US Government

Wireless Local Area Network (WLAN) Access System

Protection Profile For

Basic Robustness Environments

Information Assurance Directorate

July 25, 2007

Version 1.1

Protection Profile Title:

U.S. Government Protection Profile Wireless Local Area Network (WLAN) Access System Basic Robustness Environments

Criteria Version:

This Protection Profile "*US Government Protection Profile Wireless Local Area Network (WLAN) Access System for Basic Robustness Environments"* (PP) was updated using Version 3.1 of the Common Criteria (CC).

Editor's note: The purpose of this update was to bring the PP up to the new CC 3.1 standard without changing the authors' original meaning or purpose of the documented requirements. The original PP was developed using version 2.x of the CC. The CC version 2.3 was the final version 2 update that included all international interpretations. CC version 3.1 used the final CC version 2.3 Security Functional Requirements (SFR)s as the new set of SFRs for version 3.1. Some minor changes were made to the SFRs in version 3.1, including moving a few SFRs to Security Assurance Requirements (SAR)s. There may be other minor differences between some SFRs in the version 2.3 PP and the new version 3.1 SFRs. These minor differences were not modified to ensure the author's original intent was preserved.

The version 3.1 SARs were rewritten by the common criteria international community. The NIAP/CCEVS staff developed an assurance equivalence mapping between the version 2.3 and 3.1 SARs. The assurance equivalent version 3.1 SARs replaced the version 2.3 SARs in the PP.

Any issue that may arise when claiming compliance with this PP can be resolved using the observation report (OR) and observation decision (OD) process.

Further information, including the status and updates of this protection profile can be found on the CCEVS website: http://www.niap-ccevs.org/cc-scheme/pp/. Comments on this document should be directed to ppcomments@missi.ncsc.mil. The email should include the title of the document, the page, the section number, the paragraph number, and the detailed comment and recommendation.

Table of Contents

List of Figures and Tables

Conventions and Terminology

Conventions

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.

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 requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph C4 of Part 1 of the CC. Each of these operations is used in this PP.
The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.
The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized text*.
The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [Assignment_value].
The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).
The **security target author** operation is used to denote points in which the final determination of attributes is left to the security target writer. Security target writer operations are indicated by the words "ST AUTHOR -".
The CC paradigm also allows protection profile (PP) and security target authors to create their own requirements. Such requirements are termed '**extended requirements**' and 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. In this PP, Extended requirements will be indicated with the "EXT" following the component name.
Application Notes are provided to help the developer, either to clarify the intent of a requirement, identify implementation choices, or to define "pass-fail" criteria for a requirement. For those components where Application Notes are appropriate, the Application Notes will follow the requirement component.

NAMING CONVENTIONS

Assumptions: TOE security environment assumptions are given names beginning with "A."-- e.g., A.ADMINISTRATION.

Threats: TOE security environment threats are given names beginning with "T."-- e.g., T.SIGNAL_DETECT.

Policies: TOE security environment policies are given names beginning with "P."—e.g., P.GUIDANCE.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE.", respectively,—e.g., O.ACCESS and OE.ADMIN.

Document Organization

Section 1 provides the introductory material for this PP. It includes an introduction, a brief description of the WLAN access system TOE and additional identifying information. It also includes a discussion of the factors used to define the TOE environment and the level of Robustness selected for this PP.

Section 2 describes, in detail, the WLAN access system TOE (i.e., the TOE for this PP) and the IT environment upon which the TOE depends.

Section 3 describes the TOE security environment. This includes:

- Secure-use assumptions that describe the presumptive conditions for secure use of the TOE in the a basic robustness environment
- Threats that are to be addressed either completely or partially by the technical countermeasures implemented in the WLAN access system.
- Organizational policies that levy further requirements on the TOE.

In addition this section also identifies those threats and policies that are defined as part of the basic robustness environment that the WLAN access system does not address.

Section 4 defines the security objectives for the WLAN access system in a basic robustness environment.

Section 5 contains the functional and assurance requirements derived from the CC, Parts 2 and 3, respectively that must be satisfied by the WLAN access system. This section also identifies requirements that are levied on the TOE IT environment.

Section 6 provides a rationale to demonstrate that the information technology security objectives for the TOE and its IT environment satisfy the identified policies and threats. The section then provides rationale to show that the set of requirements are sufficient to meet each objective, and that each security objective is addressed by one or more component requirements. Therefore, the two aforementioned subsections provide arguments that the security objectives and security requirements are both necessary and sufficient, respectively and collectively, to meet the needs dictated by the policies and threats. Section also 6 provides arguments that to address any unsatisfied dependencies.

Section 7, Identifies references to noteworthy background and/or supporting materials.

Appendix A is an acronym list that defines frequently used acronyms.

Appendix B is a glossary of terms.

1. Introduction

This Protection Profile (PP) supports future Department of Defense (DoD) procurements of commercial off-the-shelf (COTS) wireless local area network (WLAN) access system components that will be used in basic robustness environments. This PP details the policies, assumptions, threats, security objectives, security functional requirements, and security assurance requirements for the WLAN access point and its supporting environment. The supporting environment includes interactions with WLAN clients, authentication servers, and audit servers.

This PP has two primary audiences: Information System Security Engineers (ISSE) and COTS WLAN access system product vendors. The ISSE may use this PP to help in designing and assessing installations in which COTS WLAN access system devices are part of the infrastructure. WLAN product vendors will use the PP to learn the DoD security requirements for new COTS WLAN devices being procured.

1.1 Identification

Title: US Government Wireless Local Area Network (WLAN) Access System For Basic Robustness Environments Protection Profile

Protection Profile Version: Version 1.1, dated July 25, 2007

Sponsor: National Security Agency (NSA)

CC Version: This PP claims conformance to Criteria for Information Technology Security Evaluation, Version 3.1, September 2006 Part 2 extended and Part 3 conformant to include applicable interpretations.

Conformance Claims: Common Criteria, v3.1 Part 2 extended, and Part 3 conformant. This PP requires demonstrable conformance.

Evaluation Level: Evaluation Assurance Level (EAL) 2 augmented with, ALC_FLR.2 (Flaw Remediation).

Keywords: Access system, basic robustness, radio, wireless, network, wireless local area network, wireless LAN, WLAN, LAN

1.2 Protection Profile Overview

This PP specifies the minimum-security requirement for a WLAN Access System (hereafter referred to as the Target of Evaluation (TOE) used by the US Government in Basic Robustness Environments. The target robustness level of "basic" is specified in the *Guidance and Policy for the Department of Defense Global Information Grid Information Assurance (GIG*).

This PP requires privacy and integrity of communications over the WLAN, using commercially available cryptographic algorithms. Security administration for the access system is also a

requirement. The assurance requirements specified in the PP are EAL 2 augmented with Flaw Remediation.

STs that claim conformance to this PP shall meet a minimum standard of demonstrable-PP conformance as defined in section D3 of part 1.

This PP defines:

- assumptions about the security aspects of the environment in which the TOE will be used;
- threats that are to be addressed by the TOE;
- security objectives of the TOE and its environment
- functional and assurance requirements to meet those security objectives; and
- rationale demonstrating how the requirements meet the security objectives.

1.3 TOE Environment Defining Factors

In trying to specify the environments in which TOEs with various levels of robustness are appropriate, it is useful to first discuss the two defining factors that characterize that environment: **value of the resources** and **authorization of the entities** to those resources.

In general terms, the environment for a TOE can be characterized by the authorization (or lack of authorization) the least trustworthy entity has with respect to the highest value of TOE resources (i.e. the TOE itself and all of the data processed by the TOE).

Note that there are an infinite number of combinations of entity authorization and value of resources; this conceptually "makes sense" because there are an infinite number of potential environments, depending on how the resources are valued by the organization, and the variety of authorizations the organization defines for the associated entities. In the next section 1.3.1, these two environmental factors will be related to the robustness required for selection of an appropriate TOE.

1.3.1 Value of Resources

Value of the resources associated with the TOE includes the data being processed or used by the TOE, as well as the TOE itself (for example, a real-time control processor). "Value" is assigned by the using organization. For example, in the DoD low-value data might be equivalent to data marked "FOUO", while high-value data may be those classified Top Secret. In a commercial enterprise, low-value data might be the internal organizational structure as captured in the corporate on-line phone book, while high-value data might be corporate research results for the next generation product. Note that when considering the value of the data one must also consider the value of data or resources that are accessible through exploitation of the TOE. For example, a firewall may have "low value" data itself, but it might protect an enclave with high value data. If the firewall was being depended upon to protect the high value data, then it must be treated as a high-value-data TOE.

1.3.2 Authorization of Entities

Authorization that entities (users, administrators, other IT systems) have with respect to the TOE (and thus the resources of that TOE, including the TOE itself) is an abstract concept reflecting a combination of the trustworthiness of an entity and the access and privileges granted to that entity with respect to the resources of the TOE. For instance, entities that have total authorization to all data on the TOE are at one end of this spectrum; these entities may have privileges that allow them to read, write, and modify anything on the TOE, including all TSF data. Entities at the other end of the spectrum are those that are authorized to few or no TOE resources. For example, in the case of a router, non-administrative entities may have their packets routed by the TOE, but that is the extent of their authorization to the TOE's resources. In the case of an OS, an entity may not be allowed to log on to the TOE at all (that is, they are not valid users listed in the OS's user database).

It is important to note that authorization **does not** refer to the **access** that the entities actually have to the TOE or its data. For example, suppose the owner of the system determines that no one other than employees was authorized to certain data on a TOE, yet they connect the TOE to the Internet. There are millions of entities that are not **authorized** to the data (because they are not employees), but they actually have connectivity to the TOE through the Internet and thus can attempt to access the TOE and its associated resources.

Entities are characterized according to the value of resources to which they are authorized; the extent of their authorization is implicitly a measure of how trustworthy the entity is with respect to compromise of the data (that is, compromise of any of the applicable security policies; e.g., confidentiality, integrity, availability). In other words, in this model the greater the extent of an entity's authorization, the more trustworthy (with respect to applicable policies) that entity is.

1.3.3 Selection of Appropriate Robustness Levels

Robustness is a characteristic of a TOE defining how well it can protect itself and its resources; a more robust TOE is better able to protect itself. This section relates the defining factors of IT environments, authorization, and value of resources to the selection of appropriate robustness levels.

When assessing any environment with respect to Information Assurance the critical point to consider is the likelihood of an attempted security policy compromise, which was characterized in the previous section in terms of entity authorization and resource value. As previously mentioned, robustness is a characteristic of a TOE that reflects the extent to which a TOE can protect itself and its resources. It follows that as the likelihood of an attempted resource compromise increases, the robustness of an appropriate TOE should also increase.

It is critical to note that several combinations of the environmental factors will result in environments in which the likelihood of an attempted security policy compromise is similar. Consider the following two cases:

The first case is a TOE that processes only low-value data. Although the organization has stated that only its employees are authorized to log on to the system and access the data, the system is connected to the Internet to allow authorized employees to access the system from home. In this case, the least trusted entities would be unauthorized entities (e.g. non-employees) exposed to the TOE because of the Internet connectivity. However, since only low-value data are being processed, the likelihood that unauthorized entities would find it worth their while to attempt to compromise the data on the system is low and selection of a basic robustness TOE would be appropriate.

The second case is a TOE that processes high-value (e.g., classified) information. The organization requires that the TOE be stand-alone, and that every user with physical and logical access to the TOE undergo an investigation so that they are authorized to the highest value data on the TOE. Because of the extensive checks done during this investigation, the organization is assured that only highly trusted users are authorized to use the TOE. In this case, even though high value information is being processed, it is unlikely that a compromise of that data will be attempted because of the authorization and trustworthiness of the users and once again, selection of a basic robustness TOE would be appropriate.

The preceding examples demonstrated that it is possible for radically different combinations of entity authorization/resource values to result in a similar likelihood of an attempted compromise. As mentioned earlier, the robustness of a system is an indication of the protection being provided to counter compromise attempts. Therefore, a basic robustness system should be sufficient to counter compromise attempts where the likelihood of an attempted compromise is low. The following chart depicts the “universe” of environments characterized by the two factors discussed in the previous section: on one axis is the authorization defined for the least trustworthy entity, and on the other axis is the highest value of resources associated with the TOE.

As depicted in the following figure, the robustness of the TOEs required in each environment steadily increases as one goes from the upper left of the chart to the lower right; this corresponds to the need to counter increasingly likely attack attempts by the least trustworthy entities in the environment. Note that the shading of the chart is intended to reflects the notion that different environments engender similar levels of “likelihood of attempted compromise”, signified by a similar color. Further, the delineations between such environments are not stark, but rather are finely grained and gradual.

While it would be possible to create many different "levels of robustness" at small intervals along the “Increasing Robustness Requirements” line to counter the increasing likelihood of attempted compromise due to those attacks, it would not be practical nor particularly useful. Instead, in order to implement the robustness strategy where there are only three robustness levels: Basic, Medium, and High, the graph is divided into three sections, with each section corresponding to set of environments where the likelihood of attempted compromise is roughly similar. This is graphically depicted in the following chart.

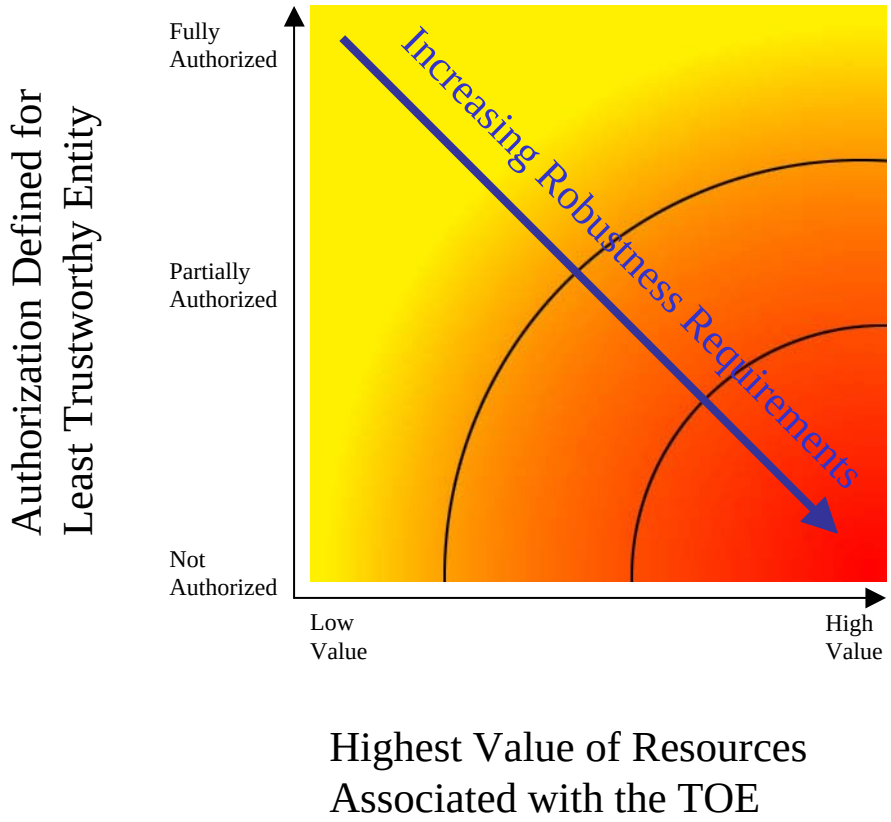

Figure 1: Value of TOE Resources vs. Trust

In this second representation of environments and the robustness plane below, the "dots" represent given instantiations of environments; like-colored dots define environments with a similar likelihood of attempted compromise. Correspondingly, a TOE with a given robustness should provide sufficient protection for environments characterized by like-colored dots. In choosing the appropriateness of a given robustness level TOE PP for an environment, then, the user must first consider the lowest authorization for an entity as well as the highest value of the resources in that environment. This should result in a "point" in the chart above, corresponding to the likelihood that that entity will attempt to compromise the most valuable resource in the environment. The appropriate robustness level for the specified TOE to counter this likelihood can then be chosen.

The difficult part of this activity is differentiating the authorization of various entities, as well as determining the relative values of resources; (e.g., what constitutes "low value" data vs. "medium value" data). Because every organization will be different, a rigorous definition is not possible. In section 3 of this PP, the targeted threat level for a basic robustness TOE is characterized. This information is provided to help organizations using this PP insure that the functional requirements specified by this basic robustness PP are appropriate for their intended application of a compliant TOE.

