered by a valid administrator or that attempt to gain administrator privileges by obtaining remote administrator login.

24 Network attacks, such as those described above, against the TOE and the network it protects 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 well-known flaws. Timely application of patches increases the likelihood that the product will be able to maintain and enforce its security policy. However, the updates to be applied must be from a trusted source; otherwise, an attacker can write their own "update" that instead contains malicious code of their choosing.

25 Although the authorized administrator is assumed to be non-hostile and trustworthy, the administrator is not considered infallible and thus some administrator actions could adversely affect the security of the TOE. For example, an administrator may unknowingly execute a program that contains malicious code or unintentionally mis-configure a security mechanism. Negotiation of security policies that result in weak protocol options being used to establish a WLAN connection is a concern that could result in the disclosure or modification of user and TSF data. Protocol interoperability and mutual agreed upon security policies requiring strong encryption are imperative for establishing wireless protection, as is the capability for the administrator to configure the TOE to use strong algorithms/options.

26 Protecting interactions with the TOE is critical to the security of the network and device. However, any security provided is useless if access to the authenticated session itself is obtained. In many operational environments, the machines used to manage a network device are accessible to those other than the administrators. There are two types of administrative sessions that need to be considered; those where the administrator is connected to the device locally (i.e., via a console) and those where the administrator is connected remotely. Regardless of the type of connection, if an active session was left unattended, anyone with physical access to the machine would have access to the session, regardless of authorization. Compromise to the machine and the underlying protected network would be obtained.

27 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. Audit compromise could allow the ability to delete the audit trail and modify audit record generation to hide any nefarious actions taken on the TOE. This could mask and fail to alert a trusted administrator to potential problems as well as make it difficult to identify who caused the malicious action. Compromise of TSF data includes authentication data, session keys, role/user information, security mechanisms, and the data the TOE protects.

28 In addition to network attacks, malicious updates, and undetected actions, errors in the TOE itself can result in threats to user data, the TOE, and the protected network that must be mitigated. The TOE must ensure that data is not persistent when resources are released by one user/process and allocated to another. Otherwise, data traversing the TOE could inadvertently be re-used and sent to a different user; this may cause a compromise that is unacceptable. The TOE must also maintain a secure state when failures are detected. Security mechanisms of the TOE generally build up from a primitive set of mechanisms (e.g., memory management, privileged modes of process execution) to more complex sets of mechanisms. Failure of the primitive mechanisms could lead to a compromise in more complex mechanisms, resulting in a compromise or failure of the TSF.

29 The following table lists the threats addressed by the WLAN Access System 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.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.RESOURCE_EXHAUSTION	A process or user may deny access to TOE services by exhausting critical resources on the TOE.
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

30 The Organization Security Policies were selected because of their applicability to the WLAN Access System. 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.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ADMIN_ACCESS	Administrators shall be able to administer the TOE both locally and remotely through protected communications channels.
P.COMPATIBILITY	The TOE must meet Request for Comments (RFC) requirements for implemented protocols to facilitate inter-operation with other network equipment (e.g., certificate authority, NTP server) using the same protocols.
P.EXTERNAL_SERVERS	The TOE must support standardized (RFCs) protocols for communication with a centralized audit server and a RADIUS authentication server.

2.3 Assumptions

31 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 not be able to provide all of its security functionality anymore. Assumptions can be on physical, personnel and connectivity of the operational environment.

Table 3: TOE Assumptions

Assumption	Description of Assumption
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available to the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.NO_TOE_BYPASS	Information cannot flow between the wireless client and the internal wired network without passing through the TOE.

Assumption	Description of Assumption
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

32 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 Security Functionality Requirements (SFR). The TOE is evaluated against the SFR.

3.1 Security Objectives for the TOE

33 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 has to meet 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 users are not communicating with some other entity pretending to be the TOE, and that the TOE is communicating with an authorized IT entity and not some other entity pretending to be an authorized IT entity.
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.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.FAIL_SECURE	The TOE shall fail in a secure manner following failure of the power-on self tests.
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
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.REPLAY_DETECTION	The TOE will provide a means to detect and reject the replay of authentication data and other TSF data and security attributes.
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.RESOURCE_AVAILABILITY	The TOE shall provide mechanisms that mitigate user attempts to exhaust TOE resources (e.g., persistent storage).
O.ROBUST_TOE_ACCESS	The TOE will provide mechanisms that control an administrator's logical access to the TOE and to control administrative access from a wireless client.

Objective	Objective Description
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.TIME_STAMPS	The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these timestamps.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
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_CLIENT_ACCESS	The TOE will provide the capability to restrict a wireless client in connecting to the TOE.

3.2 Security Objectives for the Operational Environment

34 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.

35 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_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available to the TOE, other than those services necessary for the operation, administration and support of the TOE.
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 IT environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

3.3 Security objective rationale

36 This section describes the rationale for the Security Objectives as defined in Section 3. 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.ADMIN_ERROR An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.	O.TOE_ADMINISTRATION The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators. OE. TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.	O.TOE_ADMINISTRATION plays a role in mitigating this threat by limiting the functions an administrator can perform. Revoking administrator access when not needed also reduces the chance that an error may occur. OE.TRUSTED_ADMIN mitigates this threat by ensuring the administrators are properly trained and the administrative guidance instructs the administrator how to properly configure the environment and TOE to avoid mistakes.
T.RESOURCE_EXHAUSTION A process or user may deny access to TOE services by exhausting critical resources on the TOE.	O.RESOURCE_AVAILABILITY The TOE shall provide mechanisms that mitigate user attempts to exhaust TOE resources (e.g., persistent storage).	O.RESOURCE_AVAILABILITY mitigates the threat by ensuring that the TOE has mechanisms and policy in place to deal with attempts to exhaust resources.
T.TSF_FAILURE Security mechanisms of the TOE may fail, leading to a compromise of the TSF.	O.FAIL_SECURE The TOE shall fail in a secure manner following failure of the power-on self tests. 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.FAIL_SECURE contributes to mitigating this threat by ensuring that on a detected failure the TOE maintains a secure state. 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	O.AUTH_COMM The TOE will provide a means to ensure users are not communicating with some other entity pretending to be the TOE, and that the TOE is communicating with an authorized IT entity and not some other entity pretending to be an authorized IT entity.	O.AUTH_COMM works to mitigate this threat by ensuring that the TOE identifies and authenticates all users prior to allowing TOE access or setting up a security association with that user. The TOE must also be capable of sending its own credentials to users to ensure mutual authentication prior to

Threat/Policy	Objectives Addressing the Threat and Policies	Rationale
obtain identification and authentication 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 TSF data that is transmitted between physically separated portions of the TOE, or stored outside the TOE. O.PROTECTED_COMMUNICATIONS The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities. O.ROBUST_TOE_ACCESS The TOE will provide mechanisms that control an administrator's logical access to the TOE and to control administrative access from a wireless client. O.SESSION_LOCK The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked. O.TOE_ADMINISTRATION The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators. O.REPLAY_DETECTION The TOE will provide a means to detect and reject the replay of authentication data and other TSF data and security attributes. O.WIRELESS_CLIENT_ACCESS The TOE will provide the capability to restrict a wireless client in connecting to the TOE.	communication. O.CRYPTOGRAPHIC_FUNCTIONS contributes to mitigating this threat by providing the underlying cryptographic functionality required by other protection mechanisms. O.PROTECTED_COMMUNICATIONS contributes to mitigating this threat by ensuring protection of the communication between the TOE and authorized administrator while transmitting data. O.ROBUST_TOE_ACCESS mitigates this threat by requiring the TOE to identify and authenticate all administrators prior to allowing any TOE access or any TOE mediated access on behalf of those administrators. O.SESSION_LOCK mitigates this threat by requiring the TOE to provide a way for the user to lock a session or for the TOE to lock after a certain time-period which ensures an authorized session cannot be hijacked at the terminal. O.TOE_ADMINISTRATION requires the TOE to provide mechanisms (e.g., local authentication, remote authentication, means to configure and manage the TOE both remotely and locally) that allow remote and local administration of the TOE. O.REPLAY_DETECTION prevents unauthorized access by replaying sessions (or portions of sessions) from legitimate administrators or entities that have been captured by a malicious actor. O.WIRELESS_CLIENT_ACCESS mitigates the threat by providing

Threat/Policy	Objectives Addressing the Threat and Policies	Rationale
		mechanisms to restrict wireless client access according to the desired security posture of the TOE.
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
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 and send those data to an external IT entity.	O.SYSTEM_MONITORING mitigates this threat by providing the administrator with the capability of configuring the audit mechanism to record the actions of a specific user, or review the audit trail based on the identity of the user.
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.ACCESS_BANNER The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.	O.DISPLAY_BANNER The TOE will display an advisory warning regarding use of the TOE.	O.DISPLAY_BANNER satisfies this policy by ensuring that the TOE displays an Authorized Administrator configurable banner that provides all users with a warning about the unauthorized use of the TOE.
P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE.	O.ROBUST_TOE_ACCESS The TOE will provide mechanisms that control an administrator's logical access to the TOE and to control administrative access from a wireless client. O.SYSTEM_MONITORING The TOE will provide the capability to detect and create records of security-relevant events associated with users. O.TIME_STAMPS The TOE shall provide reliable time	O.ROBUST_TOE_ACCESS supports this policy by requiring the TOE to identify and authenticate all administrators prior to allowing any TOE access or any TOE mediated access on behalf of those administrators. O.SYSTEM_MONITORING supports this policy by providing the administrator with the capability of configuring the audit mechanism to record the actions of a specific user, or review the audit trail based on

Threat/Policy	Objectives Addressing the Threat and Policies	Rationale
	stamps and the capability for the administrator to set the time used for these timestamps.	the identity of the user. O.TIME_STAMPS plays a role in supporting this policy by requiring the TOE to provide a reliable time stamp. This will be used when audit records are generated, allowing administrators to tie auditable actions to the time those actions took place, perhaps on disparate systems. This ability aids in proving accountability for users whose actions cause those audit records to be generated.
P.ADMIN_ACCESS Administrators shall be able to administer the TOE both locally and remotely through protected communications channels.	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.PROTECTED_COMMUNICATIONS The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities. O.TOE_ADMINISTRATION The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.	O.CRYPTOGRAPHIC_FUNCTIONS contributes to mitigating this threat by providing the underlying cryptographic functionality required by other protection mechanisms. O.PROTECTED_COMMUNICATIONS contributes to mitigating this threat by ensuring protection of the communication between the TOE and authorized administrator while transmitting data. O.TOE_ADMINISTRATION supports this policy by requiring the TOE to provide mechanisms (e.g., local authentication, remote authentication, means to configure and manage the TOE both remotely and locally) that allow remote and local administration of the TOE.
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.

Threat/Policy	Objectives Addressing the Threat and Policies	Rationale
P.EXTERNAL_SERVERS The TOE must support standardized (RFCs) protocols for communication with a centralized audit server and a RADIUS authentication server.	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 the policy by ensuring that the TOE can communicate with an external audit server and RADIUS authentication server, even when auditing and authentication are also provided locally.

37 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_GENERAL_PURPOSE It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available to the TOE, other than those services necessary for the operation, administration and support of the TOE.	OE.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g., compilers or user applications) available to the TOE, other than those services necessary for the operation, administration and support of the TOE.	OE.NO_GENERAL_PURPOSE ensures the TOE does not include any general-purpose computing or storage capabilities. This will protect the TSF data from malicious processes.
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 provided by the environment.	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.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 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

Assumption	Objectives Addressing the Assumption	Rationale
		and TOE to avoid mistakes.

4 Security Requirements and Rationale

38 The Security Requirements are divided into functional requirements and assurance requirements. The Security Functional Requirements (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.

39 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.

40 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.

41 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.

42 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

Table 8: TOE Security Functional Requirements

Functional Class	Functional Components
Security Audit Class (FAU)	FAU_GEN.1 Audit Data Generation
	FAU_GEN.2 User Audit Association
	FAU_SEL.1 Selective Audit
	FAU_STG.1 Protected Audit Trail Storage (Local Storage)
	FAU_STG_EXT.1 External Audit Trail Storage
	FAU_STG_EXT.3 Action in Case of Loss of Audit Server Connectivity
Cryptographic Support Class (FCS)	FCS_CKM.1(1) Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)
	FCS_CKM.1(2) Cryptographic Key Generation (Asymmetric Keys)

Functional Class	Functional Components
	FCS_CKM.2(1) Cryptographic Key Distribution (PMK)
	FCS_CKM.2(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_IPSEC_EXT.1 Extended: Internet Protocol Security (IPsec) Communications
	FCS_RBG_EXT.1 Extended: Cryptographic Operation: Random Bit Generation
User Data Protection Class (FDP)	FDP_RIP.2 Full Resident Information Protection
Identification and Authentication Class (FIA)	FIA_AFL.1 Authentication Failure Handling
	FIA_PMG_EXT.1 Password Management
	FIA_UIA_EXT.1 User Identification and Authentication
	FIA_UAU_EXT.5 Extended: Password-based Authentication Mechanisms
	FIA_UAU.6 Re-authenticating
	FIA_UAU.7 Protected Authentication Feedback
	FIA_8021X_EXT.1 Extended: 802.1X Port Access Entity (Authenticator) Authentication
	FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
	FIA_X509_EXT.1 Extended: X509 Certificates
Security Management Class (FMT)	FMT_MOF.1 Management of Security Functions Behavior
	FMT_MTD.1(1) Management of TSF Data (General TSF Data)
	FMT_MTD.1(2) Management of TSF Data (Reading of Authentication Data)
	FMT_MTD.1(3) Management of TSF Data (for reading of all symmetric keys)
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security Management Roles
Protection of the TSF (FPT)	FPT_FLS.1 Fail Secure
	FPT_RPL.1 Replay Detection
	FPT_STM.1 Reliable Time Stamp
	FPT_TST_EXT.1 Extended: TSF Testing
	FPT_TUD_EXT.1 Extended: Trusted Update
Resource Utilization (FRU)	FRU_RSA.1 Maximum Quotas
TOE Access (FTA)	FTA_SSL_EXT.1 TSF-initiated session locking

Functional Class	Functional Components
	FTA_SSL.3 TSF-initiated termination
	FTA_SSL.4 User-initiated termination
	FTA_TAB.1 Default TOE Access Banners
	FTA_TSE.1 TOE Session Establishment
Trusted Path/Channels (FTP)	FTP_ITC.1 Inter-TSF trusted channel
	FTP_TRP.1 Trusted Path

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:

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

44 *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.*

Assurance Activity:

45 *The evaluator shall check the administrative guide 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.*

46 *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.*

47 *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.*

48 *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.*

49 *Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly. For example, testing to ensure the TOE can detect replay attempts will more than likely be done to demonstrate that requirement FPT_RPL.1 is satisfied. Another example is that 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:

50 *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:

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_GEN.2	None.	

Requirement	Auditable Events	Additional Audit Record Contents
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	None.
FAU_STG.1	None.	
FAU_STG_EXT.1	None.	
FAU_STG_EXT.3	Loss of connectivity.	None.
FCS_CKM.1(1)	Failure of the key generation activity.	None.
FCS_CKM.1(2)	Failure of the key generation activity.	None.
FCS_CKM.2(1)	Failure of the key distribution activity.	None.
FCS_CKM.2(2)	Failure of the key distribution activity, including failures related to wrapping the GTK.	Identifier(s) for intended recipients of wrapped key.
FCS_CKM_EXT.4	Failure of the key zeroization process.	Identity of subject requesting or causing zeroization, 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).
FCS_IPSEC_EXT.1	Protocol failures. Establishment/Termination of an IPsec SA. Negotiation “down” from an IKEv2 to IKEv1 exchange.	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_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken (e.g., disabling of an account) and the subsequent, if appropriate, restoration to the normal state (e.g., re-enabling of a terminal).	None.
FIA_PMG_EXT.1	None.	

Requirement	Auditable Events	Additional Audit Record Contents
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU.5	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.6	Attempts to re-authenticate.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	
FIA_8021X_EXT.1	Attempts to access to the 802.1X controlled port.	Provided client identity (IP address).
FIA_PSK_EXT.1	None.	
FIA_X509_EXT.1	Attempts to load certificates. Attempts to revoke certificates.	None.
FMT_MOF.1	None.	
FMT_MTD.1(1)	None.	
FMT_MTD.1(2)	None.	
FMT_MTD.1(3)	None.	
FMT_SMF.1	None.	
FMT_SMR.1	None.	
FPT_FLS.1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.
FPT_RPL.1	Detected replay attacks.	Identity of the user that was the subject of the reply attack. Identity (e.g., source IP address) of the source of the replay attack.
FPT_STM.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.
FRU_RSA.1	Maximum quota being exceeded.	Resource identifier.
FTA_SSL_EXT.1	Locking of an interactive session by the session locking mechanism. Any attempts at unlocking of an interactive session.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	Terminating a session by quitting or logging off.	None.
FTA_TAB.1	None.	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism.	Reason for denial, origin of establishment attempt.

Requirement	Auditable Events	Additional Audit Record Contents
FTP_ITC.1	All attempts to establish a trusted channel. Detection of modification of channel data.	Identification of the initiator and target of channel.
FTP_TRP.1	All attempts to establish a remote administrative session. Detection of modification of session data.	Identification of the initiating IT entity (e.g., IP address).

FAU_GEN.2 **User Audit Association**

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Application Note:

51 *For failed login attempts, where the user ID does not match the ID of a known user, no user association is required because the user is not under TSF control until after a successful identification/authentication.*

Assurance Activity:

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

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

Application Note:

53 *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:

54 *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.

55 *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.*

Security Audit Trail Storage (FAU_STG)

FAU_STG.1	**Protected Audit Trail Storage (Local Storage)**
FAU_STG.1.1	**Refinement:** The TSF shall protect **[assignment: amount of storage] locally** stored audit records in the audit trail from unauthorized deletion.
FAU_STG.1.2	The TSF shall be able to *prevent* unauthorized modifications to the stored audit records in the audit trail.

Application Note:

56 *In addition to the capability to export the audit information, the TOE is required to have some amount of local storage. The ST writer completes the assignment with the amount of local storage available for the audit records; this can be in megabytes, average number of audit records, etc.*

Assurance Activity:
The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. The evaluator shall also examine the operational guidance to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and "cleared" periodically by sending the data to the audit server.

FAU_STG_EXT.1	**External Audit Trail Storage**
FAU_STG_EXT.1.1	The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel implementing the [selection: IPsec, SSH, TLS, TLS/HTTPS] protocol.

Application Note:

57 *The TOE also relies on a non-TOE audit server for storage and review of audit records. Although the TOE generates audit records, the storage of these audit records and the ability to allow the administrator to review these audit records is provided by the operational environment. The ST author chooses the means by which this connection is protected using the selection. The ST author also ensures that the supporting protocol requirement matching the selection is included in the ST.*

Assurance Activity:

58 *The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided. Testing of the trusted channel mechanism will be performed as specified in the associated assurance activities for the particular trusted channel mechanism. The evaluator shall also examine the operational guidance to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server. The evaluator shall perform the following test for this requirement:*

- *Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing.*

FAU_STG_EXT.3	**Action in Case of Loss of Audit Server Connectivity**
FAU_STG_EXT.3.1	The TSF shall [assignment: action] if the link to the external IT entity collecting the audit data generated by the TOE is not available.

Application Note:

59 *The ST author fills in the action the TOE takes (e.g. pages the administrator, stops passing packets) if a link to the audit server is unavailable.*

Assurance Activity:

60 *The evaluator shall examine the administrative guidance to ensure it instructs the administrator how to establish communication with the audit server. The guidance must instruct how this channel is established in a secure manner (e.g., IPsec, TLS). The evaluator checks the administrative guidance to determine what action(s) is taken if the link between the TOE and audit server is broken. This could be due to network connectivity being lost, or the secure protocol link being terminated.*

61 *The evaluator shall examine the operational guidance to determine any activities that must take place after connectivity is restored to ensure that local audit events captured during the period of loss are synchronized with the audit trail on the audit server, and informs the administrator of any limitations on the data that are able to be sent (for instance, if the duration of the outage is significant, the local store may not contain all of the records that where generated during this period).*

62 *The evaluator shall perform the following test for this requirement:*

- *Test 1: The evaluator shall test the administrative guidance by establishing a link to the audit server. Note that this will need to be done in order to perform the assurance activities prescribed under FAU_GEN.1. The evaluator shall disrupt the communication link (e.g., unplug the network cable, terminate the protocol link, shutdown the audit server) to determine that the action(s) described in the administrative guide appropriately take place.*

4.1.2 Class: Cryptographic Support (FCS)

Cryptographic Key Management (FCS_CKM)

FCS_CKM.1(1)	**Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)**
FCS_CKM.1.1(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** that meet the following: **[802.11-2007].**

Application Note:

63 *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 generation of the GTK (through the RBG specified in this PP) as well as 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.*

64 ***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.

FCS_CKM.1(2)	**Cryptographic Key Generation (Asymmetric Keys)**
FCS_CKM.1.1(2)	**Refinement:** The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance with [selection: • *NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;* • *NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key*

Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-3, "Digital Signature Standard")

- *NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes*]

and specified cryptographic key sizes *equivalent to, or greater than, a symmetric key strength of 112 bits*.

Application Note:

65 *This component requires that the TOE be able to generate the public/private key pairs that are used for key establishment purposes for the various cryptographic protocols used by the TOE (e.g., IPsec). If multiple schemes are supported, then the ST author should iterate this requirement to capture this capability. The scheme used will be chosen by the ST author from the selection.*

66 *Since the domain parameters to be used are specified by the requirements of the protocol in this PP, it is not expected that the TOE will generate domain parameters, and therefore there is no additional domain parameter validation needed when the TOE complies to the protocols specified in this PP.*

67 *The generated key strength of 2048-bit DSA and rDSA keys need to be equivalent to, or greater than, a symmetric key strength of 112 bits. See NIST Special Publication 800-57, "Recommendation for Key Management" for information about equivalent key strengths.*

Assurance Activity:

68 *The evaluator shall use the key pair generation portions of "The FIPS 186-3 Digital Signature Algorithm Validation System (DSA2VS)", "The FIPS 186-3 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)", and "The RSA Validation System (RSA2VS)" as a guide in testing the requirement above, depending on the selection performed by the ST author. 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.*

69 *In order to show that the TSF implements complies with 800-56A and/or 800-56B, depending on the selections made, the evaluator shall ensure that the TSS contains the following information:*

- *The TSS shall list all sections of the appropriate 800-56 standard(s) to which the TOE complies.*
- *For each applicable section listed in the TSS, for all statements that are not "shall" (that is, "shall not", "should", and "should not"), if the TOE implements such options it shall be described in the TSS. If the included functionality is indicated as "shall not" or "should 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 applicable section of 800-56A and 800-56B (as selected), any omission of functionality related to "shall" or "should" statements shall be described;*
- *Any TOE-specific extensions, processing that is not included in the documents, or alternative implementations allowed by the documents that may impact the security requirements the TOE is to enforce shall be described.*

FCS_CKM.2(1)	**Cryptographic Key Distribution (PMK)**
FCS_CKM.2.1(1)	**Refinement:** The TSF shall distribute **the 802.11 Pairwise Master Key** in accordance with a specified cryptographic key distribution method: [**receive from 802.1X Authorization Server**] that meets the following: [802.11-2007] **and does not expose the cryptographic keys**.

Application Note:

70 *This requirement applies to the Pairwise Master Key that is received from the RADIUS server by the TOE. The intent of this requirement is to ensure conformant TOEs implement 802.1X authentication prior to establishing secure communications with the client in addition to disallowing implementations that only support pre-shared keys. Because communications with the RADIUS server are required to be performed over an IPsec-protected connection, the transfer of the PMK will be protected.*

Assurance Activity:

71 *The evaluator shall examine the TSS to determine that it describes how the PMK is transferred (that is, through what EAP attribute) to the TSF.*

72 *The evaluator shall perform the following test:*

- *Test 1: The evaluator shall establish a session between the TOE and a RADIUS server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the RADIUS server and the TOE during a successful attempt to connect a wireless client to the TOE to determine that the PMK is not exposed.*

FCS_CKM.2(2)	**Cryptographic Key Distribution (GTK)**
FCS_CKM.2.1(2)	**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:

73 *This requirement applies to the Group Temporal Key (GTK) that is generated by the TOE for use in broadcast and multicast messages to clients 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.*

Assurance Activity:

74 *The evaluator shall check the TSS to ensure that it describes how the GTK is wrapped prior to be distributed using the AES implementation specified in this PP, and also how the GTKs are distributed when multiple clients connect to the TOE. The evaluator shall also perform the following test:*

- *Test 1: The evaluator shall successfully connect multiple clients to the TOE. As the clients are connected, the evaluator shall observe that the GTK is not transmitted in the clear between the client and the TOE.*

- *Test 2: The evaluator shall cause a broadcast message to be sent to all clients connected to the TOE. The evaluator shall ensure the message is encrypted and cannot be read.*
- *Test 3: The evaluator shall create at least two multicast groups among a subset of clients connected to the TOE, each consisting of at least two clients but less than all of the clients connected to the TOE. Some (but not all) of the clients shall be in both groups. The evaluator shall ensure that GTKs established are sent to the participating clients and cannot be determine from the traffic flowing between the clients and the TOE.*
- *Test 4: The evaluator shall cause a multicast message to be sent to the clients in each multicast group connected to the TOE. The evaluator shall ensure each message is encrypted and cannot be read.*

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

Application Note:

75 *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.*

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

Assurance Activity:

77 *The evaluator shall check to ensure the TSS describes each of the secret keys (keys used for symmetric encryption), private keys, and critical security parameters used to generate keys; 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 type of the memory or storage 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").*

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:

78 *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.*

79 *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:

80 *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:

81 *The ST Author should choose the algorithm implemented to perform digital signatures; if more than one algorithm is available, this requirement (and the corresponding FCS_CKM.1 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.*

82 *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:

83 *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:

84 *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:

85 *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:

86 *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.*

87 *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:

88 *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:

89 *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:

90 *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.*

91 *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: Internet Protocol Security (FCS_IPSEC_EXT)

92 The TOE is required to communicate with authentication servers implementing the RADIUS protocol. To provide increased protection of this connection, conformant TOEs will implement an IPsec connection with the authentication server over which the RADIUS protocol will travel. If other IT entities (e.g., audit server) or remote administrators use IPsec for a given TOE, then this requirement will apply as well; there are no RADIUS- or authentication server-unique aspects to the following requirement.