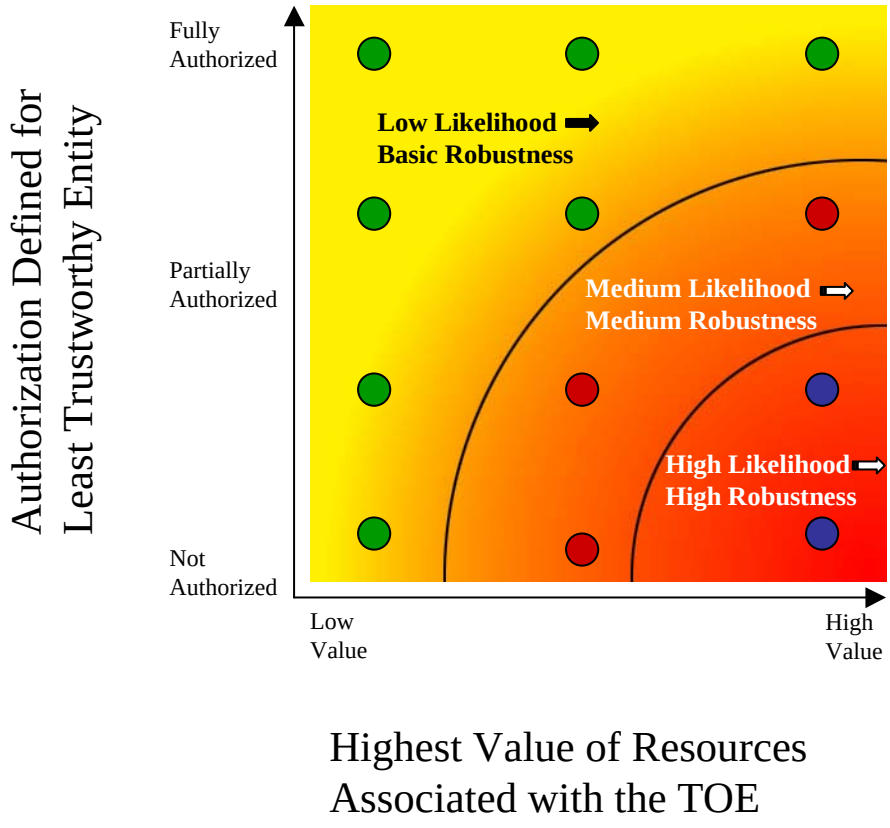

Figure 2: Value of TOE Resources vs. Robustness

1.4 Related Protection Profiles

This Profile is part of planned set of Protection Profiles for wireless communications. This PP describes the security requirements for devices used to facilitate communications between a wireless client device and, either a wired network or another wireless device in a basic robustness environment. Its counterpart, the *US Government Wireless Local Area Network (WLAN) Client Protection Profile For Basic Robustness Environments*, describes the security requirements for WLAN client devices in a basic robustness environment.

2. TOE Description

The Target of Evaluation (TOE) is a WLAN access system. For the purposes of this protection profile, a wireless LAN access system can be defined as one or more components that provide secure wireless access to a wired or wireless network. This PP will generally refer to a wired to wireless configuration. However the reader should keep in mind that it does not preclude any

other wireless configuration that may exist and meet the requirements identified in this PP. This PP does not dictate any particular configuration. Instead the PP addresses the security requirements for the system that allows access to the wired (or wireless) network while performing management functions within the system. The security requirements of the TOE are identification and authentication (I&A) for administrators (I&A provided by the IT Environment for wireless clients), audit generation, encryption, information flow control, and administration.

A WLAN is an extension of, or possibly a replacement for, a traditional wired network. It allows mobile, wireless clients to be roaming hosts on the network, and to connect to the network using access points. The traditional wireless LAN is set up as in Figure 3. In this configuration, an Access Point (AP) controls the establishment of the link between wireless clients and the wired LAN. As such, it is not intended to provide any direct network services to the users that connect through the AP. It is also important to note that the AP relies on the environment in which it resides to assist with WLAN management and providing secure access to the network. It may be the case that some WLAN access devices will not solely meet the security requirements stated in this PP. Therefore, it may be necessary for a TOE to include a layered solution, which combines additional components with a traditional WLAN access point in order to meet security requirements listed in this PP. These layered solutions (e.g., VPN, Wireless Gateway, Wireless Security Switch) are all valid as deployment architectures for a wireless access system compliant with this PP.

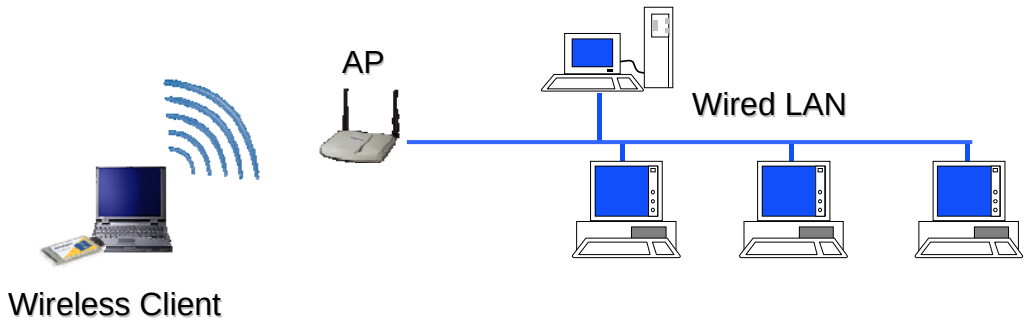

Figure 3: Traditional Wireless LAN

2.1 TOE Functionality

WLAN access systems must include the necessary management and security functions to operate in accordance with this PP. The TOE includes management capabilities, auditing functions, and authentication features. In protecting the network, the system shall address security at either Layer 2 (Link Layer) or Layer 3 (Network Layer) or both.

The functionality of a wireless access system *may* be implemented by more than one physical component. Figure 4 shows an example of a WLAN using an access system architecture. As stated in Section 2.0, AP's provide network connectivity to mobile clients and do not provide

direct network services to the user. Therefore, an AP may be one of several components that comprise the access system. It should also be noted that an AP, which is not represented in Figure 4, could be included between the wireless client and the access system to provide the network connectivity to the user. The PP specifies the functional and security requirements for a system as a whole and does not attempt to separate requirements by component. In all cases, wireless traffic must be able to pass to the wired network via the wireless access system providing the necessary security. This PP will address environmental requirements on both the wired network and the wireless access system.

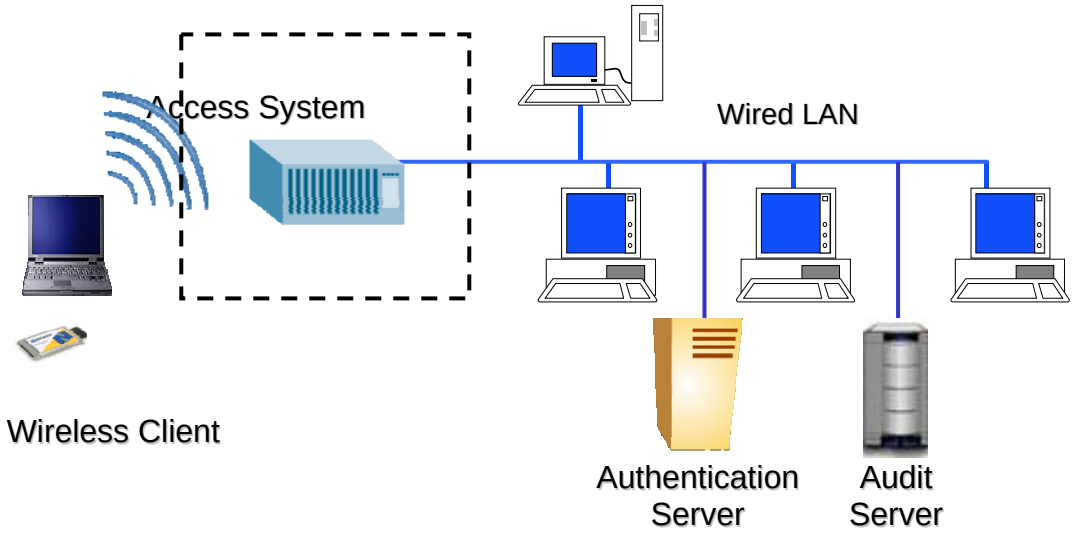

Figure 4: Example WLAN Access System with Authentication and Audit Servers

2.2 Identification and Authentication

The TOE is expected to provide multiple Identification and Authentication (I&A) mechanisms for access to services residing on the TOE or for access to networks/services mediated by the TOE. The type of authentication mechanism required depends on the origin of the authentication request (i.e., remote user from the wireless environment, remote administrative user from the wired environment, or local administrative user from a TOE console). The TOE requires that administrators be properly identified and authenticated prior to performing any administrative tasks for the TOE. The authentication of users will be based on a set of authentication credentials assigned to each user. A Unix style user ID and password is an example of authentication credentials required to access the TOE. A Unix style user ID and password is sufficient for administrative access to the TOE from the wired network or for administrator access to the TOE via the console. The TOE also requires that the individual users be authenticated in order to obtain access to network(s) mediated by the TOE.[1]

An authentication server (provided by the IT environment) may be used to perform the authentication of the individual users, as well as the remote administrator.

[1] This mediation is not to be confused with the type of mediation performed by a firewall. In the case of this TOE, access mediation simply consists of only allowing authenticated users access to the network(s) connected to the TOE.

2.3 Roles

"Administrator" refers to the role assigned to the individuals responsible for the installation, configuration, and maintenance of the TOE. These are the only users that have access to the TOE, whereas authenticated users simply send network packets to the TOE to be forwarded to the appropriate TOE interface.

2.4 Information Flow Control

The WLAN access system is an infrastructure device used to mediate access between wireless devices, and a wireless LAN and/or a wired LAN. As such it must provide the capability to limit access to those networks that it protects through its interfaces. In addition, it must ensure that information transmitted via those interfaces is protected by encryption if specified by the administrative policy.

2.5 Encryption

This TOE includes requirements for cryptographic modules. Those modules must comply with Federal Information Processing Standard Publication (FIPS PUB) 140-1/2 or later, which defines security requirements for cryptographic modules. A cryptographic module is that part of a system or application that provides cryptographic services, such as encryption, authentication, or electronic signature generation and verification. Products and systems compliant with this PP are expected to utilize cryptographic modules compliant with this FIPS PUB. FIPS PUB 140-2 has superseded FIPS PUB 140-1 however the DoD recognizes those products that currently hold the FIPS PUB 140-1 certification. For the purposes of this PP, FIPS PUB 140-1 will be accepted only if it was certified prior to the date of adoption of FIPS PUB 140-2. This PP requires the use the Advanced Encryption Standard (AES) as the encryption algorithm.

2.6 Audit

The TOE must generate audit records, and provide an administrative interface to allow the administrator to select the events that are audited. Section 5 of this document, lists the minimum set of auditable events that require the TOE generate an audit record. This section also specifies a minimum list of attributes that must be included in each audit record. The Security Target (ST) author may include additional auditable events and audit record attributes. If the ST author includes any additional functional requirements not specified by this PP, they must consider any security relevant events associated with those requirements and include them in the TOE's list of auditable events and records.

The TOE is not required to store audit events, an external device (e.g., a syslog server) may be used to store events generated by the TOE and provide an interface for post-audit management and processing.

3. TOE Security Environment

The TOE specified within this PP is intended for use in basic robustness environments. Basic robustness TOEs fall in the upper left area of the previously discussed robustness figures. A Basic Robustness TOE is considered sufficient for low threat environments or where compromise of protected information will not have a significant impact on mission objectives. This implies that the motivation of the threat agents will be low in environments that are suitable for TOEs of this robustness. In general, basic robustness results in "good commercial practices" that counter threats based in casual and accidental disclosure or compromise of data protected by the TOE.

Threat agent motivation can be considered in a variety of ways. One possibility is that the value of the data process or protected by the TOE will generally be seen as of little value to the adversary (i.e., compromise will have little or no impact on mission objectives). Another possibility, (where higher value data is processed or protected by the TOE) is that procuring organizations will provide other controls or safeguards (i.e., controls that the TOE itself does not enforce) in the fielded system in order to increase the threat agent motivation level for compromise beyond a level of what is considered reasonable or expected to be applied.

In a basic robustness environment, users are trusted to neither attempt malicious attacks nor by-pass access control measures. Users are also trusted to correctly apply the organization's security policies. The TOE is not expected to protect against sophisticated, technical attack.

The remainder of this chapter (Chapter 3) describes the assumptions, threats, and policies that are relevant to both the WLAN TOE and the WLAN TOE environment. The first section describes the Secure Usage Assumptions—these are the assumptions that support the secure use of the WLAN. Threats are countered by the security objectives. Policies support the security objectives and are used by security objectives to counter threats.

3.1 Secure Usage Assumptions

Assumptions are limiting conditions that are accepted before developing policy or considering threats. Table 1: TOE Assumptions identifies the conditions that are assumed to exist in the operational environment. In addition to the standard list of assumptions for Basic Robustness Protection Profiles, there are two assumptions that deal with the special roles of remote administration/management and audit servers in this PP.

Table 1: TOE Assumptions

Name	Assumption
A.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance.
A.NO_GENERAL_PURPOSE	There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the

	environment.
A.TOE_NO_BYPASS	Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.

3.2 Threats to Security

The threats listed in Table 2: Threats are general threats. Threats are actions that may have an adverse affect on the Basic Robustness WLAN or mission. Exposure of wireless communications in the RF transmission environment introduces unique threats for the WLAN. The WLAN interconnected to a wired network could effectively create a hole in the wired infrastructure boundary because it exposes information to the RF medium where signals can be more readily detected and intercepted. With WLANs, an adversary no longer requires physical access to the network to exploit a wireless system. For basic robustness, the threats identified do not include those that would be considered a sophisticated attack (e.g., intentional jamming, traffic analysis).

In addition to helping define the robustness appropriate for a given environment, the threat agent is a key component of the formal threat statements in the PP. Threat agents are typically characterized by a number of factors such as *expertise, available resources,* and *motivation.* Because each robustness level is associated with a variety of environments, there are corresponding varieties of specific threat agents (that is, the threat agents will have different combinations of motivation, expertise, and available resources) that are valid for a given level of robustness. The following discussion explores the impact of each of the threat agent factors on the ability of the TOE to protect itself (that is, the robustness required of the TOE).

The *motivation* of the threat agent seems to be the primary factor of the three characteristics of threat agents outlined above. Given the same expertise and set of resources, an attacker with low motivation may not be as likely to attempt to compromise the TOE. For example, an entity with no authorization to low value data none-the-less has low motivation to compromise the data; thus a basic robustness TOE should offer sufficient protection. Likewise, the fully authorized user with access to highly valued data similarly has low motivation to attempt to compromise the data, thus again a basic robustness TOE should be sufficient.

Unlike the motivation factor, however, the same can't be said for *expertise*. A threat agent with low motivation and low expertise is just as unlikely to attempt to compromise a TOE as an attacker with low motivation and high expertise; this is because the attacker with high expertise does not have the motivation to compromise the TOE even though they may have the expertise to do so. The same argument can be made for *resources* as well.

Therefore, when assessing the robustness needed for a TOE, the motivation of threat agents should be considered a “high water mark”. *That is, the robustness of the TOE should increase as the motivation of the threat agents increases.*

Having said that, the relationship between expertise and resources is somewhat more complicated. In general, if resources include factors other than just raw processing power

(money, for example), then expertise should be considered to be at the same "level" (low, medium, high, for example) as the resources because money can be used to purchase expertise. Expertise in some ways is different, because expertise in and of itself does not automatically procure resources. However, it may be plausible that someone with high expertise can procure the requisite amount of resources by virtue of that expertise (for example, hacking into a bank to obtain money in order to obtain other resources).

It may not make sense to distinguish between these two factors; in general, it appears that the only effect these may have is to lower the robustness requirements. For instance, suppose an organization determines that, because of the value of the resources processed by the TOE and the trustworthiness of the entities that can access the TOE, the motivation of those entities would be "medium". This normally indicates that a medium robustness TOE would be required because the likelihood that those entities would attempt to compromise the TOE to get at those resources is in the "medium" range. However, now suppose the organization determines that the entities (threat agents) that are the least trustworthy have no resources and are unsophisticated. In this case, even though those threat agents have medium motivation, the likelihood that they would be able to mount a successful attack on the TOE would be low, and so a basic robustness TOE may be sufficient to counter that threat.

It should be clear from this discussion that there is no "cookbook" or mathematical answer to the question of how to specify exactly the level of motivation, the amount of resources, and the degree of expertise for a threat agent so that the robustness level of TOEs facing those threat agents can be rigorously determined. However, an organization can look at combinations of these factors and obtain a good understanding of the likelihood of a successful attack being attempted against the TOE. Each organization wishing to procure a TOE must look at the threat factors applicable to their environment; discuss the issues raised in the previous paragraph; consult with appropriate accreditation authorities for input; and document their decision regarding likely threat agents in their environment.

The important general points we can make are:

- The motivation for the threat agent defines the upper bound with respect to the level of robustness required for the TOE
- A threat agent's expertise and/or resources that is "lower" than the threat agent's motivation (e.g., a threat agent with high motivation but little expertise and few resources) may lessen the robustness requirements for the TOE (see next point, however).
- The availability of attacks associated with high expertise and/or high availability of resources (for example, via the Internet or "hacker chat rooms") introduces a problem when trying to define the expertise of, or resources available to, a threat agent.

Table 2: Threats

Threat Name	Threat Definition
T.ACCIDENTAL_ADMIN_ ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.ACCIDENTAL_ CRYPTO_ COMPROMISE	A user or process may cause key, data or executable code associated with the cryptographic

Threat Name	Threat Definition
	functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.POOR_DESIGN	Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_IMPLEMENTATION	Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_TEST	The developer or tester performs insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may occur, resulting in incorrect TOE behavior being undiscovered leading to flaws that may be exploited by a mischievous user or program.
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.UNATTENDED_ SESSION	A user may gain unauthorized access to an unattended session.
T.UNAUTHORIZED_ ACCESS	A user may gain access to services (either on the TOE or by sending data through the TOE) for which they are not authorized according to the TOE security policy.
T.UNAUTH_ADMIN_ACCESS	An unauthorized user or process may gain access to an administrative account.