FCS_IPSEC_EXT.1	**Extended: Internet Protocol Security (IPsec) Communications**
FCS_IPSEC_EXT.1.1	The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602), [selection: no other algorithms, AES-GCM-128, AES-GCM-256 as specified in RFC 4106], and using [selection, choose at least one of: IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]; IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23), 4307, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]] for connections to the Authentication Server and [selection: no other servers, [assignment: list of servers to which the TOE connects]].
FCS_IPSEC_EXT.1.2	The TSF shall ensure that only ESP confidentiality and integrity security service is used.
FCS_IPSEC_EXT.1.3	The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.
FCS_IPSEC_EXT.1.4	The TSF shall ensure that [selection: IKEv1 SA lifetimes are able to be limited by number of packets and time: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs; IKEv2 SA lifetimes can be configured by an administrator based on number of packets or length of time].
FCS_IPSEC_EXT.1.5	The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [assignment: (one or more) number(s) of bits that is at least twice the "bits of security" value associated with the negotiated Diffie-Hellman group as listed in Table 2 of NIST SP 800-57, *Recommendation for Key Management – Part 1: General*] bits.
FCS_IPSEC_EXT.1.6	The TSF shall generate nonces used in IKE exchanges in a manner such that the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^[assignment: (one or more) "bits of security" value(s) associated with the negotiated Diffie-Hellman group as listed in Table 2 of NIST SP 800-57, *Recommendation for Key Management – Part 1: General*] .
FCS_IPSEC_EXT.1.7	The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP) and [selection: *24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP),* [assignment: other DH groups that

are implemented by the TOE], *no other DH groups*].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that all IKE protocols implement peer authentication using Pre-shared Keys and [selection, choose at least one of: *DSA, rDSA, ECDSA*] that use X.509v3 certificates that conform to RFC 4945.

FCS_IPSEC_EXT.1.9 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [selection: *IKEv1 Phase 1, IKEv2 IKE_SA*] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [selection: *IKEv1 Phase 2, IKEv2 CHILD_SA*] connection.

Application Note:

93 FCS_IPSEC_EXT.1 *is supported at least for protection of the RADIUS communications between the WLAN Access System and an Authentication Server. The first selection is used to identify additional cryptographic algorithms supported. Either IKEv1 or IKEv2 support must be provided, although conformant TOES can provide both; the second selection is used to make this choice. For IKEv1, the requirement is to be interpreted as requiring the IKE implementation conforming to RFC 2409 with the additions/modifications as described in RFC 4109. RFC 4868 identifies additional hash functions for use with both IKEv1 and IKEv2; if these functions are implemented, the third (for IKEv1) and fourth (for IKEv2) selection can be used. The last selection/assignment is used to specify other servers/services (e.g., an audit server) the TOE communicates with whose communications are protected by IPsec.*

94 FCS_IPSEC_EXT.1.4: *The ST author chooses either the IKEv1 requirements or IKEv2 requirements (or both, depending on the selection in the first requirement. The IKEv1 requirement can be accomplished either by providing Authorized Administrator-configurable lifetimes (with appropriate instructions in documents mandated by AGD_OPE), or by "hard coding" the limits in the implementation. For IKEv2, there are no hardcoded limits, but in this case it is required than an administrator be able to configure the values. In general, instructions for setting the parameters of the implementation, including lifetime of the SAs, should be included in the administrative guidance generated for AGD_OPE. It is appropriate to refine the requirement in terms of number of MB/KB instead of number of packets, as long as the TOE is capable of setting a limit on the amount of traffic that is protected by the same key (the total volume of all IPsec traffic protected by that key).*

95 Since the implementation may allow different Diffie-Hellman groups to be negotiated for use in forming the SAs, the assignments in FCS_IPSEC_EXT.1.5 and FCS_IPSEC_EXT.1.6 may contain multiple values. For each DH group supported, the ST author consults Table 2 in 800-57 to determine the "bits of security" associated with the DH group. Each unique value is then used to fill in the assignment (for 1.5 they are doubled; for 1.6 they are inserted directly into the assignment). For example, suppose the implementation support DH group 14 (2048-bit MODP) and group 20 (ECDH using NIST curve P-384). From Table 2, the bits of security value for group 14 is 112, and for group 20 it is 192. For FCS_IPSEC_EXT.1.5, then, the assignment would read "[224, 384]" and for FCS_IPSEC_EXT.1.6 it would read "[112,192]" (although in this case the requirement should probably be refined so that it makes sense mathematically).

96 FCS_IPSEC_EXT.1.7: *The selection is used to specify additional DH groups supported. This applies to IKEv1 and IKEv2 exchanges. In future versions of this PP, DH Groups 19 (256-bit Random ECP) and 20 (384-bit RandomECP) will be required. It should be noted that if any additional DH groups are specified, they*

must comply with the requirements (in terms of the ephemeral keys that are established) listed in FCS_CKM.1(2).

97 FCS_IPSEC_EXT.1.8: *Pre-shared keys and at least one public-key-based Peer Authentication method are required for conformant TOEs; one or more of the public key schemes is chosen by the ST Author to reflect what is implemented by the TOE. The ST author also ensures that appropriate FCS requirements reflecting the algorithms used (and key generation capabilities, if provided) are listed to support those methods. Note that the TSS will elaborate on the way in which these algorithms are to be used (for example, 2409 specifies three authentication methods using public keys; each one supported will be described in the TSS).*

98 FCS_IPSEC_EXT.1.9: *The ST author chooses either or both of the IKE selections based on what is implemented by the TOE. Obviously, the IKE version(s) chosen should be consistent not only in this element, but with other choices for other elements in this component. While it is acceptable for a TOE to allow this capability to be configurable, the default configuration in the evaluated configuration (either "out of the box" or by configuration guidance in the OPE documentation) must enable this functionality.*

Assurance Activity:

99 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_IPSEC_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 "MUST" or "SHOULD" statements shall be described;*
- *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.*

100 The evaluator shall ensure the TSS identifies all servers/services that require or allow IPsec connections. The evaluators shall also ensure that when performing testing and analysis activities, the activities apply to all servers identified. The evaluators shall ensure that at least one instance of every type of server is used in at least one test during the testing activities to provide assurance that the identified communications can take place. The evaluators shall also ensure that the configuration information (including product and version numbers) for the non-TOE endpoints of these connections is recorded in the test report.

101 The evaluator shall also perform the following test for TOEs that implement IKEv2:

- *Test 1 [conditional]: The evaluator shall configure the TOE so that it will perform NAT traversal processing as described in the TSS and RFC 4306, section 2.23. The evaluator shall initiate an IPsec connection and determine that the NAT is successfully traversed.*

102 FCS_IPSEC_EXT.1.2 - The evaluator shall examine the TSS to verify that it describes how the "confidentiality only" ESP security service is disabled. The evaluator shall also examine the operational guidance to determine that it describes any configuration necessary to ensure negotiation of

"confidentiality only" security service for ESP is disabled, and that an advisory is present indicating that tunnel mode is the preferred ESP mode since it protects the entire packet.

- *Test 1: The evaluator shall configure the TOE as indicated in the operational guidance, and attempt to establish a connection using ESP using the "confidentiality only" security service. This attempt should fail. The evaluator shall then establish a connection using ESP using the confidentiality and integrity security service.*

103 *FCS_IPSEC_EXT.1.3 - The evaluator shall examine the TSS to ensure that, in the description of the IPsec protocol supported by the TOE, it states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used. If this requires configuration of the TOE prior to its operation, the evaluator shall check the operational guidance to ensure that instructions for this configuration are contained within that guidance. The evaluator shall also perform the following tests:*

- *Test 1: The evaluator shall configure the TOE as indicated in the operational guidance, and attempt to establish a connection using an IKEv1 Phase 1 connection in aggressive mode. This attempt should fail. The evaluator should then show that main mode exchanges are supported.*

104 *FCS_IPSEC_EXT.1.4 – If IKEv1 requirements are selected, the evaluator checks to ensure that the TSS describes how lifetimes for IKEv1 SAs (both Phase 1 and Phase 2) are established. If they are configurable, then the evaluator verifies that the appropriate instructions for configuring these values are included in the operational guidance. For IKEv2 requirements, the evaluator verifies that the values can be configured and that the instructions for doing so are located in the operational guidance. The evaluator also performs the following tests, depending on whether IKEv1, IKEv2, or both are configured:*

- *Test 1 (IKEv1): The evaluator shall construct a test where a Phase 1 SA is established and attempted to be maintained for more than 24 hours before it is renegotiated. The evaluator shall observe that this SA is closed or renegotiated in 24 hours or less. If such an action requires that the TOE be configured in a specific way, the evaluator shall implement tests demonstrating that the configuration capability of the TOE works as documented in the operational guidance.*

- *Test 2 (IKEv1): The evaluator shall perform a test similar to Test 1 for Phase 2 SAs, except that the lifetime will be 8 hours instead of 24.*

- *Test 3 (IKEv1 and v2): The evaluator shall configure a maximum lifetime in terms of the # of packets allowed; this may be a hard-coded value for IKEv1, otherwise, the evaluator follows the operational guidance. The evaluator shall establish an SA and determine that once the allowed # of packets through this SA is exceeded, the connection is closed.*

- *Test 4 (IKEv2): The evaluator shall configure a time-based maximum lifetime for an SA, and then establish the SA. The evaluator shall observe that this SA is closed or renegotiated in the established time.*

105 *FCS_IPSEC_EXT.1.5, FCS_IPSEC_EXT.1.6 - The evaluator shall check to ensure that, for each DH group supported by the TSF, the TSS describes the process for generating "x" (as defined in FCS_IPSEC_EXT.1.5) and each nonce. The evaluator shall verify that the TSS indicates that the random number generated*

that meets the requirements in this PP is used, and that the length of "x" and the nonces meet the stipulations in the requirement.

106 *FCS_IPSEC_EXT.1.7 - The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being supported in the TSS. If there is more than one DH group supported, the evaluator checks to ensure the TSS describes how a particular DH group is specified/negotiated with a peer. The evaluator shall also perform the following test:*

- *Test 1: For each supported DH group, the evaluator shall test to ensure that all IKE protocols can be successfully completed using that particular DH group.*

107 *FCS_IPSEC_EXT.1.8 – The evaluator shall check to ensure that the TSS describes how pre-shared keys are established and used in authentication of IPsec connections. The evaluator shall check that the operational guidance describes how pre-shared keys are to be generated and established for a TOE. The description in the TSS and the operational guidance shall also indicate how pre-shared key establishment is accomplished for both TOEs that can generate a pre-shared key as well as TOEs that simply use a pre-shared key. The evaluator shall also perform the following test:*

- *Test 1: The evaluator shall generate a pre-shared key and use it, as indicated in the operational guidance, to establish an IPsec connection between two peers. If the TOE supports generation of the pre-shared key, the evaluator shall ensure that establishment of the key is carried out for an instance of the TOE generating the key as well as an instance of the TOE merely taking in and using the key.*

108 *The evaluator shall check that the TSS contains a description of the IKE peer authentication process used by the TOE, and that this description covers the use of the algorithm or algorithms specified in the selection. As part of the assurance activity for FCS_IPSEC_EXT.1.1, required and optional elements of RFC 4945 shall be documented. The evaluator shall also perform the following tests:*

- *Test 1: For each supported algorithm, the evaluator shall test that peer authentication using that algorithm can be successfully achieved.*

- *Test 2: For each supported identification payload (from RFC 4945), the evaluator shall test that peer authentication can be successfully achieved.*

- *Test 3: The evaluator shall devise a test that demonstrates that a corrupt or invalid certification path for a certificate will be detected during IKE peer authentication and will result in a connection not being established.*