Table 3: Basic Robustness Threats NOT Applicable to the TOE

Threat Name	Threat Definition	Rationale for NOT Including this Threat
T.ACCIDENTAL_AUDIT _COMPROMISE	A user or process may view audit records, cause	The storage/retrieval and review of audit

Threat Name	Threat Definition	Rationale for NOT Including this Threat
	audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	records is provided by the IT environment. Hence, although this threat must be addressed within the IT environment, the functional requirements specified in this PP do not provide the functionality required to protect the audit records in the external environment. The fundamental threat must be met by protecting communications path that the audit records travel for storage and review.
T.UNIDENTIFIED_ ACTIONS	The administrator may not have the ability to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.	This threat is intended to require the FAU_SAA and FAU_ARP requirements and those requirements were deemed inappropriate for the basic robustness wireless access system TOE and how it is envisioned it will be administered.

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. Table 4: Organizational Security Policies identifies the organizational security policies applicable to the WLAN.

Table 4: Organizational Security Policies

Policy Name	Policy Definition
P.ACCESS_BANNER	The TOE shall display an initial banner for administrator logins describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHIC	The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.
P.CRYPTOGRAPHY_VALIDATED	Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).
P.ENCRYPTED_CHANNEL	The TOE shall provide the capability to

	encrypt/decrypt wireless network traffic between the TOE and those wireless clients that are authorized to join the network.
P.NO_AD_HOC_NETWORKS	In accordance with the DOD Wireless Policy, there will be no ad hoc 802.11 or 802.15 networks allowed.

4. Security Objectives for the TOE

Table 5: Security Objectives for the TOE 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 table also shows the corresponding threats and policies that are addressed by the objectives. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Table 5: Security Objectives for the TOE

Name	TOE Security Objective
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events associated with users.
O.CORRECT_TSF_OPERATION	The TOE will provide the capability to verify the correct operation of the TSF.
O.CRYPTOGRAPHY	The TOE shall provide cryptographic functions to maintain the confidentiality and allow for detection of modification of user data that is transmitted between physically separated portions of the TOE, or outside of the TOE.
O.CRYPTOGRAPHY_VALIDATED	The TOE will use NIST FIPS 140-1/2 validated cryptomodules for cryptographic services implementing NIST-approved security functions and random number generation services used by cryptographic functions.
O.DISPLAY_BANNER	The TOE will display an advisory warning prior to establishing an administrator session regarding use of the TOE prior to permitting the use of any TOE services that requires authentication.
O.MANAGE	The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.

Name	TOE Security Objective
O.MEDIATE	The TOE must mediate the flow of information to and from wireless clients communicating via the TOE in accordance with its security policy.
O.RESIDUAL_ INFORMATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.
O.SELF_PROTECTION	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
O.TIME_STAMPS	The TOE shall obtain reliable time stamps.
O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.
O.ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure management.
O.CONFIGURATION_ IDENTIFICATION	The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly.
O.DOCUMENTED_ DESIGN	The design of the TOE is adequately and accurately documented.
O.PARTIAL_ FUNCTIONAL_TESTING	The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.
O.VULNERABILITY_ ANALYSIS	The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.

4.1 Security Objectives for the Environment

The assumptions identified in Section 3.1 are incorporated as security objectives for the environment and listed below. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures.

Table 6: Security Objectives for the IT and Non IT Environment identifies the security objectives for the TOE IT environment.

Table 6: Security Objectives for the IT and Non IT Environment

Name	TOE Security Objective
OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information and the authentication credentials.
OE.AUDIT_REVIEW	The IT Environment will provide the capability to selectively view audit information.
OE.MANAGE	The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
OE.NO_EVIL	Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
OE.PHYSICAL	The environment provides physical security commensurate with the value of the TOE and the data it contains.
OE.PROTECT_MGMT_COMMS	The environment shall protect the transport of audit records to the audit server, remote network management, and authentication server communications with the TOE and time service in a manner that is commensurate with the risks posed to the network.
OE.RESIDUAL_INFORMATION	The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.
OE.SELF_PROTECTION	The environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
OE.TIME_STAMPS	The TOE IT environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.

Name	TOE Security Objective
OE.TOE_ACCESS	The environment will provide mechanisms that support the TOE in providing a user's logical access to the TOE.
OE.TOE_NO_BYPASS	Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.

5. IT Security Requirements

This section provides functional and assurance requirements that must be satisfied by a PP-compliant TOE. These requirements consist of functional components from Part 2 of the Common Criteria (CC) and assurance components from Part 3 of the CC.

5.1 TOE Security Functional Requirements

The SFRs for the TOE consist of the following components from Part 2 of the CC, summarized in Table 8: TOE Security Functional Requirements. All dependencies among the SFRs are satisfied by the inclusion of the relevant requirement within the TOE security requirements.

Table 8: TOE Security Functional Requirements

Functional Component		Dependencies
FAU_GEN.1(1)	Audit data generation	FPT_STM.1
FAU_GEN.2(1)	User identity association	FAU_GEN.1 FIA_UID.1
FAU_SEL.1(1)	Selective audit	FAU_GEN.1; FMT_MTD.1(1)
FCS_BCM_(EXT).1	Extended: Baseline Cryptographic Module	None
FCS_CKM.1(1)	Cryptographic Symmetric key generation	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4 FMT_MSA.2
FCS_CKM.1(2)	Cryptographic Asymmetric key generation	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4 FMT_MSA.2
FCS_CKM.2	Cryptographic key distribution	[FDP_ITC.1 or FCS_CKM.1] FMT_MSA.2
FCS_CKM_(EXT).2	Cryptographic key handling and storage	[FDP_ITC.1 or FCS_CKM.1] FMT_MSA.2
FCS_CKM.4	Cryptographic key destruction	[FDP_ITC.1 or FCS_CKM.1] FMT_MSA.2
FCS_COP.1(1)	Cryptographic Operation (Data encryption/decryption)	[FDP_ITC.1 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2
FCS_COP.1(2)	Cryptographic Operation (Digital Signature)	[FDP_ITC.1 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2

Functional Component		Dependencies
FCS_COP.1(3)	Cryptographic Operation (Hashing)	[FDP_ITC.1 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2
FCS_COP.1(4)	Cryptographic Operation (Key agreement)	[FDP_ITC.1 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2
FCS_COP_(EXT).1	Extended: Random Number Generation	[FDP_ITC.1or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2
FDP_PUD_(EXT).1	Protection of User Data	None
FDP_RIP.1(1)	Subset residual information protection	None
FIA_AFL.1(1)	Administrator Authentication failure handling	FIA_UAU.1
FIA_ATD.1(1)	Administrator attribute definition	None
FIA_ATD.1(2)	User attribute definition	None
FIA_UAU.1	Timing of local authentication	FIA_UID.1
FIA_UAU_(EXT).5(1)	Multiple authentication mechanisms	None
FIA_UID.2	User identification before any action	None
FIA_USB.1	User-subject binding	FIA_ATD.1
FMT_MOF.1(1)	Management of security functions behavior (Cryptographic Function)	FMT_SMF.1(1) FMT_SMR.1
FMT_MOF.1(2)	Management of security functions behavior (Audit Record Generation)	FMT_SMF.1(2) FMT_SMR.1
FMT_MOF.1(3)	Management of security functions behavior (Authentication)	FMT_SMF.1 FMT_SMR.1
FMT_MSA.2	Secure security attributes	ADV_SPM.1 [FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1
FMT_MTD.1(1)	Management of Audit data	FMT_SMR.1
FMT_MTD.1(2)	Management of Authentication data (Administrator)	FMT_SMR.1
FMT_MTD.1(3)	Management of Authentication data (User)	FMT_SMR.1
FMT_SMF.1(1)	Specification of Management Functions (Cryptographic Functions)	None
FMT_SMF.1(2)	Specification of Management Functions (TOE Audit Record Generation)	None
FMT_SMF.1(3)	Specification of Management Functions	None

Functional Component		Dependencies
	(Cryptographic Key Data)	
FMT_SMR.1(1)	Security roles	FIA_UID.1
FPT_STM_(EXT).1	Reliable time stamps	None
FPT_TST_(EXT).1	TSF Testing	None
FPT_TST.1	TSF Testing of Cryptographic Modules	None
FPT_TST.2	TSF Testing of Cryptographic key generation	None
FTA_SSL.3	TSF-initiated termination	None
FTA_TAB.1	Default TOE access banners	None
FTP_ITC_(EXT).1(1)	Inter-TSF trusted channel	None
FTP_TRP.1	Trusted Path	None

5.1.1 FAU_GEN.1(1) Audit data generation

FAU_GEN.1.1(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 *minimum* level of audit; and

c) [ST AUTHOR assignment: other specifically defined auditable events].

Table 9: TOE Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None	None
FAU_GEN.2	None	None
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	The identity of the Administrator performing the function
FCS_CKM.1(1)	Generation of a key	The identity of the Administrator performing the function
FCS_CKM.1(1)	Generation of a key	The identity of the Administrator performing the function

Requirement	Auditable Events	Additional Audit Record Contents
FCS_CKM_(EXT).2	Error(s) detected during cryptographic key transfer	If available - the authentication credentials of subjects with which the invalid key is shared.
FCS_CKM.4	Destruction of a cryptographic key	If available - The identity of the Administrator performing the function
FCS_COP1(1),(2),(3),(4)	None	None
FCS_COP_(EXT).1	None	None
FDP_PUD.1_(EXT)	Enabling or disabling TOE encryption of wireless traffic	The identity of the Administrator performing the function.
FDP_RIP.1	None	None
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal	None
FIA_ATD.1	None	None
FIA_UAU.1	Use of the authentication mechanism (success or failure)	User identity - the TOE **SHALL NOT** record invalid passwords the audit log.
FIA_UAU_(EXT).5	Failure to receive a response from the remote authentication server	Identification of the Authentication server that did not reply
FIA_UID.2	None	None
FIA_USB.1	Unsuccessful binding of user security attributes to a subject	None
FMT_MOF.1(1)	Changing the TOE encryption algorithm including the selection not to encrypt communications	Encryption algorithm selected (or none)
FMT_MOF.1(2)	Start or Stop of audit record generation	None
FMT_MOF.1(3)	Changes to the TOE remote authentication settings; Changes to the threshold of failed authentication attempts; Changes to the session lock timeframe	The identity of the Administrator performing the function.
FMT_MSA.2	All offered and rejected values for security attributes	None
FMT_MTD.1(1)	Changes to the set of rules used to pre-select audit events.	None
FMT_MTD.1(2) FMT_MTD.1.(3)	Changing the TOE authentication credentials	None – the TOE **SHALL NOT** record authentication credentials in the audit log.
FMT_REV.1	Unsuccessful revocation of security attributes.	None

Requirement	Auditable Events	Additional Audit Record Contents
FMT_SMR.1	Modifications to the group of users that are part of a role	None
FPT_STM_(EXT).1	Changes to the time	None
FPT_TST_(EXT).1	Execution of the self test	Success or Failure of test
FPT_TST.1	Execution of the self test	Success or Failure of test
FPT_TST.2	Execution of the self test	Success or Failure of test
FTA_SSL.3	TSF Initiated Termination	Termination of an interactive session by the session locking mechanism.
FTP_ITC_(EXT).1	Initiation/Closure of a trusted channel;	Identification of the remote entity with which the channel was attempted/created; Success of failure of the event
FTP_TRP.1	Initiation of a trusted channel	Identification of the remote entity with which the channel was attempted/created; Success of failure of the event

FAU_GEN.1.2(1) 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 **(if applicable)**, 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 Table 9].

Application Note: Event type is defined as the BSD syslog severity level indicator, in the Terminology section of this PP.

Application Note: In column 3 of Table 9, "if available/applicable" is used to designate data that should be included in the audit record if it "makes sense" in the context of the event that generates the record. If no other information is required (other than that listed in FAU_GEN.1.2item a) for a particular audit event type, then "none" is acceptable and should be inserted at the proper location in the table.

5.1.2 FAU_GEN.2 User identity 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.

5.1.3 FAU_SEL.1 Selective audit

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

a) *user identity, event type;*

b) [device interface, wireless client identity].

Application Note: Event type is defined as the BSD syslog severity level indicator, in the Terminology section of this PP.

Application Note: The device interface is the physical interface upon which user (or administrative) data is received/sent (e.g. WLAN interface, wired LAN interface, serial port, administrative LAN interface, etc.).

Cryptographic Support (FCS)

This section specifies the cryptographic support required in the TOE. Evolving public standards on cryptographic functions and related areas have required an interim approach to writing cryptographic requirements. These cryptographic requirements are expected to be achievable in commercial products in the near term, and gradually mature over time. Today these requirements represent a step in the direction of helping to improve the security in COTS products. Over time, the Protection Profile will be updated as the underlying public standards and the body of related special publications mature.

5.1.4 Extended: Baseline Cryptographic Module (FCS_BCM_(EXT))

The cryptographic requirements are structured to accommodate use of the FIPS 140-2 standard and NIST's Cryptomodule Validation Program (CMVP) in meeting the requirements. Note that *FIPS-approved* cryptographic functions are required to be implemented in a *FIPS-validated module running in FIPS-approved mode*. FCS_BCM reflects this requirement, and it specifies the required FIPS validation levels for the security functions. Note also that some of the requirements of this Protection Profile go beyond what is required for FIPS 140-2 validation.

Application Note: A FIPS-approved cryptographic function is 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.

5.1.4.1 Extended: Baseline Cryptographic Module (FCS_BCM_(EXT).1)

FCS_BCM_(EXT).1.1 All FIPS-approved cryptographic functions implemented by the TOE shall be implemented in a cryptomodule that is FIPS 140-2 validated, and perform the specified cryptographic functions in a FIPS-approved mode of operation. The FIPS 140-2 validation shall include an algorithm validation certificate for all FIPS-approved cryptographic functions implemented by the TOE.

Application Note: This Protection Profile shall use the term "FIPS 140-2" for simplicity. FIPS PUB 140-2 is currently undergoing a regular five year review; in the near future, FIPS PUB

140-3 will supersede it. Security Targets written to comply with this Protection Profile may replace it with the successor standard that is in force at the time of evaluation.

Application Note: This requirement does not preclude additional cryptographic algorithms from being implemented in the cryptomodule, and/or used by the TOE for purposes OTHER than those explicitly stated in this Protection Profile.

FCS_BCM_(EXT).1.2 All cryptographic modules implemented in the TOE ***[selection:***

Entirely in hardware shall have a minimum overall rating of FIPS PUB 140-2, Level 3,

Entirely in software shall have a minimum overall rating of FIPS PUB 140-2, Level 1 and also meet FIPS PUB 140-2, Level 3 for the following: Cryptographic Module Ports and Interfaces; Roles, Services and Authentication; Cryptographic Key Management; and Design Assurance.

As a combination of hardware and software shall have a minimum overall rating of FIPS PUB 140-2, Level 1 and also meet FIPS PUB 140-2, Level 3 for the following: Cryptographic Module Ports and Interfaces; Roles, Services and Authentication; Cryptographic Key Management; and Design Assurance.]

Application Note: "Combination of hardware and software" means that some part of the cryptographic functionality will be implemented as a software component of the TSF. The combination of a cryptographic hardware module and a software device driver whose sole purpose is to communicate with the hardware module is considered a hardware module rather than "combination of hardware and software".

Application Note: Note that the requirements for selections (2) and (3) are the same. The ST author should make it clear how the cryptomodule is implemented.

5.1.5 Cryptographic Key Management (FCS_CKM)

NIST Special Publication 800-57, "Recommendation for Key Management" contains additional protection mechanisms that vendors are encouraged to implement. It should also be used as guidance for the cryptographic key management requirements.

5.1.5.1 Cryptographic Key Generation (for symmetric keys) (FCS_CKM.1(1))

FCS_CKM.1.1(1) **Refinement:** The TSF shall generate symmetric cryptographic keys **using a FIPS-Approved Random Number Generator as specified in FCS_COP_(EXT).1, and provide integrity protection to generated symmetric keys in accordance with NIST SP 800-57 "Recommendation for Key Management" Section 6.1.**

Application Note: NIST SP 800-57 "Recommendation for Key Management" Section 6.1 states: "Integrity protection can be provided by cryptographic integrity mechanisms (e.g. cryptographic checksums, cryptographic hashes, MACs, and signatures), non-cryptographic integrity mechanisms (e.g. CRCs, parity, etc.) […], or physical protection mechanisms."

Guidance for the selection of appropriate integrity mechanisms is given in Sections 6.2.1.2 and 6.2.2.2 of NIST SP 800-57 "Recommendation for Key Management".

Application Note: Note that there is a separate requirement for Cryptographic Key Agreement (FCS_COP.1(4)).

5.1.5.2 Cryptographic Key Generation (for asymmetric keys) (FCS_CKM.1(2))

FCS_CKM.1.1(2) Refinement: The TSF shall generate **asymmetric** cryptographic keys in accordance **with the mathematical specifications of the FIPS-approved or NIST-recommended standard [*assignment: specify standard(s)],* using a domain parameter generator and *[selection:***

a FIPS-Approved Random Number Generator as specified in FCS_COP_(EXT).1, and/or

a prime number generator as specified in ANSI X9.80 "Prime Number Generation, Primality Testing, and Primality Certificates" using random integers with deterministic tests, or constructive generation methods]

in a cryptographic key generation scheme that meets the following:

- **The TSF shall provide integrity protection and assurance of domain parameter and public key validity to generated asymmetric keys in accordance with NIST SP 800-57 "Recommendation for Key Management" Section 6.1.**
- **Generated key strength shall be equivalent to, or greater than, a symmetric key strength of 128 bits using conservative estimates.**

Application Note: NIST SP 800-57 "Recommendation for Key Management" Section 6.1 states: "Integrity protection can be provided by cryptographic integrity mechanisms (e.g. cryptographic checksums, cryptographic hashes, MACs, and signatures), non-cryptographic integrity mechanisms (e.g. CRCs, parity, etc.) […], or physical protection mechanisms." Guidance for the selection of appropriate integrity mechanisms is given in Sections 6.2.1.2 and 6.2.2.2 of NIST SP 800-57 "Recommendation for Key Management".

Application Note: Assurance of domain parameter and public key validity provides confidence that the parameters and keys are arithmetically correct. Guidance for the selection of appropriate validation mechanisms is given in NIST SP 800-57 "Recommendation for Key Management," NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography," and FIPS PUB 186-3, "Digital Signature Standard."

Application Note: See NIST Special Publication 800-57, "Recommendation for Key Management" for information about equivalent key strengths.

5.1.5.3 Cryptographic Key Distribution (FCS_CKM.2)

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method ***[selection:***

Manual (Physical) Method, and/or

Automated (Electronic) Method]

that meets the following:

- **NIST Special Publication 800-57, "Recommendation for Key Management" Section 8.1.5**
- **NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"**

Application Note: NIST Special Publication 800-56A "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" is only applicable when public key schemes are used in key transport methods.

Application Note: DoD applications may have additional key distribution requirements related to the DoD PKI and certificate formats.

5.1.5.4 Extended: Cryptographic Key Handling and Storage (FCS_CKM_(EXT).2)

FCS_CKM_(EXT).2.1 The TSF shall perform a key error detection check on each transfer of key (internal, intermediate transfers).

Application Note: A parity check is an example of a key error detection check.

FCS_CKM_(EXT).2.2 The TSF shall store persistent secret and private keys when not in use in encrypted form or using split knowledge procedures.

Application Note: Note that this requirement is stronger than the FIPS 140-2 key storage requirements, which state: "Cryptographic keys stored within a cryptographic module shall be stored in plaintext form or encrypted form."

Application Note: A persistent key, such as a file encryption key, is one that must be available in the system over long periods of time. A non-persistent key, such as a key used to encrypt or decrypt a single message or a session, is one that is ephemeral in the system.

Application Note: "When not in use" is interpreted in the strictest sense so that persistent keys only exist in plaintext form during intervals of operational necessity. For example, a file encryption key exists in plaintext form only during actual encryption and/or decryption processing of a file. Once the file is decrypted or encrypted, the file encryption key should immediately be covered for protection.

Application Note: A "split knowledge procedure" is a process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, which can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key.

FCS_CKM_(EXT)_2.3 The TSF shall destroy non-persistent cryptographic keys after a cryptographic administrator-defined period of time of inactivity.

Application Note: The cryptographic administrator must have the ability to set a threshold of inactivity after which non-persistent keys must be destroyed in accordance with FCS_CKM.4.

FCS_CKM_(EXT).2.4 The TSF shall prevent archiving of expired (private) signature keys.

Application Note: This requirement is orthogonal to typical system back-up procedures. Therefore, it does not address the problem of archiving an active (private) signature key during a system back-up and saving the key beyond its intended life span.

5.1.5.5 Cryptographic Key Destruction (FCS_CKM.4)

Application Note: Note that this requirement is stronger than the FIPS 140-2 key zeroization requirements, which state: "A cryptographic module shall provide methods to zeroize all plaintext secret and private cryptographic keys and CSPs within the module."

FCS_CKM.4.1 **Refinement:** The TSF shall destroy cryptographic keys in accordance with a **cryptographic key zeroization method** that meets the following:

a) Key zeroization requirements of FIPS PUB 140-2, "Security Requirements for Cryptographic Modules"

b) Zeroization of all plaintext cryptographic keys and all other critical cryptographic security parameters shall be immediate and complete.

Application Note: The term "immediate" here is meant to impart some urgency to the destruction: it should happen as soon as practical after the key is no longer required to be in plaintext. It is certainly permissible to complete a critical section of code before destroying the key. However, the destruction shouldn't wait for idle time, and there shouldn't be any non-determined event (such as waiting for user input) which occurs before it is destroyed.

c) The TSF shall zeroize each intermediate storage area for plaintext key/critical cryptographic 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 cryptographic security parameter to another location.

Application Note: Item c) pertains to the elimination of internal, temporary copies of keys/parameters during processing, and not to the locations that are used for the storage of the keys, which are specified in item b). The temporary locations could include memory registers, physical memory locations, and even page files and memory dumps.

d) For non-volatile memories other than EEPROM and Flash, the zeroization shall be executed by overwriting three or more times using a different alternating data pattern each time.

Application Note: Although verification of the zeroization of each intermediate location consisting of non-volatile memories is desired here (by checking for the final known alternating data pattern), it is not required at this time. However, vendors are highly encouraged to incorporate this verification whenever possible into their implementations.

e) For volatile memory and non-volatile EEPROM and Flash memories, the zeroization shall be executed by a single direct overwrite consisting of a pseudo random pattern, followed by a read-verify.

5.1.6 Cryptographic Operation (FCS_COP)

5.1.6.1 Cryptographic Operation (for data encryption/decryption) (FCS_COP.1(1))

FCS_COP.1.1(1) **Refinement:** The cryptomodule shall perform **encryption and decryption using the FIPS-approved security function AES algorithm operating in *[assignment: one or more FIPS-approved modes]* and cryptographic key size of [*selection: one or more of 128 bits, 192 bits, 256 bits*]**.

5.1.6.2 Cryptographic Operation (for cryptographic signature) (FCS_COP.1(2))

FCS_COP.1.1(2) **Refinement:** The TSF shall perform **cryptographic signature services using the FIPS-approved security function *[selection:***

Digital Signature Algorithm (DSA) with a key size (modulus) of [assignment: 2048 bits or greater],

RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of [assignment: 2048 bits or greater], or

Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of [selection: one or more of 256 bits, 384 bits, 521 bits], using only the NIST curve(s) [selection: one or more of P-256, P-384, P-521 as defined in FIPS PUB 186-3, "Digital Signature Standard"]]

that meets NIST Special Publication 800-57, "Recommendation for Key Management."

Application Note: 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 key exchange, elliptic curves will be required after all the necessary standards and other supporting information are fully established.

5.1.6.3 Cryptographic Operation (for cryptographic hashing) (FCS_COP.1(3))

FCS_COP.1.1(3) **Refinement:** The TSF shall perform **cryptographic hashing services using the FIPS-approved security function Secure Hash Algorithm and message digest size of *[selection: one or more of 256 bits, 384 bits, 512 bits].***

Application Note: The message digest size should correspond to double the system symmetric encryption key strength.

5.1.6.4 Cryptographic Operation (for cryptographic key agreement) (FCS_COP.1(4))

Application Note: "Cryptographic key agreement" is a procedure where the resultant secret keying material is a function of information contributed by two participants, so that no party can predetermine the value of the secret keying material independently from the contributions of the other parties.

FCS_COP.1.1(4) **Refinement:** The TSF shall perform **cryptographic key agreement services using the FIPS-approved security function as specified in NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"** ***[selection:***

(1) [assignment: Finite Field-based key agreement algorithm] and cryptographic key sizes (modulus) of [assignment: 2048 bits or greater], or

(2) [assignment: Elliptic Curve-based key agreement algorithm] and cryptographic key size of [assignment: one or more of 256 bits, 384 bits, 521 bits], using only the NIST curve(s) [selection: one or more of P-256, P-384, P-521 as defined in FIPS PUB 186-3, "Digital Signature Standard"]]

Application Note: 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 key exchange, elliptic curves will be required after all the necessary standards and other supporting information are fully established.

that meets NIST Special Publication 800-57, "Recommendation for Key Management."

Application Note: Some authentication mechanism on the keying material is recommended. In addition, repeated generation of the same shared secrets should be avoided.

Application Note: FIPS 140-2 Annex D specifies references for FIPS-approved Key Establishment Techniques, one of which is NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography."

5.1.6.5 Extended: Random Number Generation (FCS_COP_(EXT).1)

FCS_COP_(EXT).1.1 The TSF shall perform all random number generation (RNG) services in accordance with a FIPS-approved RNG [*assignment: one of the RNGS specified in FIPS 140-2 Annex C*] seeded by *[selection:*

(1) one or more independent hardware-based entropy sources, and/or

(2) one or more independent software-based entropy sources, and/or

(3) a combination of hardware-based and software-based entropy sources.]

Application Note: The ST author should specify how the RNG is seeded.

FCS_COP_(EXT).1.2 The TSF shall defend against tampering of the random number generation (RNG)/ pseudorandom number generation (PRNG) sources.

Application Note: The RNG/PRNG should be resistant to manipulation or analysis of its sources, or any attempts to predictably influence its states. Three examples of very different approaches the TSF might pursue to address this include: a) identifying the fact that physical security must be applied to the product, b) applying checksums over the sources, or c) designing and implementing the TSF RNG with a concept similar to a keyed hash (e.g., where periodically, the initial state of the hash is changed unpredictably and each change is protected as when provided on a tamper-protected token, or in a secure area of memory.

5.1.7 FDP_PUD_(EXT).1 Protection of User Data

FDP_PUD_(EXT).1.1 When the administrator has enabled encryption, the TSF shall:

- encrypt authenticated user data transmitted to a wireless client from the radio interface of the wireless access system using the cryptographic algorithm(s) specified in FCS_COP_(EXT).2;
- decrypt authenticated user data received from a wireless client by the radio interface of the wireless access system using the cryptographic algorithm(s) specified in FCS_COP_(EXT).2.

Application Note: This requirement allows the TOE administrator to require that all user data transmitted on the WLAN be encrypted using the cryptographic algorithms specified by FCS_COP.

5.1.8 FDP_RIP.1(1) Subset residual information protection

FDP_RIP.1.1(1) The TSF shall ensure that any previous information content of a resource is made unavailable upon the [ST Author - Selection: allocation of the resource to, deallocation of the resource from] the following objects: [network packet objects].

Application Note: This requirement ensures that the TOE does not allow data from a previously transmitted packet to be inserted into unused areas or padding in the current packet.

5.1.9 FIA_AFL.1(1) Administrator Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within the range of [ST author assignment: range of acceptable values]* of unsuccessful authentication attempts occur related to [remote administrators logging on to the WLAN access system].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent remote login by administrators until an action is taken by a local Administrator].

Application note: This requirement applies to remote administrator login and does not apply to the local login of the TOE, since it does not make sense to lock a local administrator's account in this fashion. For the purpose of this PP, remote administrator refers to administrators that do not have either Serial cable or local console access to the TOE.

Application note: This requirement does NOT require that the TOE allow remote administration. However, if the TOE does allow administrators to login to the TOE remotely (e.g. from the wired interface or a management network) then it must provide a mechanism to prevent brute force attacks on the administrative account.

5.1.10 FIA_ATD.1(1) Administrator attribute definition

FIA_ATD.1.1(1) The TSF shall maintain the following **minimum** list of security attributes belonging to individual **administrators**: [password, [ST Author Assignment: any additional administrator security attributes]].

Application Note: The ST author should indicate any additional security attributes associated with an administrator account. If the TOE uses no additional attributes this assignment should indicate "no additional attributes".

5.1.11 FIA_ATD.1(2) User attribute definition

FIA_ATD.1.1(2) The TSF shall maintain the following **minimum** list of security attributes belonging to individual **remotely authenticated users**: [ST Author Assignment: user security attributes].

Application Note: The ST author should indicate the security attributes associated with remotely authenticated users.

5.1.12 FIA_UAU.1 Timing of local authentication

FIA_UAU.1.1 The TSF shall allow [ST Author Assignment: list of TSF mediated actions] on behalf of users to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note: This requirement refers to users that are authenticated locally by the TOE. This requirement does not refer to management and control packets that must be allowed to pass between the WLAN client and the access system before authentication. It is assumed that this information is not user specific and therefore not covered by this requirement. .The ST Author may substitute FIA_UAU.2 if there are no additional TSF mediated actions before identification.

5.1.13 FIA_UAU_(EXT).5(1) Extended: Multiple authentication mechanisms

FIA_UAU_(EXT).5.1(1) The TSF shall provide local authentication, and a remote authentication mechanism to perform user authentication.

FIA_UAU_(EXT).5.2(1) The TSF shall, at the option of the administrator, invoke the remote authentication mechanism for administrators and wireless LAN users.

*Application Note: This extended requirement is needed for local administrators because there is disagreement over whether existing CC requirements specifically **require** the TSF provide authentication. That the TOE provide authentication is implied by other FIA_UAU requirements, and generally assumed to be a requirement when other FIA_UAU requirements are included in a TOE. In order to remove any potential confusion about this PP, an extended requirement for authentication has been included. This PP mandates that the TOE provide the client to facilitate remote authentication via an authentication server. The IT environment will provide the authentication server, and it is important to specify that the TSF must provide the means for local administrator authentication in case the TOE cannot communicate with the authentication server.*

Since FIA_UAU.5.1(1) and 5.2(1) require that the TSF provide authentication mechanisms, this extended requirement is needed with respect to the remote users to specify that the TSF invoke a remote authentication mechanism rather than provide it.

FIA_UAU_(EXT).5.3(1) provides the administrator the ability to configure the TOE to use the authentication mechanism of their choice.

5.1.14 FIA_UID.2User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note: This requirement does not refer to management and control packets that must be allowed to pass between the WLAN client and the access system before authentication. It is assumed that this information is not user specific and therefore not covered by this requirement.

Application Note: It is also important to note that the identification credential presented to the authentication server (e.g. a user name) will be related to but not necessarily the same as the identification credential (e.g. MAC address of a remote system) that is used to enforce FDP_PUD_(EXT).

5.1.15 FIA_USB.1 User-subject binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [ST Author Assignment: list of user security attributes].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [ST Author Assignment: rules for the initial association of attributes].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [ST Author Assignment: rules for the changing of attributes].

Application Note: The ST author should indicate the attribute associated with both subjects acting on behalf of administrators and wireless user. If necessary this requirement should be iterated.

5.1.16 FMT_MOF.1(1) Management of cryptographic security functions behavior

FMT_MOF.1.1(1) The TSF shall restrict the ability to *modify the behavior* of the **cryptographic** functions [

- Crypto: load a key
- Crypto: delete/zeroize a key
- Crypto: set a key lifetime
- Crypto: set the cryptographic algorithm
- Crypto: set the TOE to encrypt or not to encrypt wireless transmissions
- Crypto: execute self tests of TOE hardware and the cryptographic functions]

to [administrators].

5.1.17 FMT_MOF.1(2) Management of audit security functions behavior

FMT_MOF.1.1 (2) The TSF shall restrict the ability to *enable, disable, and modify the behavior* of the functions [

- Audit: pre-selection of the events which trigger an audit record,
- Audit: start and stop of the audit function]

to [administrators].

5.1.18 FMT_MOF.1(3) Management of authentication security functions behavior

FMT_MOF.1.1(3) The TSF shall restrict the ability to *modify the behavior* of the **Authentication** functions [

- Auth: allow or disallow the use of an authentication server
- Auth: set the number of authentication failures that must occur before the TOE takes action to disallow future logins
- Auth: set the length of time a session may remain inactive before it is terminated]

to [administrators].

5.1.19 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.1.20 FMT_MTD.1(1) Management of Audit pre-selection data

FMT_MTD.1.1(1) The TSF shall restrict the ability to *query*, *modify*, *clear*, [create] the [set of rules used to pre-select audit events] to [the administrator].

5.1.21 FMT_MTD.1(2) Management of Authentication data (Administrator)

FMT_MTD.1.1(2) The TSF shall restrict the ability to *query*, *modify*, *delete*, *clear*, [create] the [authentication credentials, user identification credentials] to [administrators].

5.1.22 FMT_MTD.1(3) Management of Authentication data (User)

FMT_MTD.1.1(3) The TSF shall restrict the ability to *modify* the [user authentication credentials] to [TOE users].

5.1.23 FMT_SMF.1(1) Specification of Management Functions[2] (Cryptographic Function)

FMT_SMF.1.1(1) The TSF shall be capable of performing the following security management functions: [query and set the encryption/decryption of network packets (via FCS_COP_(EXT).2) in conformance with the administrators configuration of the TOE].

Application Note: This requirement ensures that those responsible for TOE administration are able to select an encryption algorithm identified in FCS_COP_(EXT).2 or no encryption for encrypting/decrypting data transmitted by the WLAN device.

5.1.23.1 FMT_SMF.1(2) Specification of Management Functions (TOE Audit Record Generation)

FMT_SMF.1.1(2) The TSF shall be capable of performing the following security management functions: [query, enable or disable Security Audit].

[2] The FMT_SMF (Specification of Management Functions) family is documented in CCIMB interpretation 65.

Application Note: This requirement ensures that those responsible for TOE administration are able to start or stop the TOE generation of audit records

5.1.23.2 FMT_SMF.1(3) Specification of Management Functions (Cryptographic Key Data)

FMT_SMF.1.1(3) The TSF shall be capable of performing the following security management functions: [query, set, modify, and delete the cryptographic keys and key data in support of FDP_PUD_(EXT) and enable/disable verification of cryptographic key testing].

Application Note: The intent of this requirement is to provide the ability to configure the TOE's cryptographic key(s). Configuring the key data may include: setting key lifetimes, setting key length, etc.

5.1.24 FMT_SMR.1(1) Security roles

FMT_SMR.1.1(1) The TSF shall maintain the roles [administrator, wireless user].

FMT_SMR.1.2(1) The TSF shall be able to associate users with roles.

Application Note: The only user allowed direct access to the TOE is the administrator. Wireless users can pass data through the TOE but do not have direct access. A role of wireless user is included in the TOE, but the scope of that role should be defined only to the extent necessary to support the activities of wireless users passing data through the TOE.