- *Test 4: The evaluator shall devise a test that demonstrates that a certificate that has been revoked through a CRL will be detected during IKE peer authentication and will result in a connection not being established.*

109 *FCS_IPSEC_EXT.1.10 – The evaluator shall check that the TSS describes the potential strengths (in terms of the number of bits in the symmetric key) of the algorithms that are allowed for the IKE and ESP exchanges. The TSS shall also describe the checks that are done when negotiating IKEv1 Phase 2 and/or IKEv2 CHILD_SA suites to ensure that the strength (in terms of the number of bits of key in the symmetric algorithm) of the negotiated algorithm is less than or equal to that of the IKE SA this is protecting the negotiation. The evaluator shall also perform the following tests:*

- *Test 1: This test shall be performed for each version of IKE supported by the TOE. The evaluator shall successfully negotiate an IPsec connection using each of the supported algorithms and hash functions identified in the requirements.*

- *Test 2: This test shall be performed for each version of IKE supported by the TOE. The evaluator shall attempt to establish an SA for ESP that selects an encryption algorithm with more strength than that being used for the IKE SA (i.e., symmetric algorithm with a key size larger than that being used for the IKE SA). Such attempts should fail.*

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 at least one independent TSF-hardware-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:

110 *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.*

111 *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).*

112 *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.*

113 *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.*

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

115 *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:

116 *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 hardware-based noise source from which entropy is gathered, and further confirm that this noise source is located on the USB Flash Drive. The evaluator will further verify that all of the underlying functions and parameters used in the RBG are listed in the TSS.*

117 *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.*

118 *Regardless of the standard to which the RBG is claiming conformance, the evaluator perform 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.*

119 *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

120 *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.*

121 *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.*

122 *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

123 *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.*

124 *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).*

125 *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.*

126 *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 Resident 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:

127 *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:

128 *"Resources" in the context of this requirement are network packets being sent through (as opposed to "to", as is the case when an 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)

129 The TOE must support many different types of identification and authentication schemes for different human users and IT entities in the course of operation. 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 several services (e.g., IPsec, 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.

130 It should be noted that SNMP (including SNMPv3) is currently unable to meet the requirements of this PP, and therefore is not an acceptable option as the sole means to administer the TOE. However, if SNMP is tunneled inside one of the protocols listed in FTP_TRP.1.1 for remote administration, then it can be used to manage the TOE, as long as the required (by the FMT requirements) functionality is available through that interface.

131 The requirements in this section cover several distinct aspects of the I&A capabilities of conformant TOEs:

- **I&A for the human administrator.** The administrator is the only human user that is identified and authenticated by the TOE. While the wireless clients represent humans connecting to the network through that client, these human users are not identified nor authenticated by the TOE.
- **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 an "authenticator" per 802.1X.
- **Credentials.** The protocols and mechanisms specified in this and other sections of the PP rely on several different credentials that are used in the I&A process: passwords (for administrators), pre-shared keys (for IPsec and potentially other (TLS, SSH) connections to IT entities), and certificates (IPsec connections and potentially for administrators (IPsec, TLS, SSH)).

132 The following requirements are, to the extent possible, grouped according to these categories (rather than alphabetically) for clarity of presentation.

Authentication Failure Handling (FIA_AFL)

FIA_AFL.1	Authentication Failure Handling
FIA_AFL.1.1	**Refinement:** The TSF shall detect when **an Authorized Administrator configurable positive integer of successive** unsuccessful authentication attempts occur related to **administrators attempting to authenticate remotely**.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **[selection, choose one of: prevent the offending remote administrator from successfully authenticating until [assignment: action] is taken by a local Authorized Administrator; prevent the offending remote administrator from successfully authenticating until an Authorized Administrator defined time period has elapsed**].

Application Note:

133 *This requirement does not apply to an administrator at the local console, since it does not make sense to lock a local administrator's account in this fashion. This could be addressed by (for example) requiring a separate account for local administrators or having the authentication mechanism implementation distinguish local and remote login attempts. The "action" taken by a local administrator is implementation specific and would be defined in the administrator guidance (for example, lockout reset or password reset). The ST author chooses one of the selections for handling of authentication failures depending on how the TOE has implemented this handler.*

Assurance Activity:

134 *The evaluator shall examine the TSS to determine that it contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked. The TSS shall also describe the method by which the remote administrator is prevented from successfully logging on to the TOE, and the actions necessary to restore this ability. The evaluator shall also examine the operational guidance to ensure that instructions for configuring the number of successive unsuccessful authentication attempts (1.1) and time period (1.2, if implemented) are provided, and that the process of allowing the remote administrator to once again successfully log on is described for each "action" specified (if that option is chosen). If different actions or mechanisms are implemented depending on the authentication method (e.g., TSL vs. SSH), all must be described.*

135 *The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g., TLS, SSH):*

- *Test 1 [conditional on first selection item]: The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE. The evaluator shall test that once the limit is reached, attempts with valid credentials are not successful. For each action specified by the requirement, the evaluator shall show that following the operational guidance and performing each action to allow the remote administrator access are successful.*
- *Test 2 [conditional on second selection item]: The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts*

allowed by the TOE and a time period after which valid logins will be allowed for a remote administrator. After exceeding the specified number of invalid login attempts and showing that valid login is not possible, the evaluator shall show that waiting for the interval defined by the time period before another access attempt will result in the ability for the remote administrator to successfully log on using valid credentials.

Password Management (FIA_PMG)

FIA_PMG_EXT.1 Password Management

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

1. *Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")");*
2. *Minimum password length shall be settable by the Authorized Administrator, and support passwords of 8 characters or greater;*
3. *Passwords composition rules specifying the types and number of required characters that comprise the password shall be settable by the Administrator.*
4. *Passwords shall have a maximum lifetime, configurable by the Authorized Administrator.*
5. *New passwords must contain a minimum of 4 character changes from the previous password.*

Application Note:

136 *Note that it is not necessary to store a plaintext version of the password in order to determine that at least 4 characters have changed, since FIA_UAU.6 requires re-authentication when changing the password.*

137 *"Administrative passwords" refers to passwords used by administrators at the local console or over protocols that support passwords, such as SSH and HTTPS.*

138 *The intent of Item 3 above is that an Authorized Administrator is able to specify, for example, that passwords contain at least 1 upper case letter, 1 lower case letter, 1 numeric character, and 1 special character, and the TOE enforces this restriction. "Types" refers to all of the types listed in Item 1 in this element.*

Assurance Activity:

139 *The evaluator shall examine the operational guidance to determine that it provides guidance to administrators on the composition of strong passwords, and that it provides instructions on setting the minimum password length; the formulation and specification of password composition rules and how to*

configure these for the TOE; and how to configure the maximum lifetime for a password. The evaluator shall also perform the following tests. Note that one or more of these tests can be performed with a single test case.

- *Test 1: The evaluator shall configure the TOE with different password composition rules, as specified in the requirement. The evaluator shall then, for each set of rules, compose passwords that both meet the requirements, and fail to meet the requirements, in some way. For each password, the evaluator shall verify that the composition rules are enforced. While the evaluator is not required (nor is it feasible) to test all possible composition rules, the evaluator shall ensure that all characters, rule characteristics, and a minimum length listed in the requirement are supported, and justify the subset of those characters chosen for testing.*

- *Test 2: The evaluator shall ensure that the operational guidance contains instructions on setting the maximum password lifetime. The evaluator shall then configure this lifetime to several values, and ensure that it is enforced for each of those values.*

- *Test 3: The evaluator shall test that a minimum of 4 character changes from previous passwords is enforced. This shall be done for more than one password.*

FIA_UIA_EXT.1	**User Identification and Authentication**
FIA_UIA_EXT.1.1	The TSF shall allow responses to the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process: • Display the warning banner in accordance with FTA_TAB.1; • [assignment: list of services, actions performed by the TSF in response to non-TOE requests.]
FIA_UIA_EXT.1.2	The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

Application Note:

140 *This requirement applies to users (administrators and external IT entities) of services available from the TOE directly, and not services available by connecting through the TOE. While it should be the case that few or no services are available to external entities prior to identification and authentication, if there are some available (perhaps ICMP echo) these should be listed in the assignment statement; otherwise "no services" is an acceptable assignment.*

141 *Authentication can be password-based through the local console or through a protocol that supports passwords (such as SSH), or be certificate based (SSH, TLS).*

142 *For communications with external IT entities (e.g., an audit server or NTP server, for instance), such connections must be performed in accordance with FTP_ITC.1, whose protocols perform identification and authentication. This means that such communications (e.g., establishing the IPsec connection to the authentication server) would not have to be specified in the assignment, since establishing the connection "counts" as initiating the identification and authentication process.*

Assurance Activity:

143 *The evaluator shall examine the TSS to determine that it describes the logon process for each logon method (local, remote (HTTPS, SSH, etc.)) supported for the product. This description shall contain information pertaining to the credentials allowed/used, any protocol transactions that take place, and what constitutes a "successful logon". The evaluator shall examine the operational guidance to determine that any necessary preparatory steps (e.g., establishing credential material such as pre-shared keys, tunnels, certificates, etc.) to logging in are described. For each supported the login method, the evaluator shall ensure the operational guidance provides clear instructions for successfully logging on. If configuration is necessary to ensure the services provided before login are limited, the evaluator shall determine that the operational guidance provides sufficient instruction on limiting the allowed services.*

144 *The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method:*

- *Test 1: The evaluator shall use the operational guidance to configure the appropriate credential supported for the login method. For that credential/login method, the evaluator shall show that providing correct I&A information results in the ability to access the system, while providing incorrect information results in denial of access.*
- *Test 2: The evaluator shall configure the services allowed (if any) according to the operational guidance, and then determine the services available to an external remote entity. The evaluator shall determine that the list of services available is limited to those specified in the requirement.*
- *Test 3: For local access, the evaluator shall determine what services are available to a local administrator prior to logging in, and make sure this list is consistent with the requirement.*

FIA_UAU_EXT.5	**Password-based Authentication Mechanism**
FIA_UAU_EXT.5.1	The TSF shall provide a local password-based authentication mechanism, [selection: [assignment: *other authentication mechanism(s)*], none] to perform administrative user authentication.
FIA_UAU_EXT.5.2	The TSF shall ensure that administrative users with expired passwords are [selection: required to create a new password after correctly entering the expired password, locked out until their password is reset by an administrator].

Application Note:

145 *This requirement only applies to the local administrator login, and essentially requires that a password-based mechanism exists on the TOE for this purpose. The ST author can fill in the assignment with any other supported authentication mechanisms (such as an authentication server) for administrative users that are not local. If no external authentication mechanisms for administrative users are supported, the ST author should choose "none" in the selection.*

Assurance Activity:

146 *Assurance activities for this requirement are covered under those for FIA_UIA_EXT.1. If other authentication mechanisms are specified, the evaluator shall include those methods in the activities for FIA_UIA_EXT.1*

FIA_UAU.6 **Re-authenticating**

FIA_UAU.6.1 The TSF shall re-authenticate the administrative user under the conditions: *when the user changes their password*, [*selection: following TSF-initiated locking (FTA_SSL), [assignment: other conditions], no other conditions*].

Assurance Activity:

147 *The evaluator shall perform the following test for each of the conditions specified in the requirement:*

- *Test 1: The evaluator shall attempt to change their password as directed by the operational guidance. While making this attempt, the evaluator shall verify that re-authentication is required.*

FIA_UAU.7 **Protected Authentication Feedback**

FIA_UAU.7.1 The TSF shall provide only *obscured feedback* to the administrative user while the authentication is in progress at the local console.

Application Note:

148 *"Obscured feedback" implies the TSF does not produce a visible display of any authentication data entered by a user (such as the echoing of a password), although an obscured indication of progress may be provided (such as an asterisk for each character). It also implies that the TSF does not return any information during the authentication process to the user that may provide any indication of the authentication data.*

Assurance Activity:

149 *The evaluator shall perform the following test for each method of local login allowed:*

- *Test 1: The evaluator shall locally authenticate to the TOE. While making this attempt, the evaluator shall verify that at most obscured feedback is provided while entering the authentication information.*

802.1X Port Access Control Authentication (FIA_8021X_EXT)

FIA_8021X_EXT.1 **802.1X Port Access Entity (Authenticator) Authentication**

FIA_8021X_EXT.1.1 The TSF shall conform to IEEE Standard 802.1X for a Port Access Entity (PAE) in the "Authenticator" role.

FIA_8021X_EXT.1.2 The TSF shall support communications to a RADIUS authentication server conforming to RFCs 2865 and 3579.

FIA_8021X_EXT.1.3 The TSF shall ensure that no access to its 802.1X controlled port is given to the wireless client prior to successful completion of this authentication exchange.