This PP also assumes that the TOE will contain a local authentication mechanism and the capability to use a remote authentication server. Although users are sometimes referred to as local or remote, these references do not imply a role.

5.1.25 FPT_STM_(EXT).1 Reliable time stamps

FPT_STM_(EXT).1.1 The TSF shall be able to provide reliable time stamps, **synchronized via an external time source,** for its own use.

Application Note: The TOE must be capable of obtaining a time stamp via an NTP server.

5.1.26 Explicit: TSF Testing (FPT_TST_EXP.1)

FPT_TST_EXP.1.1 The TSF shall run a suite of self tests during the initial start-up and also either periodically during normal operation, or at the request of an authorized administrator to demonstrate the correct operation of the TSF.

FPT_TST_EXP.1.2 The TSF shall provide authorized administrators with the capability to verify the integrity of stored TSF executable code through the use of the TSF-provided cryptographic services.

Application Note: Refer to FCS_COP.1.1(2) and FCS_COP.1.1(3) for TSF-provided cryptographic services .

5.1.27 TSF Testing (for cryptography) (FPT_TST.1(1))

FPT_TST.1.1(1) **Refinement:** The TSF shall run a suite of self tests **in accordance with FIPS PUB 140-2 and Appendix C of this profile** during initial start-up **(on power on)**, at the request of the **cryptographic administrator (on demand)**, **under various conditions defined in section 4.9.1 of FIPS 140-2,** and periodically **(at least once a day)** to demonstrate the correct operation of the **following cryptographic functions:i**

a) key error detection;

b) cryptographic algorithms;

c) RNG/PRNG

Application Note: These tests apply regardless of whether the cryptographic functionality is implemented in hardware, software, or firmware.

FPT_TST.1.2(1) **Refinement:** The TSF shall provide authorized **cryptographic administrators** with the capability to verify the integrity of **TSF data related to the cryptography by using TSF-provided cryptographic functions**.**ii**

Application Note: Refer to FCS_COP.1.1(2) and FCS_COP.1.1(3) for TSF-provided cryptographic services

.FPT_TST.1.3(1) **Refinement:** The TSF shall provide authorized **cryptographic administrators** with the capability to verify the integrity of stored TSF executable code **related to the cryptography by using TSF-provided cryptographic functions**.**iii**

Application Note: Refer to FCS_COP.1.1(2) and FCS_COP.1.1(3) for TSF-provided cryptographic services .

5.1.28 TSF Testing (for key generation components) (FPT_TST.1(2))

FPT_TST.1.1(2) **Refinement**: The TSF shall **perform** self tests **immediately after generation of a key** to demonstrate the correct operation **of each key generation component**. **If any of these tests fails, that generated key shall not be used, the cryptographic module shall react as required by FIPS PUB 140-2 for failing a self-test, and this event will be audited**.[iv]

Application Note: Key generation components are those critical elements that compose the entire key generation process (e.g., any algorithms, any RNG/PRNGs, any key generation seeding processes, etc.).

Application Note: These self-tests on the key generation components can be executed here as a subset of the full suite of self-tests run on the cryptography in FPT_TST.1(1) as long as all elements of the key generation process are tested.

FPT_TST.1.2(2) **Refinement:** The TSF shall provide authorized **cryptographic administrators** with the capability to verify the integrity of TSF data **related to the key generation by using TSF-provided cryptographic functions**.[v]

Application Note: Refer to FCS_COP.1.1(2) and FCS_COP.1.1(3) for TSF-provided cryptographic services

.FPT_TST.1.3(2) **Refinement:** The TSF shall provide authorized **cryptographic administrators** with the capability to verify the integrity of stored TSF executable code **related to the key generation by using TSF-provided cryptographic functions**.[vi]

Application Note: Refer to FCS_COP.1.1(2) and FCS_COP.1.1(3) for TSF-provided cryptographic services .

5.1.29 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate a **local** interactive **or wireless** session after **an** [administrator configurable time interval of user inactivity].

Application Note: This requirement applies to both local administrative sessions and wireless users that pass data through the TOE.

5.1.29.1 FTA_TAB.1 Default TOE access banners

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

5.1.30 FTP_ITC_(EXT).1(1) Inter-TSF trusted channel

FTP_ITC_(EXT).1.1(1)	The **TOE** shall provide **an encrypted** communication channel between itself **and entities in the TOE IT Environment** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC_(EXT).1.2(1)	The TSF shall permit *the TSF*, or ***the IT Environment entities*** to initiate communication via the trusted channel.
FTP_ITC_(EXT).1.3(1)	The TSF shall initiate communication via the trusted channel for [all authentication functions, remote logging, time, [ST Author selection: [ST Author assignment: communications with authorized IT entities determined by the ST author], none]].

Application Note: If a certificate authority server plays a role in the authentication of users, then the CA is considered an authorized IT entity and the TSF is expected to initiate secure communications with this entity. It is assumed that the IT environment includes an NTP server, an audit server and/or an authentication server.

5.1.31 FTP_TRP.1 Trusted path

FTP_TRP.1.1	The TSF shall provide a communication path between itself and wireless users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification, **replay** or disclosure.
FTP_TRP.1.2	The TSF shall permit ***wireless client devices*** to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for ***wireless user authentication***, [ST AUTHOR selection: [assignment: *other services for which trusted path is required, none*]].-

Application Note: This requirement ensures that the initial exchange of authentication information between the wireless client and the access system is protected.

5.2 Security Requirements for the IT Environment

This Protection Profile includes functional requirements for the IT Environment. The IT environment includes an authentication server, a time server, an audit collection server, and possibly a certificate authority.

In support of the audit server, the environment shall provide the capability to protect audit information and authentication credentials. The environment shall also provide the capability to selectively view audit data.

In support of the authentication server, the environment shall provide facilities to manage authentication information and limit brute force password attacks.

If these entities are not located on the same physical device as the TOE, it is expected that the communications between these entities and the TOE will be protected. In addition, the TOE IT environment is responsible for protecting itself and ensuring that its security mechanisms cannot be bypassed.

Table 10: Security Functional Requirements for the TOE IT Environment

Functional Component		Dependencies[3]
FAU_GEN.1(2)	Audit data generation	None
FAU_SAR.1	Audit review	FAU_GEN.1
FAU_SAR.2	Restricted audit review	FAU_SAR.1
FAU_SAR.3	Selectable audit review	FAU_SAR.1
FAU_STG.1	Protected audit trail storage	FAU_GEN.1
FAU_STG.3	Action in case of possible audit data loss	FAU_STG.1
FDP_RIP.1(2)	Subset Residual Information Protection	None
FIA_AFL.1(2)	Remote User failure handling	FIA_UAU.1
FIA_ATD.1(3)	User attribute definition	None
FIA_UAU_(EXT).5(2)	Remote authentication mechanisms	FIA_UID.1
FIA_UID.1	Timing of identification	None
FMT_MOF.1(4)	Management of Security Functions Behavior	FMT_SMF.1(1)(2)(3) FMT_SMR.1
FMT_MTD.1(4)	Management of time data	FMT_SMR.1
FMT_SMR.1(2)	Security roles	None
FTP_ITC_(EXT).1	Inter-TSF trusted channel	None
FPT_STM.1	Reliable time stamps	None

Application Note: This protection profile requires that the TOE IT environment provide significant functionality. It is also acceptable for an ST claiming compliance with this PP to satisfy some or all of the requirements levied on the IT environment by including the same requirements as part of the TOE.

[3] The purpose of requirements on the IT environment is to supplement the TOE and to ensure that the TOE and the IT environment together satisfy all security objectives. In order to limit the scope of the IT environment, only those IT environmental requirements that directly contribute to the satisfaction of objectives have been included in this PP. Requirements for the IT environment necessary simply to satisfy management guidance, audit guidance, or dependency chains have not been included in this PP.

5.2.1.1 FAU_GEN.1(2) Audit data generation

FAU_GEN.1.1(2) The **TOE IT Environment** 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 [*minimum*] level of audit; and

c. [other specifically defined auditable events].

Table 11: TOE IT Environment Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None	None
FAU_SAR.1	None	None
FAU_SAR.2	Unsuccessful attempt to read the audit records	The identity of the user attempting to perform the function
FAU_SAR.3	None	None
FAU_STG.1	None	None
FAU_STG.3	Any actions taken when audit trail limits are exceeded	None
FDP_RIP.1	None	None
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal	None
FIA_ATD.1	None	None
FIA_UAU_(EXT).5	Use of the authentication mechanism (success or failure)	User identity - the TOE **SHALL NOT** record invalid passwords the audit log.
FIA_UID.1	None	None
FMT_MOF.1	Changes to audit server settings Changes to authentication server settings Changes to time server settings	None
FMT_MTD.1(4)	Changes to the time data	None
FMT_SMR.1	None	None

Requirement	Auditable Events	Additional Audit Record Contents
FTP_ITC_(EXT).1	Initiation/Closure of a trusted channel;	Identification of the remote entity with which the channel was attempted/created; Success of failure of the event
FPT_STM.1	Setting time/date	Identity of the administrator that performed the action

FAU_GEN.1.2(2) The **TOE IT environment** shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity **(if applicable)**, 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 Table 11].

Application Note: Event type is defined as the BSD syslog severity level indicator in the Terminology section of this PP.

Application Note: In column 3 of the table 10, "if available/applicable" is used to designate data that should be included in the audit record if it "makes sense" in the context of the event that generates the record. If no other information is required (other than that listed in FAU_GEN.1.2 item a) for a particular audit event type, then "none" is acceptable and should be inserted at the proper location in the table.

5.2.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The **TOE IT environment** shall provide **only the** [Administrator] with the capability to read [all audit data] from the audit records.

FAU_SAR.1.2 The **TOE IT environment** shall provide the audit records in a manner suitable for the **administrator** to interpret the information.

Application Note: This requirement ensures that the TOE IT environment provides the administrator with functionality necessary for the administrator to review the audit records generated by the TOE.

5.2.3 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The **TOE IT environment** shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Application Note: This requirement ensures that access to audit records generated by the TOE is limited to those authorized to view the information.

5.2.4 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The **TOE IT environment** shall provide the ability to perform [ST AUTHOR selection: *searches, sorting, ordering*] of audit data based on [event type, date, time and/or [ST Author Assignement: additional sort/search/ordering criteria]].

5.2.5 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The **TOE IT environment** shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The **TOE IT environment** shall be able to *prevent* unauthorized modifications to the audit records in the audit trail.

5.2.6 FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The **TOE IT environment** shall [immediately alert the administrators by displaying a message at the local console, [ST AUTHOR -selection:[assignment: other actions determined by the ST AUTHOR], "none"]] if the audit trail exceeds [an administrator-settable percentage of storage capacity].

Application Note: The ST Author should determine if there are other actions that should be taken when the audit trial setting is exceeded, and put these in the assignment. If there are no other actions, then the ST Author should select "none".

5.2.7 FDP_RIP.1(2) Subset Residual Information Protection

FDP_RIP.1.1(2) The **TOE IT Environment** shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* the following objects: [network pack objects].

Application Note: This requirement ensures that the TOE environment does not allow data from a previously transmitted packet to be inserted into unused areas or padding in the current packet. Since operations on requirement for the IT environment must be completed, the selection "allocation of resources to" has been made because it is encompassing of the two options (e.g. a system that make the information contents of resource unavailable when the resource is freed can also claim to meet the requirement that the content of the resource be freed prior to reallocation).

5.2.8 FIA_AFL.1(2) Remote User Authentication failure handling

FIA_AFL.1.1(2) The **TOE IT Environment** shall detect when *an administrator configurable positive integer within [assignment: range of acceptable values]* of unsuccessful authentication attempts occur related to [remote users logging on to the WLAN access system].

FIA_AFL.1.2 (2) When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the remote user from authenticating until action is taken by an administrator].

Application Note: This requirement ensures that the TOE IT Environment has the capability to detect multiple authentication attempts and take action to disable subsequent authentication attempts. Since the remote user authentication function is split between the TOE and the IT environment, it is possible that the TOE may provide this functionality, in that case this requirement should be move into the TOE requirements in an ST claiming conformance to this PP. I

5.2.8.1 FIA_ATD.1(3) User attribute definition

FIA_ATD.1.1(3) The TOE IT environment shall maintain the following **minimum** list of security attributes belonging to individual **remotely authenticated users**: [ST Author Assignment: user security attributes].

Application Note: The ST author should indicate the security attributes maintained in the IT environment and associated with remotely authenticated users.

5.2.8.2 FIA_UAU_(EXT).5(2) Remote authentication mechanisms

FIA_UAU_(EXT).5.1(2) The **TOE IT Environment** shall provide [a remote authentication mechanism] to **provide TOE remote** user authentication.

FIA_UAU_(EXT).5.2(2) The **TOE IT Environment** shall authenticate any user's claimed identity according to the [ST Author Assignment: rules describing how the remote authentication mechanisms provide authentication for TOE **remote** users].

*Application Note: This extended requirement is needed because there is confusion over whether on not existing CC requirements specifically **require** the TSF (or IT environment) provide authentication. That the TOE provide authentication is implied by FIA_UAU and FIA_UID requirements, and generally assumed to be a requirement when those requirements are included in a PP/ST. In order to remove any potential confusion about this PP, an extended requirement for authentication has been included. This PP allows the IT environment to provide an authentication server to be used for authentication of remote users, the ST author should use the*

assignment to indicate the remote authentication requirements specific to their TOE and its environment.

5.2.8.3 FIA_UID.1 Timing of identification

FIA_UID.1.1 The **TOE IT environment** shall allow [ST Author Assignment: list of **IT environment**-mediated actions] on behalf of the **TOE remote user** to be performed before the user is identified.

FIA_UID.1.2 The **TOE IT environment** shall require each **TOE remote** user to identify itself before allowing any other **IT environment or** TSF-mediated actions on behalf of that **TOE remote** user.

Application Note: This requirement does not refer to management and control packets that must be allowed to pass between the wlan client and the access system before authentication. It is assumed that this information is not user specific and therefore not covered by this requirement.

Application Note: It is also important note that the identification credential presented to the authentication server (e.g. a user name) will be related to but necessarily the same as the identification credential (e.g. MAC address of a remote system) that is used to enforce **FDP_PUD_(EXT)**.

5.2.9 FMT_MOF.1(4) Management of Security Functions Behavior

FMT_MOF.1.1(4) The **TOE IT environment** shall restrict the ability to *determine the behavior* of the functions: [

- Audit,
- Remote Authentication
- Time service]

to [the administrator].

Application Note: The TOE IT environment must be managed in conjunction with the TOE.

5.2.10 FMT_MTD.1(4) Management of time data

FMT_MTD.1.1(4) The **TOE IT environment** shall restrict the ability to [set] the [time and date used to form the time stamps in FPT_STM.1] to [the Security Administrator or authorized IT entity].

5.2.11 FMT_SMR.1(2) Security roles

FMT_SMR.1.1(2) The **TOE IT environment** shall maintain the roles [administrator].

FMT_SMR.1.2(2) The **TOE IT environment** shall be able to associate users with roles.

Application Note: The TOE IT environment must include an administrative role for its own management.

5.2.12 FTP_ITC_(EXT).1(2) Inter-TSF trusted channel

FTP_ITC_(EXT).1.1(2)	The **TOE IT environment** shall provide **an encrypted** communication channel between itself **and the TOE** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC_(EXT).1.2(2)	The TOE IT Environment shall permit *the TSF*, or ***the TOE IT Environment entities*** to initiate communication via the trusted channel.
FTP_ITC_(EXT).1.3(2)	The **TOE IT environment** shall initiate communication via the trusted channel for [all authentication functions, remote logging, time, [ST Author selection: [ST Author assignment: communications with authorized IT entities determined by the ST author], none]].

Application Note: For FTP_ITC_(EXT).1.1(2) it is expected that the environment be able to provide and encrypted channel between the environment and the TOE. This is to provide for communications between itself and the TOE, as end points, to protect the communications between the TOE and the IT environment.

Application Note: If a certificate authority server plays a role in the authentication of users, then the CA is considered an authorized IT entity and the TSF is expected to initiate secure communications with this entity. It is assumed that the IT environment includes an NTP server, an audit server and/or an authentication server.

5.2.13 FPT_STM.1 Reliable time stamps

FPT_STM.1.1	The **TOE IT environment** shall be able to provide reliable time **and date** stamps for **the TOE and** its own use.

Application Note: The TOE IT environment must provide reliable time stamps (for example: an NTP server). It is also acceptable for the TOE to satisfy this requirement by providing its own time stamp.

5.3 TOE Security Assurance Requirements

The TOE security assurance requirements summarized in **Error! Reference source not found.**, identify the management and evaluative activities required to address the threats and policies identified in section 3 of this protection profile. Section 5 provides a justification for the chosen

security assurance requirements and the selected assurance level EAL2 augmented with ALC_FLR.2 (Flaw Remediation).

Table 5: TOE Assurance Requirements

Assurance Class	ASSURANCE COMPONENTS	ASSURANCE COMPONENTS DESCRIPTION
DEVELOPMENT	ADV_ARC.1	Architectural Design with domain separation and non-bypassability
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic design
GUIDANCE DOCUMENTS	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
LIFE CYCLE SUPPORT	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	**Flaw Reporting Procedures**
TESTS	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - conformance
VULNERABILITY ASSESSMENT	AVA_VAN.2	Vulnerability analysis

5.3.1 Class ADV: Development

5.3.1.1 ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements:

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

5.3.1.2 ADV_FSP.2 Security-enforcing functional specification

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

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

ADV_FSP.2.2E The evaluator *shall determine* that the functional specification is an accurate and complete instantiation of the SFRs.

5.3.1.3 ADV_TDS.1 Basic design

Dependencies: ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall describe the behavior of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C The design shall summarize the SFR-enforcing behavior of the SFR-enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all behavior described in the TOE design is mapped to the TSFIs that invoke it.

Evaluator action elements:

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

ADV_TDS.1.2E The evaluator *shall determine* that the design is an accurate and complete instantiation of all security functional requirements.

5.3.2 Class AGD: Guidance documents

5.3.2.1 AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user 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.

5.3.2.2 AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

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

5.3.3 Class ALC: Life-cycle support

5.3.3.1 ALC_CMC.2 Use of a CM system

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMC.2.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.2.1C The TOE shall be labeled with its unique reference.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

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

5.3.3.2 ALC_CMS.2 Parts of the TOE CM coverage

Dependencies: No dependencies.

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; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

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

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

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

5.3.3.3 ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

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

5.3.3.4 ALC_FLR.2 Flaw reporting procedures

Dependencies: No dependencies.

Developer action elements:

ALC_FLR.2.1D The developer shall document flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.

Content and presentation elements:

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

ALC_FLR.2.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

Evaluator action elements:

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

5.3.4 Class ATE: Tests

5.3.4.1 ATE_COV.1 Evidence of coverage

Dependencies: ADV_FSP.2 Security-enforcing functional specification
ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

Evaluator action elements:

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

5.3.4.2 ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:

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

5.3.4.3 ATE_IND.2 Independent testing - sample

Dependencies: ADV_FSP.2 Security-enforcing functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_COV.1 Evidence of coverage
ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

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

ATE_IND.2.2E The evaluator *shall execute* a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator *shall test* a subset of the TSF to confirm that the TSF operates as specified.

5.3.5 Class AVA: Vulnerability assessment

5.3.5.1 AVA_VAN.2 Vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description
ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.2.1C The TOE shall be suitable for testing.

Evaluator action elements:

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

AVA_VAN.2.2E The evaluator *shall perform* a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator *shall perform* an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E 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.

Application Note: The TOE version used as the basis for testing should include a reference to the specific signature set in place when this activity is conducted.

6. Rationale

This section describes the rationale for the Security Objectives and Security Functional Requirements as defined in Section 3 and Section 4, respectively. Additionally, this section describes the rationale for not satisfying all of the dependencies. Table 13 illustrates the mapping from Security Objectives to Threats and Policies.

6.1 Rationale for Security Objectives

Table 13: Security Objectives to Threats and Policies Mappings

Threat/Policy	Objectives Addressing the Threat	Rationale
T.ACCIDENTAL_ADMIN_ ERROR An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.	O.ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure management. O.MANAGE The TOE will provide those functions and facilities necessary to support the administrators in their management of the security of the TOE. OE.NO_EVIL Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance. OE.NO_GENERAL_PURPOSE There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or	O.ADMIN_GUIDANCE helps to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is insecure. O.MANAGE also contributes to mitigating this threat by providing administrators the capability to view and manage configuration settings. For example, if the administrator made a mistake when configuring the set of permitted users' authentication credentials, providing the capability to view the lists of authentication credentials affords them the ability to review the list and discover any mistakes that might have been made. OE.NO_EVIL contributes to mitigating this threat by ensuring that the administrators are non-hostile and are trained to appropriately manage and administer the TOE.

Threat/Policy	Objectives Addressing the Threat	Rationale
	user applications) available on the TOE.	OE.NO_GENERAL_PURPOSE also helps to mitigate this threat by ensuring that there can be no accidental errors due to the introduction of unauthorized software or data, by ensuring that there are no general-purpose or storage repository applications available on the TOE.
T.ACCIDENTAL_CRYPTO_COMPROMISE A user or process may cause key data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.	O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource is not released when the resource is reallocated. OE.RESIDUAL_INFORMATION The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. O.SELF_PROTECTION The TOE will maintain a domain for itself and the TOE's own execution that protects them and their resources from external interference, tampering, or unauthorized disclosure through their interfaces. OE.SELF_PROTECTION The environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.	O.RESIDUAL_INFORMATION; OE.RESIDUAL_INFORMATION contributes to the mitigation of this threat by ensuring that any residual data is removed from network packet objects and ensuring that cryptographic material is not accessible once it is no longer needed. O.SELF_PROTECTION ensures that the TOE will have adequate protection from external sources and that all TSP functions are invoked. OE.SELF_PROTECTION ensures that the TOE IT environment will have protection similar to that of the TOE.

Threat/Policy	Objectives Addressing the Threat	Rationale
T.MASQUERADE A user may masquerade as an authorized user or the authentication server to gain access to data or TOE resources.	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE. OE.TOE_ACCESS The environment will provide mechanisms that support the TOE in providing users logical access to the TOE. OE.TOE_NO_BYPASS Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.	O.TOE_ACCESS mitigates this threat by controlling logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanism, this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE. Finally, the TOE includes requirements that ensure protected channels are used to authenticate wireless users and to communicate with critical portions of the TOE IT environment. OE.TOE_ACCESS supports TOE authentication by providing an authentication server in the TOE IT environment. The environment also includes requirements that ensure protected channels are used to communicate with critical portions of the TOE IT environment. OE.TOE_NO_BYPASS contributes to mitigating this threat by ensuring that wireless clients must be configured for all information flowing between a wireless client and another client or other host on the network without passing through the TOE.

Threat/Policy	Objectives Addressing the Threat	Rationale
T.POOR_DESIGN Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.	O.CONFIGURATION_ IDENTIFICATION The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly. O.DOCUMENTED_ DESIGN The design of the TOE is adequately and accurately documented. O.VULNERABILITY_ ANALYSIS The TOE will undergo vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.CONFIGURATION_IDENTIFICATION plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE's design documentation and the ability to report and resolve security flaws. O.DOCUMENTED_DESIGN counters this threat, to a degree, by requiring that the TOE be developed using sound engineering principles. The use of a high level design and the functional specification ensure that developers responsible for TOE development understand the overall design of the TOE. This in turn decreases the likelihood of design flaws and increases the chance that accidental design errors will be discovered. ADV_RCR.1 ensures that the TOE design is consistent across the High Level Design and the Functional Specification. O.VULNERABILITY_ANALYSIS_TEST ensures that the TOE has been analyzed for obvious vulnerabilities and that any vulnerabilities found have been removed or otherwise mitigated, this includes analysis of any probabilistic or permutational mechanisms incorporated into a TOE claiming conformance to this PP.

Threat/Policy	Objectives Addressing the Threat	Rationale
T.POOR_IMPLEMENTATION Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.	O.CONFIGURATION_ IDENTIFICATION The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly. O.PARTIAL_FUNCTIONAL_TESTI NG The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements. O.VULNERABILITY_ ANALYSIS The TOE will undergo vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.CONFIGURATION_IDENTIFICATION plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE's design. This ensures that changes to the TOE are performed in structure manner and tracked. O.PARTIAL_FUNCTIONAL_TESTING ensures that the developers provide evidence and demonstration that all security functions perform as specified through independent sample testing. O.VULNERABILITY_ANALYSIS_TEST ensures that the TOE has been analyzed and tested to demonstrate that it is resistant to obvious vulnerabilities.
T.POOR_TEST The developer or tester performs insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may occur, resulting in incorrect TOE behavior being undiscovered leading to flaws that may be exploited by a mischievous user or program.	O.CORRECT_ TSF_OPERATION The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site. O.PARTIAL_FUNCTIONAL_TESTI NG The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements. O.VULNERABILITY_ ANALYSIS The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws. O.DOCUMENTED_DESIGN The design of the TOE is adequately and accurately documented.	O.CORRECT_ TSF_OPERATION provides assurance that the TSF continues to operate as expected in the field. O.PARTIAL_FUNCTIONAL_TESTING increases the likelihood that any errors that do exist in the implementation will be discovered through testing. O.VULNERABILITY_ANALYSIS_TEST addresses this concern by requiring a vulnerability analysis be performed in conjunction with testing that goes beyond functional testing. This objective provides a measure of confidence that the TOE does not contain security flaws that may not be identified through functional testing. O.DOCUMENTED_DESIGN. helps to ensure that the TOE's documented design satisfies the security functional requirements. In order to ensure the TOE's design is correctly realized in its implementation, the appropriate level of functional testing of the TOE's security mechanisms must be performed during the evaluation of the TOE.

Threat/Policy	Objectives Addressing the Threat	Rationale
T.RESIDUAL_DATA A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.	O.RESIDUAL_ INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. OE.RESIDUAL_INFORMATION The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.	O.RESIDUAL_INFORMATION and TOE.RESIDUAL_INFORMATION contributes to the mitigation of this threat by ensuring that any residual data is removed from network packet objects and ensuring that cryptographic material is not accessible once it is no longer needed.
T.TSF_COMPROMISE A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).	O.MANAGE The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE. OE.MANAGE The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. O.RESIDUAL_ INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. OE.RESIDUAL_INFORMATION The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. O.SELF_PROTECTION The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its interfaces. OE.SELF_PROTECTION The environment will maintain a domain for its own execution that protects itself and its resources from	O.MANAGE mitigate this threat by restricting access to administrative functions and management of TSF data to the administrator. OE.MANAGE ensures that the administrator can view security relevant audit events. O.RESIDUAL_INFORMATION and OE.RESIDUAL_INFORMATION contributes to the mitigation of this threat by ensuring that any residual data is removed from network packet objects and ensuring that cryptographic material is not accessible once it is no longer needed. O.SELF_PROTECTION requires that the TOE environment be able to protect itself from tampering and that the security mechanisms in the TOE cannot be bypassed. Without this objective, there could be no assurance that users could not view or modify TSF data or TSF executables. OE.SELF_PROTECTION ensures that the TOE IT environment will have protection similar to that of the TOE.

Threat/Policy	Objectives Addressing the Threat	Rationale
	external interference, tampering, or unauthorized disclosure through its own interfaces.	
T.UNATTENDED_SESSION A user may gain unauthorized access to an unattended session.	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	The only sessions that are established with the TOE are anticipated to be administrative sessions. Hence, this threat is restricted to administrative sessions. The termination of general user sessions is expected to be handled by the IT environment. O.TOE_ACCESS helps to mitigate this threat by including mechanisms that place controls on administrator sessions. Administrator sessions are dropped after an Administrator defined time period of inactivity. Dropping the connection of a session (after the specified time period) reduces the risk of someone accessing the machine where the session was established, thus gaining unauthorized access to the session.
T.UNAUTHORIZED_ACCESS A user may gain access to services (either on the TOE or by sending data through the TOE) for which they are not authorized according to the TOE security policy.	O.MEDIATE The TOE must mediate the flow of information to and from wireless clients communicating via the TOE in accordance with its security policy. O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE. OE.TOE_ACCESS The environment will provide mechanisms that support the TOE in providing user's logical access to the TOE. O.SELF_PROTECTION The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure. OE.SELF_PROTECTION The IT environment will maintain a domain for its own execution that protects itself and its resources from	O.MEDIATE works to mitigate this threat by ensuring that all network packets that flow through the TOE are subject to the information flow policies. O.TOE_ACCESS and OE.TOE ACCESS. The TOE requires authentication prior to gaining access to certain services on or mediated by the TOE. O.SELF_PROTECTION and OE.SELF_PROTECTION. The TSF and its environment must ensure that all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services. O.MANAGE and OE.MANAGE. The TOE and its environment restrict the ability to modify the security attributes associated with the TOE to the administrator. These objectives ensure that no other user can modify the information flow policy to bypass the intended TOE security policy. OE.TOE_NO_BYPASS contributes to mitigating this threat by ensuring that wireless clients must be configured to use the wireless access system for all information flowing

Threat/Policy	Objectives Addressing the Threat	Rationale
	external interference, tampering, or unauthorized disclosure through its own interfaces. O.MANAGE The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. OE.MANAGE The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. OE.TOE_NO_BYPASS Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.	between a wireless client and any other host on the network. If the clients are properly configured, any information passing through the TOE will be inspected to ensure it is authorized by TOE polices.
T.UNAUTH_ADMIN_ACCESS An unauthorized user or process may gain access to an administrative account.	O.ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure management. O.MANAGE The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. OE.MANAGE The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE. OE.TOE_ACCESS	O.ADMIN_GUIDANCE helps to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is not secure. O.MANAGE and OE.MANAGE mitigate this threat by restricting access to administrative functions and management of TSF data to the administrator. O.TOE_ACCESS and OE.TOE_ACCESS helps to mitigate this threat by including mechanisms to authenticate TOE administrators and place controls on administrator sessions. OE.NO_EVIL helps to mitigate this threat by ensuring that the TOE administrators have guidance that instructs them in how to administer the TOE in a secure manner.

Threat/Policy	Objectives Addressing the Threat	Rationale
	The environment will provide mechanisms that support the TOE in providing user's logical access to the TOE. OE.NO_EVIL Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.	
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 system.	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 administrator configurable banner that provides all users with a warning about unauthorized use of the TOE. A banner will be presented for all TOE services that allow direct access to the TOE. In other words, it will be required for all administrative actions. The presentation of banners prior to actions that take place as a result of the passing of traffic through the TOE is assumed to be provided by the IT environment.
P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE.	O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security-relevant events associated with users. OE.AUDIT_PROTECTION The IT Environment will provide the capability to protect audit information and the authentication credentials. OE.AUDIT_REVIEW The IT Environment will provide the capability to selectively view audit information. O.MANAGE The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE., and restrict these functions and facilities from unauthorized use. OE.MANAGE The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators	O.AUDIT_GENERATION addresses 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 the identity of the user. Additionally, the administrator's ID is recorded when any security relevant change is made to the TOE (e.g. access rule modification, start-stop of the audit mechanism, establishment of a trusted channel, etc.). OE.AUDIT_PROTECTION provides protected storage of TOE and IT environment audit data in the environment. OE.AUDIT_REVIEW Further supports accountability by providing mechanisms for viewing and sorting the audit logs O.MANAGE ensures that access to administrative functions and management of TSF data is restricted to the administrator. OE.MANAGE ensures that the administrator can manage audit functionality in the TOE IT environment. O.TIME_STAMPS plays a role in supporting this policy by requiring the TOE to provide a reliable time stamp (via an external NTP server).

Threat/Policy	Objectives Addressing the Threat	Rationale
	in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. O.TIME_STAMPS The TOE shall obtain reliable time stamps and the capability for the administrator to set the time used for these time stamps. OE.TIME_STAMPS The TOE IT environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps. O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE. OE.TOE_ACCESS The environment will provide mechanisms that support the TOE in providing user's logical access to the TOE.	The audit mechanism is required to include the current date and time in each audit record. All audit records that include the user ID, will also include the date and time that the event occurred. OE.TIME_STAMPS ensures that the TOE IT environment provides time services. O.TOE_ACCESS and OE.TOE_ACCESS support this policy by controlling logical access to the TOE and its resources. This objective ensures that users are identified and authenticated so that their actions may be tracked by the administrator .
P.CRYPTOGRAPHY The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.	O.CRYPTOGRAPHY The TOE shall provide cryptographic functions to maintain the confidentiality and allow for detection of modification of user data that is transmitted between physically separated portions of the TOE, or outside of the TOE. O.RESIDUAL_ INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.	O.CRYPTOGRAPHY satisfies this policy by requiring the TOE to implement NIST FIPS validated cryptographic services. These services will provide confidentiality and integrity protection of TSF data while in transit to remote parts of the TOE. O.RESIDUAL_INFORMATION satisfies this policy by ensuring that cryptographic data are cleared according to FIPS 140-1/2.
P.CRYPTOGRAPHY_VALIDATED Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.;	O.CRYPTOGRAPHY The TOE shall provide cryptographic functions to maintain the confidentiality and allow for detection of modification of user data that is transmitted between physically separated portions of the TOE, or outside of the TOE. O.CRYPTOGRAPHY_VALIDATED	O.CRYPTOGRAPHY satisfies this policy by requiring the TOE to implement NIST FIPS validated cryptographic services. These services will provide confidentiality and integrity protection of TSF data while in transit to remote parts of the TOE. O.CRYPTOGRAPHY_VALIDATED satisfies this policy by requiring that all cryptomodules for cryptographic services be NIST 140-1/2 validated. This will provide assurance that the

Threat/Policy	Objectives Addressing the Threat	Rationale
encryption, decryption, signature, hashing, key exchange, and random number generation services).	The TOE will use NIST FIPS 140-1/2 validated cryptomodules for cryptographic services implementing NIST-approved security functions and random number generation services used by cryptographic functions.	NIST-approved security functions and random number generation will be in accordance with NIST and validated according the FIPS 140-1/2
P.ENCRYPTED_CHANNEL The TOE shall provide the capability to encrypt/decrypt wireless network traffic between the TOE and those wireless clients that are authorized to join the network.	O.CRYPTOGRAPHY The TOE shall provide cryptographic functions to maintain the confidentiality and allow for detection of modification of user data that is transmitted between physically separated portions of the TOE, or outside of the TOE. O.CRYPTOGRAPHY_VALIDATED The TOE will use NIST FIPS 140-1/2 validated cryptomodules for cryptographic services implementing NIST-approved security functions and random number generation services used by cryptographic functions. O.MEDIATE The TOE must mediate the flow of information to and from wireless clients communicating via the TOE in accordance with its security policy. OE.PROTECT_MGMT_COMMS The environment shall protect the transport of audit records to the audit server, remote network management, and authentication server communications with the TOE in a manner that is commensurate with the risks posed to the network.	O.CRYPTOGRAPHY and O.CRYPTOGRAPHY_VALIDATED satisfy this policy by requiring the TOE to implement NIST FIPS validated cryptographic services. These services will provide confidentiality and integrity protection of TSF data while in transit to wireless clients that are authorized to join the network. O.MEDIATE further allows the TOE administrator to set a policy to encrypt all wireless traffic. OE.PROTECT_MGMT_COMMS provides that the audit records, remote network management information and authentication data will be protected by means of a protected channel in the environment.
P.NO_AD_HOC_NETWORKS In concordance with the DOD Wireless Policy, there will be no ad hoc 802.11 or 802.15 networks allowed.	O.MEDIATE The TOE must mediate the flow of information to and from wireless clients communicating via the TOE in accordance with its security policy. OE.TOE_NO_BYPASS Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE	O.MEDIATE works to support this policy by ensuring that all network packets that flow through the TOE are subject to the information flow policies. OE.TOE_NO_BYPASS supports this policy by ensuring that wireless clients must be configured to use the wireless access system for all information flowing between a wireless client and any other host on the network. If the clients are properly configured, any information passing through the TOE will be inspected to ensure it is authorized by TOE polices.