Application Note:

150 *This requirement covers the TOE's role as the authenticator in an 802.1X authentication exchange. If the exchange is completed successfully, the TOE will obtain the PMK from the RADIUS server and perform the 4-way handshake with the wireless client (supplicant) to begin 802.11 communications.*

151 *As indicated previously, there are at least three communication paths present during the exchange; two with the TOE as an endpoint and one with TOE acting as a transfer point only. The TOE establishes an EAP over LAN (EAPOL) connection with the wireless client as specified in 802.1X-2007. The TOE also establishes (or has established) a RADIUS protocol connection (which is tunnelled inside of an IPsec connection) with the RADIUS server. The wireless client and RADIUS server establish an EAP-TLS session (RFC 5216); in this transaction the TOE merely takes the EAP-TLS packets from its EAPOL/RADIUS endpoint and transfers them to the other endpoint. Because the specific authentication method (TLS in this case) is opaque to the TOE, there are no requirements with respect to RFC 5126 in this PP. However, the base RADIUS protocol (2865) has an update (3579) that will need to be addressed in the implementation and assurance activities. Additionally, RFC 5080 contains implementation issues that will need to be addressed by developers, but which levy no new requirements.*

152 *The point of performing 802.1X authentication is to provide 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 wireless client has access to the "controlled port" maintained by the TOE.*

Assurance Activity:

153 *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.*

154 *Because the connection to the RADIUS server will be contained in an IPsec tunnel (FCS_IPSEC_EXT.1), the security mechanisms detailed in the RFCs identified in the requirement are not relied on to provide protection for these communications. Consequently, no extensive analysis of the RFCs is required. However, the evaluator shall ensure that the TSS describes the measures (documentation, testing) that are taken by the product developer to ensure that the TOE conforms to the RFCs listed in this requirement.*

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

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

- *Test 2: The evaluator shall demonstrate that a wireless client 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 wireless client still being unable to access the test network.*

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

156 *It should be noted that tests 2 and 3 above are not tests that "EAP-TLS works", although that's a by-product of the test. The test is actually that a failed authentication (under two failure modes) results in denial of access to the network, which is the 3rd element of this component.*

Pre-Shared Key Composition (FIA_PSK_EXT)

157 The TOE must minimally support pre-shared keys for use in the IPsec protocol, and may use pre-shared keys in other protocols (excepting WPA2) as well. There are two types of pre-shared keys that must be supported by the TOE, as specified in the requirements below. The first type is referred to as “text-based pre-shared keys”, which refer to pre-shared keys that are entered by users as a string of characters from a standard character set, similar to a password. Such pre-shared keys must be conditioned so that the string of characters is transformed into a string of bits, which is then used as the key.

158 The second type is referred to as “bit-based pre-shared keys” (for lack of a standard term); this refers to keys that are either generated by the TSF on a command from the administrator, or input in "direct form" by an administrator. "Direct form" means that the input is used directly as the key, with no "conditioning" as was the case for text-based pre-shared keys. An example would be a string of hex digits that represent the bits that comprise the key.

159 The requirements below mandate that the TOE must support both text-based and bit-based pre-shared keys, although generation of the bit-based pre-shared keys may be done either by the TOE or in the operational environment.

FIA_PSK_EXT.1	**Extended: Pre-Shared Key Composition**
FIA_PSK_EXT.1.1	The TSF shall be able to use pre-shared keys for IPsec and [**selection: *no other protocols,* [assignment: other protocols that use pre-shared keys]].**
FIA_PSK_EXT.1.2	The TSF shall be able to accept text-based pre-shared keys that: • **are 22 characters and *[selection: [assignment: other supported lengths], no other lengths]*;** • **composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).**

FIA_PSK_EXT.1.3	The TSF shall condition the text-based pre-shared keys by using [selection: SHA-1, SHA-256, SHA-512, [assignment: *method of conditioning text string*]].
FIA_PSK_EXT.1.4	The TSF shall be able to [selection: accept, generate using the random bit generator specified in FCS_RBG_EXT.1] bit-based pre-shared keys.

Application Note:

160 *In the first selection, if other protocols can use pre-shared keys, they should be listed in the assignment as well; otherwise "no other protocols" should be chosen. The intent of this requirement is that all protocols will support both text-based and bit-based pre-shared keys.*

161 *For the length of the text-based pre-shared keys, a common length (22 characters) is required to help promote interoperability. If other lengths are supported they should be listed in the assignment; this assignment can also specify a range of values (e.g., "lengths from 5 to 55 characters") as well.*

162 *In the selection for FIA_PSK_EXT.1.3, the ST author selects or fills in the method by which the text string entered by the administrator is "conditioned" into the bit string used as the key. This can be done by using one of the specified hash functions, or some other method through the assignment statement.*

163 *For FIA_PSK_EXT.1.4, the ST author specifies whether the TSF merely accepts bit-based pre-shared keys, or is capable of generating them. If it generates them, the requirement specified that they must be generated using the RBG provided by the TOE.*

Assurance Activity:

164 *The evaluator shall examine the operational guidance to determine that it provides guidance to administrators on the composition of strong text-based pre-shared keys, and (if the selection indicates keys of various lengths can be entered) that it provides information on the merits of shorter or longer pre-shared keys. The guidance must specify the allowable characters for pre-shared keys, and that list must be a super-set of the list contained in FIA_PSK_EXT.1.2.*

165 *The evaluator shall examine the TSS to ensure that it identifies all protocols that allow both text-based and bit-based pre-shared keys, and states that text-based pre-shared keys of 22 characters are supported. For each protocol identified by the requirement, the evaluator shall confirm that the TSS states the conditioning that takes place to transform the text-based pre-shared key from the key sequence entered by the user (e.g., ASCII representation) to the bit string used by the protocol, and that this conditioning is consistent with the last selection in the FIA_PSK_EXT.1.3 requirement.*

166 *The evaluator shall confirm the operational guidance contains instructions for either entering bit-based pre-shared keys for each protocol identified in the requirement, or generating a bit-based pre-shared key (or both). The evaluator shall also examine the TSS to ensure it describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this functionality), and confirm that this process uses the RBG specified in FCS_RBG_EXT.1.*

167 *The evaluator shall also perform the following tests for each protocol (or instantiation of a protocol, if performed by a different implementation on the TOE). Note that one or more of these tests can be performed with a single test case.*

- *Test 1: The evaluator shall compose a pre-shared key of 22 characters that contains a combination of the allowed characters in accordance with the operational guidance, and demonstrates that a successful protocol negotiation can be performed with the key.*

- *Test 2 [conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall repeat Test 1 using the minimum length; the maximum length; and an invalid length. The minimum and maximum length tests should be successful, and the invalid length must be rejected by the TOE.*

- *Test 3 [conditional]: If the TOE does not generate bit-based pre-shared keys, the evaluator shall obtain a bit-based pre-shared key of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.*

- *Test 4 [conditional]: If the TOE does generate bit-based pre-shared keys, the evaluator shall generate a bit-based pre-shared key of the appropriate length and use it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.*

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 IPsec and [selection: no other protocols, TLS, SSH] connections.
FIA_X509_EXT.1.2	The TSF shall store and protect certificate(s) from unauthorized deletion and modification.
FIA_X509_EXT.1.3	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:

168 *For FIA_X509_EXT.1.1, the ST author should select the protocols that are used to implement administrative connectivity that also use certificates for authentication. 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.*

169 *Depending on the protocols selected, there may be additional protocol-specific certificate-related requirements (and associated assurance activities) specified (for instance, RFC 4945 for IPsec). These additional requirements are specified in the requirements associated with that protocol.*

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 *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 "MUST" or "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.*

172 *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.*

173 *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.*

174 *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.*

175 *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.*

4.1.5 Class: Security Management (FMT)

176 The primary intent in this section is to call out critical activities that must be performed by an administrator to prevent a negligent user from putting the WLAN Access System in an insecure state. The administration model for conformant TOEs is described in Section 1.1.3 of this PP. If additional capabilities are provided by the TOE, the appropriate management and I&A requirements from Appendix C should be included in the ST.

FMT_MOF.1	**Management of Security Functions Behavior**
FMT_MOF.1.1	**Refinement:** The TSF shall restrict the ability to **enable, disable, determine and modify the behavior of all of the security functions of the TOE identified in this PP** to **the Authorized Administrator**.

Application Note:

177 *The only human users of the TOE are administrative users; therefore, this requirement is present to underscore the fact that non-administrative users will not be able to manipulate the mechanisms of the TOE used to implement the security requirements of the PP. These capabilities explicitly cover functions*

implemented in the TOE dealing with adding TOE components to the network and structuring them from a management or redundancy standpoint.

Assurance Activity:

178 *The evaluator shall review the operational guidance to determine that each of the functions implemented in response to the requirements of this PP is identified, and that configuration information is provided to ensure that only administrators have access to the functions. The evaluator shall include in this list of functions to be examined those mechanisms dealing with adding additional instances of a TOE to a configuration, and configuration of the multiple TOE instances into a management hierarchy and/or redundant architecture. The evaluator shall examine the TSS to determine that, for each administrative function identified in the operational guidance, those that are accessible through an interface prior to administrator log-in are identified. For each of these functions, the evaluator shall also confirm that the TSS details how the ability to manipulate the configuration of the system through this interface is disallowed for non-administrative users.*

Management of TSF Data (FMT_MTD)

FMT_MTD.1(1)	**Management of TSF Data (General TSF Data)**
FMT_MTD.1.1(1)	The TSF shall restrict the ability to *manage* the *TSF data* to the *Authorized Administrators*.

Application Note:

179 *The word "manage" includes but is not limited to create, initialize, view, change default, modify, delete, clear, and append. This requirement is intended to be the "default" requirement for management of TSF data; other iterations of FMT_MTD should place different restrictions or operations available on the specifically-identified TSF data. TSF data includes cryptographic information as well; managing these data would include the association of a cryptographic protocol with an interface, for instance.*

Assurance Activity:

180 *Since administrative functions manipulate the TSF data, the analysis performed by the evaluators in the Assurance Activity for FMT_MOF.1 will demonstrate that this requirement is met.*

FMT_MTD.1(2)	**Management of TSF Data (Reading of Authentication Data)**
FMT_MTD.1.1(2)	**Refinement:** The TSF shall **prevent reading of** the **password-based authentication data.**

Application Note:

181 *The intent of the requirement is that no user or administrator be able to read the raw authentication data (such as an unencrypted password) through "normal" interfaces if the reading of such data could lead to someone impersonating that user. An all-powerful administrator of course could directly read memory or do a raw read of the file system to capture a password but is trusted not to do so.*

Assurance Activity:

182 *The evaluator shall examine the TSS to determine that it details all authentication data that are subject to this requirement, and how they are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If passwords or other authentication data are not stored in plaintext, the TSS shall describe how the passwords are protected and how they are able to be used (e.g., administrator-entered passphrase).*

FMT_MTD.1(3)	**Management of TSF Data (for reading of all symmetric keys)**
FMT_MTD.1.1(3)	**Refinement:** The TSF shall **prevent** *reading of all pre-shared keys, symmetric key, and private keys.*

Application Note:

183 *The intent of the requirement is that no user or administrator be able to read or view the identified keys (stored or ephemeral) through "normal" interfaces. While an authorized administrator of course could directly read memory to view these keys, they are trusted not to do so.*

Assurance Activity:

184 *The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.*

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 security management functions: • *Ability to configure the list of TOE services available before an entity is identified and authenticated, as specified in FIA_UIA.1, respectively.* • *Ability to configure the cryptographic functionality.* • *Ability to update the TOE, and to verify the updates using the digital signature capability (FCS_COP.1(2)) and [selection: no other functions, [assignment: other cryptographic functions (or other functions) used to support the update capability]].* • *Ability to configure the TOE advisory notice and consent warning message regarding unauthorized use of the TOE.* • ***Ability to configure all security management functions identified in other sections of this PP**.*

Application Note:

185 *The security management functions for FMT_SMF.1 are distributed throughout the PP and are included as part of the requirements in FMT_MOF, FMT_MSA, FMT_MTD, FMT_REV, FPT_TST_EXT, and any cryptographic management functions specified in the reference standards.*

Assurance Activity:

186 *This requirement merely ensures that the mechanisms called for in other requirements are actually instantiated in the TOE; therefore, verification that these mechanisms exist and work in a manner consistent with the other requirements is provided through the Assurance Activities associated with those other requirements.*

Security Management Roles (FMT_SMR)

FMT_SMR.1	**Security Management Roles**
FMT_SMR.1.1	The TSF shall maintain the roles: • **Authorized Administrator;** • ***[No other roles]***
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
FMT_SMR.1.3	The TSF shall ensure that the conditions • **Authorized Administrator role shall be able to administer the TOE locally;** • **Authorized Administrator role shall be able to administer the TOE remotely;** • **The ability to remotely administer the TOE remotely from a wireless client shall be disabled by default;** are satisfied.

Application Note:

187 *FMT_SMR.1.2 requires that user accounts be associated with only one role. However, note that multiple users may have the same role, and the TOE is not required to restrict roles to a single person.*

188 *FMT_SMR.1.3 requires that an authorized administrator be able to administer the TOE through the local console and through a remote mechanism (IPsec, SSH, TLS/HTTPS). For multiple component TOEs, only the TOE components providing the management control and configuration of the other TOE components require a local administration interface.*

Assurance Activity:

189 *The evaluator shall review the operational guidance to ensure that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration. In the course of performing the testing activities for the evaluation, the evaluator shall use all supported interfaces, although it is not necessary to repeat each test involving an administrative action with each interface. The evaluator shall ensure, however, that each supported method of administering the TOE that conforms to the requirements of this PP be tested;*

for instance, if the TOE can be administered through a local hardware interface; SSH; and TLS/HTTPS; then all three methods of administration must be exercised during the evaluation team's test activities.

190 *The evaluator shall also perform the following test:*

- *Test 1: The evaluator shall demonstrate that after configuring the TOE for first use from the operational guidance, it is possible to establish an administrative session with the TOE on the "wired" portion of the device. They shall then demonstrate that an identically configured wireless client that can successfully connect to the TOE cannot be used to perform administration.*

4.1.6 Class: Protection of the TSF (FPT)

Fail Secure (FPT_FLS)

FPT_FLS.1	**Fail Secure**
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: **failure of the power-on self-tests.**

Application Note:

191 *The intent of this requirement is to express the fail secure capabilities that the TOE possesses. This means that the TOE must be able to attain a secure/safe state when any of the identified failures occurs. If the TOE should encounter a failure in the middle of a critical operation, the TOE should not just quit operating leaving key material and user data unprotected.*

Assurance Activity:

192 *The evaluator shall review the TSS section to determine that the TOE's implementation of the fail secure functionality is documented. The evaluator shall first examine the TSS section to ensure that all failure modes specified in the ST are described. The evaluator shall then ensure that the TOE will attain a secure state after inserting each specified failure mode type. The evaluator shall review the TSS to determine that the definition of secure state is defined and is suitable to ensure protection of key material and user data.*

Replay Detection (FPT_RPL)

FPT_RPL.1	**Replay Detection**
FPT_RPL.1.1	The TSF shall detect replay for the following entities: [*network packets terminated at the TOE*].
FPT_RPL.1.2	The TSF shall perform: [*reject the data]* when replay is detected.

Application Note:

193 *Receiving multiple network packets due to network congestion or lost packet acknowledgments is not considered a replay attack. The intent of this requirement is to ensure that any communications of a*

trusted nature (administrator to TOE, IT entity to TOE, TOE to TOE) are covered by the element and cannot be replayed.

Reliable Time Stamps (FPT_STM)

FPT_STM.1	Reliable Time Stamp
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps for its own use.

TSF Self Test (FPT_TST)

FPT_TST_EXT.1	Extended: TSF Testing
FPT_TST_EXT.1.1	The TSF shall run a suite of self tests during the 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 service specified in FCS_COP.1(2).

Assurance Activity:

194 *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.*

195 *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, which includes the generation and protection of the "check value" used to ensure integrity as well as the verification step. This description shall also cover the digital signature service used in performing these functions. The evaluator also checks the operational guidance to ensure that any actions required by the administrator to initialize or operate this functionality are present.*

196 *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: Following the operational guidance, the evaluator shall initialize the integrity protection system. The evaluator shall perform actions to cause TSF software to load and observe that the integrity mechanism does not flag any executables as containing integrity errors.*
- *Test 2: The evaluator modifies the TSF executable, and causes that executable to be loaded by the TSF. The evaluator observes that an integrity violation is triggered (care must be taken so that the integrity violation is determined to be the cause of the failure to load the*

module, and not the fact that the module was modified so that it was rendered unable to run because its format was corrupt).

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:

197 *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:

198 *Updates to the TOE are signed by an authorized source and may have a hash associated. For the digital signature mechanism, 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, and if implemented, calculating the hash of the updates; and the actions that take place for successful (signature, and hash if included, verifications) and unsuccessful (signature, and hash if included. 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: Resource Utilization (FRU)

Resource Allocation (FRU_RSA)

FRU_RSA.1	Maximum Quotas
FRU_RSA.1.1	The TSF shall enforce maximum quotas of the following resources: [assignment: *resources supporting the administrative interface*], [selection: [assignment: *controlled resources*], *no other resources*] that [selection: *individual user, defined group of users, subjects*] can use [selection: *simultaneously, over a specified period of time*].

Application Note:

199 *At a minimum, compliant TOEs must impose quotas on exhaustible resources used to support the remote administrative interface; these are listed in the first assignment. Other resources that can be controlled (e.g., TCP connection resources) should be listed in the second assignment; if there are no other resources then the last item in the selection should be chosen. The second selection should be chosen to reflect the consumers of the resource that are to be controlled. The last selection is used to limit the timeframe associated with the use of the controlled resources (e.g., a quota on the number of TCP connection requests from a given IP address in 30 seconds).*

Assurance Activity:

200 *The evaluator shall examine the TSS to ensure that it identifies all resources controlled through the quota mechanism, and that this list contains those resources used to support the administrative interface. The evaluator shall ensure that the TSS describes how each resource is counted as "used" and how a maximum quota or use is determined, as well as the action taken when the quota is reached. The TSS shall also describe whether the quota is imposed on users or subjects (in this case TOE processes) and whether the quota imposed is for simultaneous use or cumulative use over a period of time. The evaluator shall examine the operational guidance to determine that it contains instructions for establishing quotas (if they are configurable), and describes any actions administrators can or should take in response to a quota being reached.*

201 *The evaluator shall also perform the following tests for each controlled resource:*

- *Test 1: The evaluator follows the operational guidance to configure quotas for the resource (if such a capability is provided). The evaluator then causes the resource quota to be reached, and observes that the action specified in the TSS occurs.*

4.1.8 Class: TOE Access (FTA)

TSF-initiated Session Locking and Termination (FTA_SSL)

FTA_SSL_EXT.1	TSF-initiated session locking
FTA_SSL_EXT.1.1	**Refinement:** The TSF shall, for **local** interactive sessions, [selection: • lock the session – clear or overwrite display devices, making the current contents unreadable, disable any activity of the user's data access/display devices other than unlocking the session, and

require that the administrator re-authenticate to the TSF prior to unlocking the session;
- terminate the session]

after an Authorized Administrator specified time period of inactivity.

Assurance Activity:

202 *The evaluator shall perform the following test:*

- *Test 1: The evaluator follows the operational guidance to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a local interactive session with the TOE. The evaluator then observes that the session is either locked or terminated after the configured time period. If locking was selected from the component, the evaluator then ensures that re-authentication is needed when trying to unlock the session.*

FTA_SSL.3	**TSF-initiated termination**
FTA_SSL.3.1	The TSF shall terminate a **remote** interactive session after an **Authorized Administrator-configurable time interval of session inactivity**.

Assurance Activity:

203 *The evaluator shall perform the following test:*

- *Test 1: The evaluator follows the operational guidance to configure several different values for the inactivity time period referenced in the component; these shall consist at least of the minimum and maximum allowed values as specified in the operational guidance, as well as one other value. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.*

FTA_SSL.4	**User-initiated termination**
FTA_SSL.4.1	The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

Assurance Activity:

204 *The evaluator shall perform the following test:*

- *Test 1: The evaluator initiates an interactive local session with the TOE. The evaluator then follows the operational guidance to exit or log off the session and observes that the session has been terminated.*
- *Test 2: The evaluator initiates an interactive remote session with the TOE. The evaluator then follows the operational guidance to exit or log off the session and observes that the session has been terminated.*

TOE Access Banners (FTA_TAB)

FTA_TAB.1	Default TOE Access Banners
FTA_TAB.1.1	**Refinement:** Before establishing **an administrative user** session the TSF shall be capable of displaying **an Authorized Administrator-specified** advisory **notice and consent** warning message regarding unauthorized use of the TOE.

Application Note:

205 *This requirement is intended to apply to interactive sessions between a human user and a TOE. IT entities establishing connections or programmatic connections (e.g., remote procedure calls over a network) are not required to be covered by this requirement.*

Assurance Activity:

206 *The evaluator shall check the TSS to ensure that it details each method of access (local and remote) available to the administrator (e.g., serial port, SSH, HTTPS). The evaluator shall also perform the following test:*

- *Test 1: The evaluator follows the operational guidance to configure a notice and consent warning message. The evaluator shall then, for each method of access specified in the TSS, establish a session with the TOE. The evaluator shall verify that the notice and consent warning message is displayed in each instance.*

TOE Session Establishment (FTA_TSE)

FTA_TSE.1	TOE Session Establishment
FTA_TSE.1.1	**Refinement:** The TSF shall be able to deny establishment **of a wireless client session** based on **location, time, day, [assignment: other attributes]**.

Application Note:

207 *The "location" can be specified in terms of a port number, IP address, subnet, VLAN, TOE interface, etc.*

208 *The assignment is to be used by the ST author to specify additional attributes on which denial of session establishment can be based.*

Assurance Activity:

209 *The evaluator shall examine the TSS to determine that all of the attributes on which a client session can be denied 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 successfully establishes a client session with a wireless client. The evaluator then follows the operational guidance to configure the system so that that client's access is denied based on a specific value of the attribute. The evaluator shall then attempt*

to establish a session in contravention to the attribute setting (for instance, the location is denied based upon the client's IP address). The evaluator shall observe that the access attempt fails.

4.1.9 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, IPsec, and [selection: SSH, TLS, TLS/HTTPS, no other protocols]** to provide a **trusted** communication channel between itself and **all authorized IT entities** 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*, ***or the authorized IT entities*** to initiate communication via the trusted channel.
FTP_ ITC.1.3	The TSF shall initiate communication via the trusted channel for [assignment: *list of services for which the TSF is able to initiate communications*].

Application Note:

210 *The intent of the above requirement is to use a cryptographic protocol to protect all external communications with authorized IT entities that the TOE interacts with to perform its functions. 802.11-2007 is required for communications with wireless clients; IPsec is required at least for communications with the authentication server. If communications with other necessary authorized IT entities (NTP server, audit server), then they must use IPsec or one of the other listed protocols (SSH, TLS and TLS/HTTPS are allowed), and the ST author makes the appropriate selections.. After the ST author has made the selections, they are to select the detailed requirements in Annex C corresponding to their selection to put in the ST.*

211 *While there are no requirements on the party initiating the communication, the ST author lists in the assignment for FTP_ITC.1.3 the services for which the TOE can initiate the communication with the authorized IT entity.*

212 *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:

213 *The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities, each communications mechanism is identified in terms of the allowed protocols for that IT entity. 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 allowed protocols with each authorized IT entity, 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 communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.*
- *Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the operational guidance to ensure that in fact the communication channel can be initiated from the TOE.*
- *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, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted. The evaluator shall ensure that when physical connectivity is restored, communications are appropriately protected.*

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

Trusted Path (FTP_TRP)

FTP_TRP.1	**Trusted Path**
FTP_TRP.1.1	**Refinement:** The TSF shall **use [selection, choose at least one of: IPsec, SSH, TLS, TLS/HTTPS]** provide **a trusted** communication path between itself and **remote administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *disclosure and detection of modification of the communicated data*.
FTP_TRP.1.2	**Refinement:** The TSF shall permit **remote administrators** to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for *initial administrator authentication and all remote administration actions*.

Application Note:

215 *This requirement ensures that authorized remote administrators (and other ST author specified roles) initiate all communication with the TOE via a trusted path, and that all communications with the TOE by remote administrators is performed over this path. The data passed in this trusted communication*

channel are encrypted as defined the protocol chosen in the first selection. The ST author chooses the mechanism or mechanisms supported by the TOE, and then ensures the detailed requirements in Annex C corresponding to their selection are copied to the ST if not already present.

Assurance Activity:

216 *The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST. The evaluator shall confirm that the operational guidance contains instructions for establishing the remote administrative sessions for each supported method. The evaluator shall also perform the following tests:*

- *Test 1: The evaluators shall ensure that communications using each specified (in the operational guidance) remote administration method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.*
- *Test 2: For each method of remote administration supported, the evaluator shall follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish a remote administrative sessions without invoking the trusted path.*
- *Test 3: The evaluator shall ensure, for each method of remote administration, the channel data is not sent in plaintext.*
- *Test 4: The evaluator shall ensure, for each method of remote administration, modification of the channel data is detected by the TOE.*

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

4.2 Rationale for Security Functional Requirements

218 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.