6.2 Rationale for Security Objectives in the TOE Environment

Four of the security objectives for the TOE are simply restatements of an assumption found in Section 3. Therefore, these four objectives for the environment, OE.NO_EVIL, OE.PHYSICAL, OE.NO_GENERAL_PURPOSE, and OE.TOE_NO_BYPASS trace to the assumptions trivially.

The remainder of the security objectives for the IT environment have been included in this Protection Profile in order to support the TOE IT environment security functions. The rationale support is documented in Table 13 along with the rationale for security objectives for the TOE. All of the security objectives are either referenced in the previous section with regards to specific threats or they are direct rephrasing of assumptions.

6.3 Rationale for TOE Security Requirements

Table 14: Rationale for TOE Security Requirements

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure management.	ALC_DEL.1 AGD_PRE.1 AGD_OPE.1	ALC_DEL.1 ensures that the administrator has the ability to begin their TOE installation with a *clean* (e.g., malicious code has not been inserted once it has left the developer's control) version of the TOE, which is necessary for secure management of the TOE The AGD_PRE.1 requirement ensures the administrator has the information necessary to install the TOE in the evaluated configuration. Often times a vendor's product contains software that is not part of the TOE and has not been evaluated. The Installation, Generation and Startup (IGS) documentation ensures that once the administrator has followed the installation and configuration guidance the result is a TOE in a secure configuration. The AGD_OPE. requirement mandates the developer provide the administrator with guidance on how to operate the TOE in a secure manner. This includes describing the interfaces the administrator uses in managing the TOE and any security parameters that are configurable by the administrator. The documentation also provides a description of how to set up and use the auditing features of the TOE. The AGD_OPE is also intended for non-administrative users. If the TOE provides facilities/interfaces for this type of user, this

Objective	Requirements Addressing the Objective	Rationale
		guidance will describe how to use those interfaces securely. This could include guidance on the setup of wireless clients for use with the TOE. If it is the case that the wireless clients may be configured by administrators that are not administrators of this TOE, then that guidance may be user guidance from the perspective of this TOE. AGD_OPE.1 AND AGD_PRE.1 analysis during evaluation will ensure that the guidance documentation can be followed unambiguously to ensure the TOE is not misconfigured in an insecure state due to confusing guidance.
O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security-relevant events associated with users.	FAU_GEN.1 FAU_GEN.2 FAU_SEL.1 FIA_USB.1 FPT_STM_(EXT).1 FTP_ITC_(EXT).1	FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that the administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. There is a minimum of information that must be present in every audit record and this requirement defines that, as well as the additional information that must be recorded for each auditable event. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements an ST author adds to this PP. FAU_GEN.2 ensures that the audit records associate a user identity with the auditable event. In the case of authorized users, the association is accomplished with the user ID. In all other cases, the association is based on the source network identifier, which is presumed to be the correct identity, but cannot be confirmed since these subjects are not authenticated. FAU_SEL.1allows for the selection of events to be audited. This requires that the criteria used for the selection of auditable events to be defined. For example, the user identity can be used as selection criterion for the events to be audited. FIA_USB.1 plays a role is satisfying this objective by requiring a binding of security attributes associated with users that are authenticated with the subjects that represent them in the TOE. This only applies to authorized users, since the identity of unauthenticated users cannot be confirmed. Therefore, the audit trail may not always have the proper identity of the subject that causes an audit record to be generated (e.g., presumed network address of an unauthenticated user may be a spoofed address).

Objective	Requirements Addressing the Objective	Rationale
		FPT_STM_(EXT).1 supports the audit functionality by ensuring that the TOE is capable of obtaining a time stamp for use in recording audit events. FTP_ITC_(EXT).1 provides a trusted channel for services provided by the TOE IT environment (the audit server and the time server).
O.CONFIGURATION_ IDENTIFICATION The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly.	ALC_CMC.2 ALC_CMS.2 ALC_FLR.2	ALC_CMC.2 contributes to this objective by requiring the developer have a configuration management plan that describes how changes to the TOE and its evaluation deliverables are managed. ALC_CMS.2 is necessary to define the items that must be under the control of the CM system. This requirement ensures that the TOE implementation representation, design documentation, test documentation (including the executable test suite), user and administrator guidance, and CM documentation are tracked by the CM system. ALC_FLR.2 plays a role in satisfying this objective by requiring the developer to have procedures that address flaws that have been discovered in the product, either through developer actions (e.g., developer testing) or discovery by others. The flaw remediation process used by the developer corrects any discovered flaws and performs an analysis to ensure new flaws are not created while fixing the discovered flaws.
O.CORRECT_ TSF_OPERATION The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.	FPT_TST_(EXT).1 FPT_TST.1(1) FPT_TST.1(2)	FPT_TST_(EXT).1 is necessary to ensure the correctness of the TSF software and TSF data. If TSF software is corrupted it is possible that the TSF would no longer be able to enforce the security policies. This also holds true for TSF data, if TSF data is corrupt the TOE may not correctly enforce its security policies. The FPT_TST.1(1) for crypto and FPT_TST.1(2) for key generation functional requirement has been included to address the critical nature and specific handling of the cryptographic related TSF data. Since the cryptographic TSF data has specific FIPS PUB requirements associated with them it is important to ensure that any fielded testing on the integrity of these data maintains the same level of scrutiny as specified in the FCS functional requirements.
O.CRYPTOGRAPHY The TOE shall provide cryptographic functions to maintain the confidentiality and allow for detection of modification of user data that is transmitted between physically separated portions of the	FCS_CKM.1(1) FCS_CKM.1(2) FCS_CKM.2 FCS_CKM.4 FCS_CKM_(EXT).2 FCS_BCM_(EXT).1 FCS_COP.1(1)	Baseline cryptographic services are provided in the TOE by FIPS PUB 140-2 compliant modules implemented in hardware, in software, or in hardware/software combinations [FCS_BCM_(EXT).1]. The cryptographic services offered by this baseline capability are augmented and customized in the TOE to support medium

Objective	Requirements Addressing the Objective	Rationale
TOE, or outside of the TOE.	FCS_COP.1(2) FCS_COP.1(3) FCS_COP.1(4) FCS_COP_(EXT).1	robustness environments. These TOE services are based primarily upon functional security requirements in the areas of key management and cryptographic operations. In the area of key management there are functional requirements that address the generation of symmetric keys [FCS_CKM.1 (1)], and the generation of asymmetric keys [FCS_CKM.1 (2)]; methods of manual and automated cryptographic key distribution [FCS_CKM.2]; cryptographic key destruction [FCS_CKM.4]; techniques for cryptographic key validation and packaging [FCS_CKM.1]; and cryptographic key handling and storage [FCS_CKM_(EXT).2]. Specific functional requirements in the area of cryptographic operations address data encryption and decryption [FCS_COP.1 (1)]; cryptographic signatures [FCS_COP.1 (2)]; cryptographic hashing [FCS_COP.1 (3)]; cryptographic key agreement [FCS_COP.1 (4)]; and improved random number generation [FCS_COP_(EXT).1].
O.CRYPTOGRAPHY_VALIDATED The TOE will use NIST FIPS 140-1/2 validated cryptomodules for cryptographic services implementing NIST-approved security functions and random number generation services used by cryptographic functions.	FCS_CKM.1(1) FCS_CKM.1(2) FCS_CKM.2 FCS_CKM.4 FCS_CKM_(EXT).2 FCS_BCM_(EXT).1 FCS_COP.1(1) FCS_COP.1(2) FCS_COP.1(3) FCS_COP.1(4) FCS_COP_(EXT).1	Baseline cryptographic services are provided in the TOE by FIPS PUB 140-2 compliant modules implemented in hardware, in software, or in hardware/software combinations [FCS_BCM_(EXT).1]. The cryptographic services offered by this baseline capability are augmented and customized in the TOE to support medium robustness environments. These TOE services are based primarily upon functional security requirements in the areas of key management and cryptographic operations. In the area of key management there are functional requirements that address the generation of symmetric keys [FCS_CKM.1 (1)], and the generation of asymmetric keys [FCS_CKM.1 (2)]; methods of manual and automated cryptographic key distribution [FCS_CKM.2]; cryptographic key destruction [FCS_CKM.4]; techniques for cryptographic key validation and packaging [FCS_CKM.1]; and cryptographic key handling and storage [FCS_CKM_(EXT).2]. Specific functional requirements in the area of cryptographic operations address data encryption and decryption [FCS_COP.1 (1)]; cryptographic signatures [FCS_COP.1 (2)]; cryptographic hashing [FCS_COP.1 (3)]; cryptographic key agreement [FCS_COP.1 (4)]; and improved random number generation [FCS_COP_(EXT).1].

Objective	Requirements Addressing the Objective	Rationale
O.DISPLAY_BANNER The TOE will display an advisory warning regarding use of the TOE prior to permitting the use of any TOE services that require authentication.	FTA_TAB.1	FTA_TAB.1 meets this objective by requiring that the TOE display an administrator defined banner before a user can establish an authenticated session. This banner is under complete control of the administrator, who can specify any warnings regarding unauthorized use of the TOE and remove any product or version information if they desire. The only time that it is envisioned that an authenticated session would need to be established is for the performance of TOE administration. Bannering is not necessary prior to use of services that pass network traffic through the TOE.
O.DOCUMENTED_DESIGN	ADV_FSP.2 ADV_TDS.1	ADV_FSP.2 and ADV_TDS.1 support this objective by requiring that the TOE be developed using sound engineering principles. The use of a high level design and the functional specification ensure that developers responsible for TOE development understand the overall design of the TOE. This in turn decreases the likelihood of design flaws and increases the chance that accidental design errors will be discovered. ADV_TDS.1 and ADV_FSP.2 are also used to ensure that the TOE design is consistent across the Design and the Functional Specification.
O.MANAGE The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FMT_MOF.1(1) FMT_MOF.1(2) FMT_MOF.1(3) FMT_MSA.2 FMT_MTD.1(1) FMT_MTD.1(2) FMT_MTD.1(3) FMT_SMR.1(1) FMT_SMF.1(1) FMT_SMF.1(2) FMT_SMF.1(3)	The FMT requirements are used to satisfy this management objective, as well as other objectives that specify the control of functionality. The requirements' rationale for this objective focuses on the administrator's capability to perform management functions in order to control the behavior of security functions. FMT_MOF.1(1)(2) and (3) ensure that the administrator has the ability manage the cryptographic, audit, and authentication functions. FMT_MSA.2 provides the administrator the ability to accept only secure values and modify security attributes. FMT_MTD.1(1) (2) and (3) ensure that the administrator can manage TSF data. This PP specifically identifies audit preselection, identification, and authentication data. An ST author, may use additional iterations to address TSF data that has not already been specified by other requirements. This is necessary because the ST author may add TSF data in assignments that cannot be addressed a priori by the PP authors.

Objective	Requirements Addressing the Objective	Rationale
		FMT_MTD.1(4) helps satisfy this objective by providing that there be a management function of the Security Administrator or an authorized IT entity that will set the time and date used to provide reliable time stamps to the TOE. FMT_SMR.1 defines the specific security roles to be supported. FMT_SMF.1(1), (2), and (3) support this objective by identifying the management functions for cryptographic data, audit records, and cryptographic key data.
O.MEDIATE The TOE must mediate the flow of information to and from wireless clients communicating via the TOE RF Transmitter/Receiver interface in accordance with its security policy.	FIA_UAU.1 FIA_UAU_(EXT).5 FIA_UID.2 FDP_PUD_(EXT).1	FIA_UAU.1, FIA_UAU_(EXT).5 and FIA_UID.2 ensure that the TOE has the ability to mediate packet flow based upon the authentication credentials of the wireless user. FDP_PUD_(EXT).1 allows the administrator to control whether or not unencrypted data will be allowed to pass through the TOE.
O.PARTIAL_FUNCTIONAL_TESTING The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.	ATE_COV.1 ATE_FUN.1 ATE_IND.2	ATE_FUN.1 requires the developer to provide the necessary test documentation to allow for an independent analysis of the developer's security functional test coverage. In addition, the developer must provide the test suite executables and source code, which the evaluator uses to independently verify the vendor test results and to support of the test coverage analysis activities. ATE_COV.1 requires the developer to provide a test coverage analysis that demonstrates the extent to which the TSFI are tested by the developer's test suite. This component also requires an independent confirmation of the extent of the test suite, which aids in ensuring that correct security relevant functionality of a TSFI is demonstrated through the testing effort. ATE_IND.2 requires an independent confirmation of the developer's test results by mandating that a subset of the test suite be run by an independent party. This component also requires an independent party to craft additional functional tests that address functional behavior that is not demonstrated in the developer's test suite. Upon successful completion of these requirements, the TOE's conformance to the specified security functional requirements will have been demonstrated.

Objective	Requirements Addressing the Objective	Rationale
O.RESIDUAL_ INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.	FDP_RIP.1(1) FCS_CKM_(EXT).2 FCS_CKM.4	FDP_RIP.1 is used to ensure the contents of resources are not available once the resource is reallocated. 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). FCS_CKM_(EXT).2 places requirements on how cryptographic keys are managed within the TOE. This requirement places restrictions in addition to FDP_RIP.1, in that when a cryptographic key is moved from one location to another (e.g., calculated in some scratch memory and moved to a permanent location) that the memory area is immediately cleared as opposed to waiting until the memory is reallocated to another subject. FCS_CKM.4 applies to the destruction of cryptographic keys used by the TSF. This requirement specifies how and when cryptographic keys must be destroyed. The proper destruction of these keys is critical in ensuring the content of these keys cannot possibly be disclosed when a resource is reallocated to a user.
O.SELF_PROTECTION The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure.	ADV_ARC.1	ADV_ARC.1 provides the security architecture description of the security domains maintained by the TSF that are consistent with the SFRs**.** Since self-protection is a property of the TSF that is achieved through the design of the TOE and TSF, and enforced by the correct implementation of that design, self-protection will be achieved by that design and implementation
O.TIME_STAMPS The TOE shall obtain reliable time stamps from the IT Environment and the capability for the administrator to set the time used for these time stamps.	FPT_STM_(EXT).1	FPT_STM_(EXT).1 requires that the TOE be able to obtain 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_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	FIA_AFL.1 FIA_ATD.1(1) FIA_ATD.1(2) FIA_UAU.1 FIA_UAU_(EXT).5	FIA_UID.2 plays a role in satisfying this objective by ensuring that every user is identified before the TOE performs any mediated functions. In most cases, the identification cannot be authenticated (e.g., a user attempting to send a data packet through the TOE that does not require authentication. It is impractical to require authentication of all users that

Objective	Requirements Addressing the Objective	Rationale
	FIA_UID.2 FTA_SSL.3 FTP_TRP1 FTP_ITC_(EXT).1	attempt to send data through the TOE, therefore, the requirements specified in the TOE require authentication where it is deemed necessary. This does impose some risk that a data packet was sent from an identity other than that specified in the data packet. FIA_UAU.1 and FIA_UAU_(EXT).5 contribute to this objective by ensuring that administrators and users are authenticated before they are provided access to the TOE or its services. In order to control logical access to the TOE an authentication mechanism is required. The local administrator authentication mechanism is necessary to ensure an administrator has the ability to login to the TOE regardless of network connectivity (e.g., it would be unacceptable if an administrator could not login to the TOE because the authentication server was down, or that the network path to the authentication server was unavailable). FIA_AFL.1 ensures that the TOE can protect itself and its users from brute force attacks on their authentication credentials. FIA_ATD.1(1) and (2) Management requirements provide additional control to supplement the authentication requirements. FTA_SSL.3 ensures that inactive user and administrative sessions are dropped. FTP_TRP.1 ensures that remote users have a trusted path in order to authenticate. FTP_ITC_(EXT).1 provides a trusted channel for services provided by the TOE IT environment (the remote authentication server)
O.VULNERABILITY_ ANALYSIS The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.	AVA_VAN.2	The **AVA_VAN.2** component provides the necessary level of confidence that vulnerabilities do not exist in the TOE that could cause the security policies to be violated. AVA_VAN.2 requires the evaluator to perform a search for potential vulnerabilities in all the TOE deliverables. For those vulnerabilities that are not eliminated by the developer, a rationale must be provided that describes why these vulnerabilities cannot be exploited by a threat agent with a basic attack potential, which is in keeping with the desired assurance level of this TOE. This component provides the confidence that security flaws do not exist in the TOE that could be exploited by a threat agent of basic attack potential to violate the TOE's security policies. For this TOE, the vulnerability analysis is specified for an attack potential of basic.