219 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 users are not communicating	FCS_IPSEC_EXT.1 [FCS_TLS_EXT.1 FCS_SSH_EXT.1	FTP_ITC.1 and FTP_TRP.1 (and the supporting protocols 802.11-2007, FCS_IPSEC_EXT.1, FCS_TLS_EXT.1,

with some other entity pretending to be the TOE, and that the TOE is communicating with an authorized IT entity and not some other entity pretending to be an authorized IT entity.	FCS_HTTPS_EXT.1] FTP_ITC.1 FTP_TRP.1 FIA_8021X_EXT.1 FIA_UIA_EXT.1 FIA_PSK_EXT.1	FCS_SSH_EXT.1, and FCS_HTTPS_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. FIA_X8021X_EXT.1 provides the two-way authentication necessary to allow a wireless client access to the wired network, and serves as a part of the 802.11-2007 WPA2 protocol to establish the communication channel with the wireless client. FIA_UIA_EXT.1 requires administrators (including remote administrators) to be identified and authenticated by the TOE, providing assurance for that end of the communication path. FIA_PSK_EXT.1 requires the TOE support the formation of strong pre-shared keys (either though a large character set for text-based pre-shared keys, or through generation by the TOE's (or an off-box) RBG function) that can be used to mutually authenticate the TOE and its communication partner. *Application Note: The ST author will modify the rationale to reflect the protocols that are implemented by the TOE.*
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.	FCS_CKM.1(1) FCS_CKM.1(2) FCS_CKM.2(1) FCS_CKM.2(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(1) and FCS_CKM.1(2) generate symmetric and asymmetric key, respectively. These keys are used by the AES encryption/decryption functionality specified in FCS_COP.1(5) and used for cryptographic signatures as specified in FCS_COP.1(2). FCS_CKM.2(1) and FCS_CKM.2(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. This applies not only to key that resides in the TOE, but also to intermediate areas (physical memory,

		page files, memory dumps, etc.) where key material may appear. 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 identification and authentication of authorized IT entities and remote administrators. 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. FCS_RBG_EXT.1 ensures that keying material is robustly generated. FIA_X509_EXT.1 requires that the certificates used to support many of the cryptographic operations previously mentioned conform to an appropriate standard.
O.DISPLAY_BANNER The TOE will display an advisory warning regarding use of the TOE.	FTA_TAB.1	FTA_TAB.1 requires the TOE to display an administrator defined banner before a user can establish an authenticated session. This banner is under complete control of Authorized Administrators in which they specify any warnings regarding unauthorized use of the TOE.
O.FAIL_SECURE The TOE shall fail in a secure manner following failure of the power-on self tests.	FPT_FLS.1	FPT_FLS.1 requires that on a detected failure the TOE maintains a secure state.
O.PROTECTED_COMMUNICATIONS The TSF shall protect TSF data when it is in transit between the TSF and another trusted IT entity.	FAU_STG_EXT.1 FCS_IPSEC_EXT.1 [FCS_TLS_EXT.1 FCS_SSH_EXT.1 FCS_HTTPS_EXT.1] FTP_ITC.1 FTP_TRP.1 FIA_8021X_EXT.1 FPT_RPL.1	FAU_STG_EXT.1 protects the audit records through transmission between external audit storage. FTP_ITC.1 and FTP_TRP.1 (and the supporting protocols 802.11-2007, FCS_IPSEC_EXT.1, FCS_TLS_EXT.1, FCS_SSH_EXT.1, and FCS_HTTPS_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. FIA_X8021X_EXT.1 provides the two-way authentication necessary to allow a wireless client access to the wired network, and serves as a part of the 802.11-2007 WPA2 protocol to establish the communication channel with the wireless client. FPT_RPL.1 ensures that administrator sessions or data communicated with an authorized IT entity cannot be replayed. *Application Note: The ST author will modify the rationale to reflect the protocols that are implemented by the TOE.*
O.PROTOCOLS The TOE will ensure that standardized protocols are implemented in the TOE to RFC and/or Industry specifications to ensure interoperability.	FCS_IPSEC_EXT.1 [FCS_TLS_EXT.1 FCS_SSH_EXT.1 FCS_HTTPS_EXT.1] FTP_ITC.1 FIA_8021X_EXT.1	FCS_IPSEC_EXT.1, FCS_TLS_EXT.1, FCS_SSH_EXT.1, FCS_HTTPS_EXT.1, FTP_ITC.1 (for 802.11-2007) and FIA_8021X_EXT.1 (in support of 802.11-2007) all reference the standards (and indicate any restrictions on those standards) applicable to the protocol they require to be implemented. *Application Note: The ST author will modify the rationale to reflect the protocols that are implemented by the TOE.*
O.REPLAY_DETECTION The TOE will provide a means to detect and reject the replay of authentication data and other TSF data and security attributes.	FPT_RPL.1	FPT_RPL.1 requires the TOE to detect and reject any attempted replay of authentication data from a remote user.
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.RESOURCE_AVAILABILITY The TOE shall provide mechanisms that mitigate user attempts to exhaust TOE resources (e.g., persistent storage).	FRU_RSA.1	FRU_RSA.1 imposes quotas on exhaustible resources such that resources can be controlled and DoS attacks may be mitigated.
O.ROBUST_TOE_ACCESS The TOE will provide mechanisms that control an administrator's logical access to the TOE and to control administrative access from a wireless client.	FIA_AFL.1 FIA_PMG_EXT.1 FIA_UAU_EXT.5 FIA_UAU.6 FIA_UAU.7 FIA_UIA_EXT.1 FMT_SMR.1 FTA_SSL_EXT.1 FTA_SSL.3 FTA_SSL.4	FIA_AFL. provides a settable unsuccessful authentication attempt threshold that prevents unauthorized users acting remotely from gaining access to authorized administrator's account by guessing authentication data by locking the targeted account until the Authorized Administrator takes some action (e.g., re-enables the account) or for some Authorized Administrator defined time period. FIA_PMG_EXT.1 defines the attributes of passwords used by administrative users to ensure that strong passwords and passphrases can be chosen and maintained. FIA_UAU_EXT.5 requires that the TSF provides local authentication methods (one of which is required to be a local password-based mechanism, with other optional (potentially off-box) mechanisms allowed) to ensure that unauthorized users cannot gain logical access to the TOE. FIA_UAU.6 requires a user to reauthenticate when a password is changed or the session is locked and FIA_UAU.7 ensures that authentication feedback is obscured at the local console. FIA_UIA_EXT.1 plays a role in satisfying this objective by ensuring that every user is identified and authenticated before the TOE performs any mediated functions. FMT_SMR.1 controls the administrator's ability to perform administrative actions from a wireless client; the capability must be disabled by default. FTA_SSL_EXT.1 provides the Authenticated Administrator the capability to specify a time interval of inactivity in which an unattended local administrative session would be locked and will require the administrator responsible for that session to re-authenticate before the session can be

		used to access TOE resources. FTA_SSL.3 takes into account remote sessions. After an Administrator-defined time interval of inactivity remote sessions will be terminated, this includes user proxy sessions and remote administrative sessions. This component is especially necessary since remote sessions are not typically afforded the same physical protections that local sessions are provided. FTA_SSL.4 provides administrators the capability to exit or logoff administrative sessions, rather than wait for the session to be terminated.
O.SESSION_LOCK The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.	FTA_SSL_EXT.1 FTA_SSL.3 FTA_SSL.4	FTA_SSL_EXT.1 provides an authenticated Administrator the capability to specify a time interval of inactivity in which an unattended local administrative session would be locked and will require the administrator responsible for that session to re-authenticate before the session can be used to access TOE resources. FTA_SSL.3 takes into account remote sessions. After an Authorized Administrator defined time interval of inactivity remote sessions will be terminated, this includes user proxy sessions and remote administrative sessions. This component is especially necessary because remote sessions are not typically afforded the same physical protections that local sessions are provided. FTA_SSL.4 provides administrators the capability to exit or logoff administrative sessions, rather than wait for the session to be terminated.
O.SYSTEM_MONITORING The TOE will provide the capability to generate audit data and send those data to an external IT entity.	FAU_GEN.1 FAU_GEN.2 FAU_SEL.1 FAU_STG.1 FAU_STG_EXT.1 FAU_STG_EXT.3 FPT_STM.1	FAU_GEN.1 defines the set of events that the TOE must be capable of recording. FAU_GEN.2 ensures the audit records associate a user identity with the auditable event. FAU_SEL.1 allows the administrator to configure which auditable events will be recorded in the audit trail. FAU_STG.1 requires some amount of local audit storage which must be

		protected from unauthorized access. FAU_STG_EXT.1 protects the audit records through transmission between external audit storage. FAU_STG_EXT.3 defines the set of events that must occur when the link to the external audit storage is not available. FPT_STM.1 requires that the TOE be able to provide reliable time stamps for use in audit records.
O.TIME_STAMPS The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these timestamps	FPT_STM.1	FPT_STM.1 requires that the TOE be able to provide reliable time stamps for its own use and therefore, partially satisfies this objective. Time stamps include date and time and are reliable in that they are always available to the TOE, and the clock must be monotonically increasing.
O.TOE_ADMINISTRATION The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.	FIA_PMG_EXT.1 FIA_UAU.5 FMT_MTD.1(1)-(3) FMT_MOF.1 FMT_SMF.1 FMT_SMR.1 FTP_TRP.1	FIA_PMG_EXT.1 defines management capabilities and requirements for administrator specification of password/secret strength. FIA_UAU_EXT.5 requires that the TSF provides local authentication methods (one of which is required to be a local password-based mechanism, with other optional (potentially off-box) mechanisms allowed) to ensure that unauthorized users cannot gain logical access to the TOE. FMT_MTD.1 and FMT_MOF.1 restrict the ability to manage certain functionality and identify security attributes of an authorized administrator. FMT_SMF.1 specifies the management functions that an only administrator must perform. FMT_SMR.1 defines at least one administrator role (Authorized Administrator) to perform administrative actions. The TSF is able to associate a human user to this role. FTP_TRP.1 requires that the TSF provide a trusted path for remote administration.
O.TSF_SELF_TEST	FPT_FLS.1 FPT_TST_EXT.1	FPT_FLS.1 requires that on a detected

The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.		failure the TOE maintains a secure state. FPT_TST_EXT.1 requires the TOE to provide a suite of self tests to assure the correct operation of the TSF.
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_CLIENT_ACCESS The TOE will provide the capability to restrict a wireless client in connecting to the TOE.	FTA_TSE.1	FTA_TSE.1 provides the capability to control access by wireless clients based on time of day, their location (e.g., IP address), and other attributes that may be implemented by the TOE.

4.3 Security Assurance Requirements

220 The Security Objectives for the TOE in Section 3.1 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.

221 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.

222 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.

223 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

Assurance Class	Assurance Components	Assurance Components Description
	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

224 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

225 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.

226 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. Because the TOE supports both remote and local administration of the TOE, the interfaces that provide local and remote authentication and the administrator access to configuration/maintenance functionality must be described.

227 When the TOE is a multiple component TOE, the interfaces used to create a virtual management network are described.

228 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:

229 *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 the there is insufficient interface information, then an adequate functional specification has not been provided.*

4.3.2 Class AGD: Guidance Documents

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

231 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 login to the TOE locally and remotely.

232 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:

233 *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.*

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

235 *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.*

236 *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.*

237 *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:*

1. *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.*

2. *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).*

3. *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:

238 *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.*

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

- *Instructions and information is provided to the administrator detailing how to configure the virtual management network so that control/configuration network traffic between TOE components is encrypted and that this is the only allowed configuration for conformant TOEs. If the TOE is a multiple component TOE, 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.

- *As indicated in the introductory material, administration of the TOE is performed by administrator role. At a high level, the guidance must contain the appropriate instructions to allow local and remote authenticated administrator access.*

4.3.3 Class ATE: Tests

240 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

241 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:

242 *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.*

243 *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.*

244 *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.*

245 *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

246 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:

247 *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 Access System 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

248 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

249 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:

250 *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

251 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:

252 *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

253 The rationale for choosing these security assurance requirements is that this is the first U.S. Government 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 and References

[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

Acronyms

AES	Advanced Encryption Standard
AF	Authorization factor
AS	Authorization subsystem
CAVS	Cryptographic Algorithm Validation System
CC	Common Criteria
CCTL	Common Criteria Testing Laboratory
CM	Configuration management
COTS	Commercial Off-The-Shelf
CMVP	Cryptomodule 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_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_SMF.1, FMT_SMR.1
AC-6	Least Privilege	FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3)
AC-7	Unsuccessful Login Attempts	FIA_AFL.1
AC-8	System use Notification	FTA_TAB.1
AC-11	Session Lock	FIA_UAU.6, FTA_SSL_EXT.1
AC-14	Permitted Actions Without Identification	FIA_UIA_EXT.1
AC-17(7)	Remote Access	FCS_SSH_EXT.1
AU-2	Auditable Events	FAU_GEN.1
AU-2(4)		FAU_GEN.1
AU-3	Content of Audit Records	FAU_GEN.1, FAU_GEN.2
AU-3(1)		FAU_GEN.1
AU-5	Response to Audit Processing Failures	FAU_STG_EXT.3
AU-7	Audit Reduction and Report Generation	FAU_SEL.1
AU-8	Time Stamps	FPT_STM.1
AU-9	Protection of Audit Information	FAU_STG.1, FAU_STG_EXT.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-2	Identification and Authentication	FIA_UIA_EXT.1, FIA_UAU_EXT.5, FPT_RPL.1
IA-3	Device Identification and Authentication	FIA_8021X_EXT.1, FTP_ITC
IA-5	Authenticator Management	FIA_PMG_EXT.1, FIA_PSK_EXT.1, FIA_X509_EXT.1
IA-6	Authenticator Feedback	FIA_UAU.7
SC-4	Information in Shared Resources	FDP_RIP.2
SC-6	Resource Priority	FRU_RSA.1
SC-8	Transmission Integrity	FCS_IPSEC_EXT.1, FCS_TLS_EXT.1, FCS_HTTPS_EXT.1, FCS_SSH_EXT.1, FTP_ITC.1
SC-9	Transmission Confidentiality	FCS_IPSEC_EXT.1, FCS_TLS_EXT.1, FCS_HTTPS_EXT.1, FCS_SSH_EXT.1, FTP_ITC.1
SC-10	Network Disconnect	FTA_SSL.3
SC-11	Trusted Path	FTP_TRP.1
SC-12	Cryptographic Key Establishment and Management	FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2(1), FCS_CKM.2(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_FLS.1, FPT_TST_EXT.1

Appendix C: Additional Requirements

254 *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 Access System products) are welcome and solicited.*

255 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)

256 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:

257 *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: Cryptographic Support (FCS)

Extended: HTTPS (FCS_HTTPS_EXT)

If HTTPS is selected as a supported protocol then this requirement must be included in the ST.

FCS_HTTPS_EXT.1	**Extended: HTTP Security (HTTPS)**
FCS_HTTPS_EXT.1.1	The TSF shall implement the HTTPS protocol that complies with RFC 2818.
FCS_HTTPS_EXT.1.2	The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

Application Note:

258 *The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done either by adding elements to this component, or by additional detail in the TSS.*

Assurance Activity:

259 *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_HTTPS_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 "MUST" or "SHOULD" statements shall be described;*
- *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.*

260 *FCS_HTTPS_EXT.1.2 - The evaluator shall check the TSS to ensure that it is clear on how HTTPS uses TLS to establish an administrative session, focusing on any client authentication required by the TLS protocol*

vs. administrator authentication which may be done at a different level of the processing stack. Testing for this activity is done as part of the TLS testing; this may result in additional testing if the TLS tests are done at the TLS protocol level.

Extended: Secure Shell (FCS_SSH_EXT)

If SSH is selected as a supported protocol then this requirement must be included in the ST.

FCS_SSH_EXT.1	**Extended: Secure Shell (SSH)**
FCS_SSH_EXT.1.1	The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.
FCS_SSH_EXT.1.2	The TSF shall ensure that the SSH connection be rekeyed after no more than 2^{28} packets have been transmitted using that key.
FCS_SSH_EXT.1.3	The TSF shall ensure that the SSH protocol implements a timeout period for authentication as defined in RFC 4252 of [assignment: timeout period], and provide a limit to the number of failed authentication attempts a client may perform in a single session to [assignment: maximum number of attempts] attempts.
FCS_SSH_EXT.1.4	The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.
FCS_SSH_EXT.1.5	The TSF shall ensure that, as described in RFC 4253, packets greater than [assignment: number of bytes] bytes in an SSH transport connection are dropped.
FCS_SSH_EXT.1.6	The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256-CBC, [assignment: AEAD_AES_128_GCM, AEAD_AES_256_GCM, no other encryption algorithms].
FCS_SSH_EXT.1.7	The TSF shall ensure that the SSH transport implementation uses SSH_RSA and [selection: PGP-SIGN-RSA, PGP-SIGN-DSS, no other public key algorithms] as its public key algorithm(s).
FCS_SSH_EXT.1.8	The TSF shall ensure that the data integrity algorithm used in the SSH transport connection is hmac-sha1 and [selection: no other algorithm, hmac-sha1-96, hmac-md5, hmac-md5-96].
FCS_SSH_EXT.1.9	The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

Application Note:

261 *FCS_SSH_EXT.1.1 - The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done either by adding elements to this component, or by additional detail in the TSS.*

262 *FCS_SSH_EXT.1.3 –In the first assignment, the ST author should insert the timeout period (e.g., "10 minutes") from the initiation of authentication session after which the session should timeout if authentication has been unsuccessful. In the second assignment, the maximum number of failed authentication attempts is specified. The RFC indicates the server should drop the session after this number of failed attempts.*

263 *FCS_SSH_EXT.1.5 - RFC 4253 provides for the acceptance of "large packets" with the caveat that the packets should be of "reasonable length" or dropped. The assignment should be filled in by the ST author with the maximum packet size accepted, thus defining "reasonable length" for the TOE.*

264 *FCS_SSH_EXT.1.6 - In subsequent publications of this PP, it is likely that AES-GCM will be required and CBC will become optional. In the assignment, the ST author can select the AES-GCM algorithms, or "no other algorithms" if AES-GCM is not supported. If AES-GCM is selected, there should be corresponding FCS_COP entries in the ST.*

265 *FCS_SSH_EXT.1.7 - RFC 4253 specifies required and allowable public key algorithms. This requirement makes SSH-RSA "required" and allows two others to be claimed in the ST. The ST author should make the appropriate selection, selecting "no other public key algorithms" if only SSH_RSA is implemented.*

266 *FCS_SSH_EXT.1.8 – As per the RFC, HMAC-SHA1 is required, but there are additional integrity algorithms that are allowed. The ST author chooses the algorithm(s) implemented by the TOE; if there are no additional algorithms, then that should be selected.*

Assurance Activity:

267 *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_SSH_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 "MUST" or "SHOULD" statements shall be described;*
- *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.*

268 *FCS_SSH_EXT.1.2 - The evaluator shall examine the TSS to ensure that it specifies that the TOE rekeys an SSH connection before more than 2^{28} packets have been sent with a given key. If this effect is achieved by configuration of the TOE, then the evaluator shall examine the operational guidance to ensure that it contains instructions on setting the appropriate values.*

269 *FCS_SSH_EXT.1.3 - The evaluator shall check to ensure that the TSS specifies the timeout period and the method for dropping a session connection after the number of failed authentication attempts specified in*

the requirement. If these values are configurable and may be specified by the administrator, the evaluator shall check the operational guidance to ensure that it contains instructions for configuring these values. The evaluator shall also perform the following tests:

- *Test 1: The evaluator shall demonstrate that taking longer than the timeout period to authenticate to the TOE results in a disconnection of the current session and requires that the evaluator initiate a new session to attempt to connect. If the timeout period is configurable, the evaluator shall ensure that the operational guidance is followed to implement at least two different periods in order to ensure that the mechanism works as specified.*

- *Test 2: The evaluator shall demonstrate that performing a number of failed SSH authentication attempts equal to the value specified in the requirement results in a disconnection of the current session and requires that the evaluator initiate a new session to attempt to connect. If this number is configurable, the evaluator shall ensure that the operational guidance is followed to implement at least two different limits (e.g., 3 attempts and 5 attempts) in order to ensure that the mechanism works as specified.*

270 *FCS_SSH_EXT.1.4 - The evaluator shall check to ensure that the TSS contains a description of the public key algorithms that are acceptable for use for authentication, that this list conforms to FCS_SSH_EXT.1.7, and ensure that password-based authentication methods are also allowed. The evaluator shall also perform the following tests:*

- *Test 1: The evaluator shall, for each public key algorithm supported, show that the TOE supports the use of that public key algorithm to authenticate a user connection. Any configuration activities required to support this test shall be performed according to instructions in the operational guidance.*

- *Test 2: Using the operational guidance, the evaluator shall configure the TOE to accept password-based authentication, and demonstrate that a user can be successfully authenticated to the TOE over SSH using a password as an authenticator.*

271 *FCS_SSH_EXT.1.5 - The evaluator shall check that the TSS describes how "large packets" in terms of RFC 4253 are detected and handled. The evaluator shall also perform the following test:*

- *Test 1: The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.*

272 *FCS_SSH_EXT.1.6 - The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the encryption algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the encryption algorithms 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 SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements). The evaluator shall also perform the following test:*

- *Test 1: The evaluator shall establish a SSH connection using each of the encryption algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of a protocol to satisfy the intent of the test.*

273 *FCS_SSH_EXT.1.7 - The assurance activity associated with FCS_SSH_EXT.1.4 verifies this requirement.*

274 *FCS_SSH_EXT.1.8 - The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms, and that that list corresponds to the list in this component. The evaluator shall also check the operational guidance to ensure that it contains instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the "none" MAC algorithm is not allowed).*

275 *FCS_SSH_EXT.1.9 - The evaluator shall ensure that operational guidance contains configuration information that will allow an authorized administrator to configure the TOE so that all key exchanges for SSH are performed using DH group 14. If this capability is "hard-coded" into the TOE, the evaluator shall check the TSS to ensure that this is stated in the discussion of the SSH protocol. The evaluator shall also perform the following test:*

- *Test 1: The evaluator shall attempt to perform a diffie-hellman-group1-sha1 key exchange, and observe that the attempt fails. The evaluator shall then attempt to perform a diffie-hellman-group14-sha1 key exchange, and observe that the attempt succeeds.*

Extended: Transport Layer Security (FCS_TLS_EXT)

If TLS is selected as a supported protocol then this requirement must be included in the ST.

FCS_TLS_EXT.1	**Extended: Transport Layer Security (TLS)**
FCS_TLS_EXT.1.1	The TSF shall implement one or more of the following protocols [selection: TLS 1.0 (RFC 2346), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites: **Mandatory Ciphersuites:** 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* *TLS_RSA_WITH_AES_256_CBC_ SHA256* *TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256* *TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256* *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256* *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
].

Application Note:

276 *The ST author must make the appropriate selections and assignments to reflect the TLS implementation. The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done either by adding elements to this component, or by additional detail in the TSS.*

277 *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. If administrative steps need to be taken so that the suites negotiated by the implementation are limited to those in this requirement, the appropriate instructions need to be contained in the guidance called for by AGD_OPE.*

278 *The Suite B algorithms (RFC 5430) listed above are the preferred algorithms for implementation. Future publications of this PP will require support for TLS 1.2 (RFC 5246). In addition, future publications of this PP will require that the TOE offer a means to deny all connection attempts using specified older versions of the SSL/TLS protocol.*

Assurance Activity:

279 *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_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 "MUST" or "SHOULD" statements shall be described;*
- *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.*

280 *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). The evaluator shall also perform the following test:*

- *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 a HTTPS 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).

C.3 Class: Protection of the TSF (FPT)

281 In the case that the TOE is physically distributed among several components, communications between those components must be protected. This is to be accomplished in the same manner as communications with authorized IT entities.

FPT_ITT.1	**Basic Internal TSF Data Transfer Protection**
FPT_ITT.1.1(1)	**Refinement**: The TSF shall protect TSF data from *disclosure* ***and protect it from modification*** when it is transmitted between separate parts of the TOE **through the use [selection, choose at least one of: IPsec, SSH, TLS, TLS/HTTPS]**.

Application Note:

282 *This requirement ensures all communications between components of a distributed TOE is protected through the use of an encrypted communications channel. The data passed in this trusted communication channel are encrypted as defined the protocol chosen in the first selection. The ST author chooses the mechanism or mechanisms supported by the TOE, and then ensures the detailed requirements in Annex C corresponding to their selection are copied to the ST if not already present.*

Assurance Activity:

283 *The evaluator shall examine the TSS to determine that the methods and protocols used to protect distributed TOE components are described. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST. The evaluator shall confirm that the operational guidance contains instructions for establishing the communication paths for each supported method. The evaluator shall also perform the following tests:*

- *Test 1: The evaluators shall ensure that communications using each specified (in the operational guidance) communications method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.*
- *Test 2: The evaluator shall ensure, for each method of communication, the channel data is not sent in plaintext.*
- *Test 3: The evaluator shall ensure, for each method of communication, modification of the channel data is detected by the TOE.*

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

C.4 Audit Requirements

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
FCS_TLS_EXT.1	Protocol failures. Establishment/Termination of a TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_SSH_EXT.1	Protocol failures Establishment/Termination of an SSH session	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_HTTPS_EXT.1	Protocol failures Establishment/Termination of a HTTPS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FPT_ITT.1	None	

Appendix D: Document Conventions

285 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.

286 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

287 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

288 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

289 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

290 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.

291 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

292 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

293 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

294 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) Access Systems
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:	WLAN, Access Point, WLAN Access System, EAP, IEEE 802.11