Objective	Requirements Addressing the Objective	Rationale
		This requirement ensures the evaluator has performed an analysis of the authentication mechanism to ensure the probability of guessing a user's authentication data would require a medium-attack potential, as defined in Annex B of the CEM.

6.4 Rationale for TOE IT Environment Security Requirements

Table 15: Rationale for Requirements on the TOE IT Environment

Objective	Requirements Addressing the Objective	Rationale
OE.AUDIT_PROTECTION The IT Environment will provide the capability to protect audit information and the authentication credentials.	FAU_SAR.2 FAU_STG.1 FAU_STG.3 FMT_MOF.1 FMT_SMR.1	FAU_SAR.2 restricts the ability to read the audit records to only the administrator. The exception to this is that all administrators have access to the audit record information presented in the alarm indicating a potential security violation. FAU_STG.1restricts the ability to delete or modify audit information to the administrators. The TSF will prevent modifications of the audit records in the audit trail. FAU_STG.3 ensures that the administrator will take actions when the audit trail exceeds pre-defined limits. FMT_MOF.1and FMT_SMR.1specifies the ability of the administrators to control the security functions associated with audit and alarm generation. The ability to control these functions has been assigned to the appropriate administrative roles.
OE.AUDIT_REVIEW The IT Environment will provide the capability to selectively view audit information.	FAU_GEN.1 FAU_SAR.1 FAU_SAR.3	FAU_SAR.1 ensures that the IT environment provides those responsible for the TOE with facilities to review the TOE audit records (e.g., the administrator can construct a sequence of events provided the necessary events were audited). FAU_SAR.3 provides the administrator with the ability to selectively review the contents of the audit trail based on established criteria. This capability allows the administrator to focus their audit review to what is pertinent at that time. FAU_GEN.1ensures that the TOE IT environment will generate appropriate audit events to support the

Objective	Requirements Addressing the Objective	Rationale
		TOE.
OE.MANAGE The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FMT_MOF.1 FMT_SMR.1	FMT_MOF.1 ensures that the TOE IT environment limits access to TSF management functions to the administrator. FMT_SMR.1 ensures that the TOE IT environment provides an administrative role that may be used to manage both the TOE and the IT environment.
OE.NO_EVIL Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.	AGD_OPE.1	The AGD_OPE.1 requirement mandates the developer provide the administrator with guidance on how to operate the TOE in a secure manner. This includes describing the interfaces the administrator uses in managing the TOE and any security parameters that are configurable by the administrator. The documentation (AGD_PRE.1)also provides a description of how to setup and review the auditing features of the TOE.
OE.NO_GENERAL_PURPOSE There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.	A.NO_GENERAL_PURPOSE	It is assumed that there will be no general-purpose computing or storage capabilities available on the TOE therefore no SFR is necessary.
OE.PHYSICAL The IT environment provides physical security, commensurate with the value of the TOE and the data it contains.	A.Physical	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment. Therefore, an extended requirement is not necessary.
OE.PROTECT_MGMT_COMMS The environment shall protect the transport of audit records to the audit server, remote network management, and authentication server communications with the TOE in a manner that is commensurate with the risks posed to the network.	FTP_ITC_(EXT).1	FTP_ITC_(EXT).1 provides a trusted channel for services provided by the TOE IT environment to the TOE (the remote authentication server, syslog server and time server)
OE.RESIDUAL_INFORMATION The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not	FDP_RIP.1	FDP_RIP.1 ensures that the TOE IT environment provides same protections for residual information in a network packet that the TOE will provide. This ensures that neither the TOE nor the TOE IT environment will allow data from previously

Objective	Requirements Addressing the Objective	Rationale
released when the resource is reallocated.		transmitted packets to be insert into new packets.
OE.SELF_PROTECTION The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.	ADV_ARC.1	The TOE IT environment must protect itself in a manner similar to that provided for the TOE. ADV_ARC.1 provides the security architecture description of the security domains maintained by the TSF that are consistent with the SFRs**.** Since self-protection is a property of the TSF that is achieved through the design of the TOE and TSF, and enforced by the correct implementation of that design, self-protection will be achieved by that design and implementation
OE.TOE_ACCESS The environment will provide mechanisms that support the TOE in providing user's logical access to the TOE.	FIA_AFL.1 FIA_ATD.1 FIA_UAU_(EXT).5 FIA_UID.1	The TOE IT environment will provide a remote authentication mechanism in order to support TOE authentication of users. FIA_UAU_(EXT).5 and FIA_UID.1 ensure that users are identified and authenticated. FIA_ATD.1 and FIA_AFL.1ensure that the proper attributes are associated with users and that authentication failure is handled properly.
OE.TOE_NO_BYPASS Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.	FIA_UAU.1 FIA_UAU_(EXT).5 FIA_UID.1	FIA_UAU.1, FIA_UAU_(EXT).5, and FIA_UID.1 ensure that the TOE has the ability to mediate packet flow based upon the authentication credentials of the wireless user.
OE.TIME_STAMPS The TOE IT environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.	FPT_STM.1 FMT_MTD.1(4)	FPT_STM.1 requires that the TOE IT environment be able to provide reliable time stamps for its own use and that of the TOE. 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. FMT_MTD.1(4) helps satisfy this objective by providing that there be a management function of the Security Administrator or an authorized IT entity that will set the time and date used to provide reliable time stamps to the TOE.

6.5 Rationale for Assurance Requirements

EAL2 augmented was chosen to ensure a level of confidence in security services used to protect information in a Basic Robustness Environment. The assurance selection was based on:

- Recommendations documented in the GIG; and
- The postulated threat environment.

The EAL definitions in Part 3 of the CC were reviewed and the *Basic Robustness Assurance Package* (Evaluation Assurance Level (EAL) 2 augmented withALC_FLR.2 (Flaw Remediation) was believed to best achieve this goal. The sponsor concluded that EAL2 augmented is applicable since this PP addresses circumstances where users require a basic level of independently assured security in commercial products. This level of assurance is commensurate with low threat environments or where compromise of protected information will not have a significant impact on mission objectives. This collection of assurance requirements requires TOE developers to gain assurance from good software engineering development practices, which do not require substantial specialist knowledge, skills, and other resources.

The postulated threat environment specified in Section 3 of this PP was used in conjunction with the Information Assurance Technical Framework (IATF) Robustness Strategy guidance to derive the chosen assurance level.

These three factors were taken into consideration and the conclusion was that the basic robustness assurance package was the appropriate level of assurance.

6.6 Satisfaction of Dependencies

Each functional requirement, including extended requirements was analyzed to determine that all dependencies were satisfied. All requirements were then analyzed to determine that no additional dependencies were introduced as a result of completing each operation. With the exception of dependencies related to FMT_MSA.2, all dependencies in this PP have been satisfied.

FMT_MSA.2 is included in this PP as a dependency of the Cryptographic Support family (FCS_COP and FCS_CKM). It is used there to ensure that security attributes related to cryptographic objects (e.g. cryptographic keys) are protected. However, FMT_MSA family is also used to ensure the protection of security attributes related to access control policies (FDP_IFC and FDP_AFC) and includes a dependency upon those Security Functional Requirements. However, this PP does not require that the TOE implement an access control policy and those requirements have not been included in the PP.

6.7 Rationale for Extended requirements

Table 16 presents the rationale for the inclusion of the extended requirements found in this PP.

Table 16: Rationale for Extended Requirements

Extended Requirement	Identifier	Rationale

Extended Requirement	Identifier	Rationale
FCS_BCM_(EXT).1	Baseline cryptographic module	This extended requirement is necessary since the CC does not provide a means to specify a cryptographic baseline of implementation.
FCS_CKM_(EXT).2	Cryptographic key handling and storage	This extended requirement is necessary since the CC does not specifically provide components for key handling and storage.
FCS_COP_(EXT).1	Random number generation	This extended requirement is necessary since the CC cryptographic operation components address only specific algorithm types and operations requiring specific key sizes.
FDP_PUD_(EXT).1	Protection of User Data	This extended requirement is necessary because the Common Criteria IFC/AFC requirements do not accommodate access control policies that are not object/attribute based. The FDP_PUP_(EXT).1 requirement allows the administrator allow or disallow access based upon an administrator setting indicating whether or not unencrypted data may transit the wireless LAN.
FIA_UAU_(EXT).5	Multiple authentication mechanisms	This extended requirement is needed for local administrators because there is concern over whether or not existing CC requirements specifically **require** that the TSF provide authentication. Authentication provided by the TOE is implied by other FIA_UAU requirements and is generally assumed to be a requirement when other FIA_UAU requirements are included in a TOE. In order to remove any potential confusion

Extended Requirement	Identifier	Rationale
		about this PP, an extended requirement for authentication has been included. This PP also requires the IT environment to provide an authentication server to be used for authentication of remote users. It is important to specify that the TSF must provide the means for local administrator authentication in case the TOE cannot communicate with the authentication server. In addition, the TOE must provide the portions of the authentication mechanism necessary to obtain and enforce an authentication decision from the IT environment.
FPT_TST_(EXT).1	TSF Testing	This extended requirement is necessary to divide the TOE testing requirements between those necessary for the TOE itself and those specific to FIPS 140 cryptomodules.
FTP_ITC_(EXT).1	Inter-TSF trusted channel	This extended requirement is necessary because the existing trusted channel requirement is written with the intent of protecting communication between distributed portions of the TOE rather than between the TOE and its trusted IT environment.

Appendix A. Acronyms

AES	Advanced Encryption Standard
AP	Access Point
ASCII	American Standard Code for Information Interchange
CC	Common Criteria
CM	Configuration Management
COTS	Commercial Off-The-Shelf
DoD	Department of Defense
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
GIG	Global Information Grid
HARA	High-Assurance Remote Access
I&A	Identification and Authentication
IATF	Information Assurance Technical Framework
IGS	Installation Generation Startup
ISSE	Information System Security Engineers
IT	Information Technology
NIST	National Institute of Standards and Technology
OS	Operating System
PKI	Public Key Infrastructure
PP	Protection Profile
PUB	Publication
RF	Radio Frequency
SBU	Sensitive But Unclassified
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network

Appendix B. Terminology

In the CC, Section 2.3 of Part 1 defines many terms. In addition to terms defined in the CC, this PP references the following defined terms.

Access -- Interaction between an entity and an object that results in the flow or modification of data.

Access Control -- Security service that controls the use of resources[4] and the disclosure and modification of data.[5]

Access System --Equipment that provides the interface between mobile clients and the wired network.

Accountability -- Property that allows activities in an IT system to be traced to the entity responsible for the activity.

Administrator -- A user who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TSP. Administrators may possess special privileges that provide capabilities to override portions of the TSP.

Attack -- An intentional act attempting to violate the security policy of an IT system.

Audit Server -- A central location where audit events/records are stored.

Authentication -- Security measure that verifies a claimed identity.

Authentication credentials -- Information used to verify a claimed identity.

Authentication Server -- A central location where the users and administrators authentication credentials are stored.

Authorization -- Permission, granted by an entity authorized to do so, to perform functions and access data.

Availability -- Timely[6], reliable access to IT resources.

Compromise -- Violation of a security policy.

Confidentiality -- A security policy pertaining to disclosure of data.

Critical Security Parameters (CSP) -- Security-related information (e.g., cryptographic keys, authentication data such as passwords and pins, and cryptographic seeds) appearing in plaintext or otherwise unprotected form and whose

[4] Hardware and software.
[5] Stored or communicated.
[6] According to a defined metric.

disclosure or modification can compromise the security of a cryptographic module or the security of the information protected by the module.

Cryptographic boundary -- An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.

Cryptographic key (key) -- A parameter used in conjunction with a cryptographic algorithm that determines [7]:

- the transformation of plaintext data into cipher text data,
- the transformation of cipher text data into plaintext data,
- a digital signature computed from data,
- the verification of a digital signature computed from data, or
- a digital authentication code computed from data.

Cryptographic Module -- The set of hardware, software, and/or firmware that implements FIPS Approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.

Cryptographic Module Security Policy -- A precise specification of the security rules under which a cryptographic module must operate, including the rules derived from the requirements of this PP and additional rules imposed by the vendor.

Discretionary Access Control (DAC) -- A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. These controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Embedded Cryptographic Module -- A Cryptographic Module that is built as an integral part of a larger and more general surrounding system (i.e., one that is not easily removable from the surrounding system).

Enclave -- A collection of entities under the control of a single authority and having a homogeneous security policy. They may be logical, or may be based on physical location and proximity.

Entity -- A subject, object, user, or another IT device, which interacts with TOE objects, data, or resources.

Event Type -- For the purposes of this Protection Profile, event type is defined to be the severity level indicator as it is defined in section 4.1.1 or IETF RFC 3146 *The BSD syslog Protocol.*

External IT entity -- Any trusted Information Technology (IT) product or system, outside of the TOE, which may, in accordance with the TSP, perform an operation.

Integrity -- A security policy pertaining to the corruption of data and TSF mechanisms.

MAC Address -- Media Access Control Address, the globally unique 48 bit media layer address of a network device. Sometimes referred to as the physical address.

Operating Environment -- The total environment in which a TOE operates. It includes the physical facility and any physical, procedural, administrative and personnel controls.

Operating System (OS) -- An entity within the TSC that causes operations to be performed. Subjects can come in two forms: trusted and untrusted. Trusted subjects are exempt from part or all of the TOE security policies. Untrusted subjects are bound by all TOE security policies.

Robustness -- A characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly. DoD has three levels of robustness:

- **Basic:** Security services and mechanisms that equate to good commercial practices. Basic robustness equates to EAL-2 plus; ALC_FLR (Flaw Remediation).

- **Medium:** Security services and mechanisms that provide for layering of additional safeguards above good commercial practices. Medium robustness equates to EAL-4 plus; as documented in the Protection Profile Medium Robustness Consistency Guidance.

- **High:** Security services and mechanisms that provide the most stringent protection and rigorous security countermeasures.

Secure State -- Condition in which all TOE security policies are enforced.

Threat -- Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.

Threat Agent - Any human user or Information Technology (IT) product or system, which may attempt to violate the TSP and perform an unauthorized operation with the TOE.

TOE Security Function (TSF) Data -- Information used by the TSF in making TOE security policy (TSP) decisions. TSF data may be influenced by users if allowed by the TSP. Security attributes, authentication data, and access control list entries are examples of TSF data.

Unauthorized User -- Any person who is not authorized, under the TSP, to access the TOE. This definition authorized users who seek to exceed their authority.

User -- Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Vulnerability -- A weakness that can be exploited to violate the TOE security policy.

Wireless Client -- A device consisting of hardware and software used to provide a wirelessly interface to communicate with other wireless devices

---

i A deletion of CC text was performed in FPT_TST.1.1(1). Rationale: The word "TSF" was deleted to allow for the demonstration of the correct operation of a number of cryptographic related self tests.

FPT_TST.1.1(1) **Refinement:** The TSF shall run a suite of self-**tests in accordance with FIPS PUB 140-2, Level 4 (as identified in Table 5.3)** during initial start-up **(on power on)**, at the request of the **cryptographic administrator (on demand)**, **under various conditions,** and periodically **(at least once a day)** to demonstrate the correct operation of the ~~TSF~~ **following …**

ii A deletion of CC text was performed in FPT_TST.1.2(2). Rationale: The word "users" was deleted to replace it with the role of " cryptographic administrator". "Only authorized cryptographic administrators should be given the capability to verify the integrity of cryptographically related TSF data.

FPT_TST.1.2(1) **Refinement:** The TSF shall provide authorized ~~users~~ **cryptographic administrators** with the capability to verify the integrity of **TSF data related to the cryptography by using TSF-provided cryptographic functions.**.

iii A deletion of CC text was performed in FPT_TST.1.3(1). Rationale: The word “users” was deleted to replace it with the role of " cryptographic administrator". Only authorized cryptographic administrators should be given the capability to verify the integrity of cryptographically related TSF executable code.

FPT_TST.1.3(1) **Refinement:** The TSF shall provide authorized ~~users~~ **cryptographic administrators** with the capability to verify the integrity of stored **cryptographically related** TSF executable code.

iv A deletion of CC text was performed in FPT_TST.1.1(2). Rationale: The words "the TSF" was deleted to allow for the demonstration of the correct operation of each key generation component. The word “perform” replaced “run a suite of” for clarity and better flow of the requirement.

FPT_TST.1.1(2) **Refinement:** The TSF shall ~~run a suite of~~ **perform** self-tests **immediately after generation of a key** to demonstrate the correct operation of ~~the TSF~~ **each key generation component**. **If any of these tests fails, that generated key shall not be used, the cryptographic module shall react as required by FIPS PUB 140 for failing a self-test, and this event will be audited.**

v A deletion of CC text was performed in FPT_TST.1.2(2). Rationale: The word "users" was deleted to replace it with the role of "cryptographic administrator".

FPT_TST.1.2(2) **Refinement:** The TSF shall provide authorized ~~users~~ **cryptographic administrators** with the capability to verify the integrity of TSF data **related to the key generation**.

vi A deletion of CC text was performed in FPT_TST.1.3(2). Rationale: The word “users” was deleted to replace it with the role of "cryptographic administrator".

FPT_TST.1.3(2) **Refinement:** The TSF shall provide authorized ~~users~~ **cryptographic administrators** with the capability to verify the integrity of stored TSF executable code **related to the key generation**.