DRAFT

Peer-to-Peer
Wireless Local Area Network (WLAN)
for
Sensitive But Unclassified Environments
Protection Profile

Version 0.6

28 September 2001

Prepared By: Booz·Allen & Hamilton and
Tresys Technology

Prepared For: Department of Defense

Disclaimer

This is a work in-progress document and subject to change. This draft document is not an official DoD document and its content is not binding until officially approved.

DRAFT

Foreword

This Protection Profile (PP) was written by Booz·Allen & Hamilton, National Security Team, and Tresys Technology to support the Information Assurance Solutions Group. Please send comments on this PP to Brian Green at Booz·Allen & Hamilton, 900 Elkridge Landing Road, Linthicum, MD 21090.

Table of Contents

FOREWORD ..... **I**

TABLE OF CONTENTS ..... **II**

LIST OF TABLES AND FIGURES ..... **IV**

CONVENTIONS AND TERMINOLOGY ..... **V**

CONVENTIONS V
TERMINOLOGY VIII

DOCUMENT ORGANIZATION ..... **IX**

1. INTRODUCTION **1**

1.1 IDENTIFICATION 1
1.2 PROTECTION PROFILE OVERVIEW 1
1.3 RELATED PROTECTION PROFILES 2

2. TOE DESCRIPTION **3**

3. TOE SECURITY ENVIRONMENT **4**

3.1 SECURE USAGE ASSUMPTIONS 5
3.2 THREATS TO SECURITY 6
3.3 ORGANIZATIONAL SECURITY POLICIES 7

4. SECURITY OBJECTIVES **8**

4.1 SECURITY OBJECTIVES FOR THE TOE 8
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT 9

5. IT SECURITY REQUIREMENTS **12**

5.1 SECURITY FUNCTIONAL REQUIREMENTS 12
5.1.1 Strength of Function Claims 12
5.1.2 Identification of Standards Compliance Methods 12
5.1.3 TOE Security Functional Requirements 12
5.2 TOE SECURITY ASSURANCE REQUIREMENTS 19
5.2.1 Authorization Controls (ACM_CAP.3) 19
5.2.2 TOE CM Coverage (ACM_SCP.1) 20
5.2.3 Delivery Procedures (ADO_DEL.1) 21
5.2.4 Installation, Generation, and Startup Procedures (ADO_IGS.1) 21
5.2.5 Informal Functional Specification (ADV_FSP.1) 22
5.2.6 Security Enforcing High-Level Design (ADV_HLD.2) 22
5.2.7 Informal Correspondence Demonstration (ADV_RCR.1) 23
5.2.8 Administrator Guidance (AGD_ADM.1) 23
5.2.9 User Guidance (AGD_USR.1) 24
5.2.10 Identification of Security Measures (ALC_DVS.1) 25
5.2.11 Analysis of Coverage (ATE_COV.2) 25
5.2.12 Testing: High-Level Design (ATE_DPT.1) 26
5.2.13 Functional Testing (ATE_FUN.1) 26
5.2.14 Independent Testing—Sample (ATE_IND.2) 27
5.2.15 Examination of Guidance (AVA_MSU.1) 27
5.2.16 Strength of TOE Security Function Evaluation (AVA_SOF.1) 28
5.2.17 Developer Vulnerability Analysis (AVA_VLA.1) 29

6. RATIONALE 30

6.1 SECURITY OBJECTIVES RATIONALE 30
6.2 SECURITY REQUIREMENTS RATIONALE 35
6.2.1 TOE Assurance Requirements 35
6.2.2 Dependencies Not Met 35
6.2.3 Strength of Function Rationale 36
6.2.4 Traceability 36
6.2.5 Suitability 37

7. REFERENCES 41

APPENDIX A. ACRONYMS 1

List of Tables and Figures

Table 1. Functional Requirements Operation Conventions v
Table 2. TOE Assumptions 5
Table 3. Threats 6
Table 4. Organizational Security Policies 7
Table 5. Security Objectives for the TOE 8
Table 6. Security Objectives for the Environment 9
Table 7. TOE Security Functional Requirements 12
Table 8. TOE Assurance Requirements 19
Table 9. Security Objectives Justification 30
Table 10. Mapping of Requirements to Security Objectives 36

Figure 2. Peer-to-Peer WLAN Topology 3

Conventions and Terminology

Conventions

Except for replacing United Kingdom spelling with American spelling (at the client's request), the notation, formatting, and conventions used in this PP are consistent with version 2.1 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the PP reader.

The CC permits four functional component operations—assignment, iteration, refinement, and selection—to be performed on functional requirements. These operations are defined in CC, Part 2, paragraph 2.1.4 as

- Assignment: allows the specification of an identified parameter
- Iteration: allows a component to be used more than once with varying operations
- Refinement: allows the addition of details
- Selection: allows the specification of one or more elements from a list.

With the exception of iteration, these operations are expressed by using bolded, italicized, and underlined text. The author used brackets ("[]") to set off all assignments or selections that require future action by the developer to prepare a Security Target (ST). The text "ST Assignment:" or "ST Selection:" is indicated within the brackets. Iterations are not used in this PP.

Table 1. Functional Requirements Operation Conventions

Convention	Purpose	Operation
Bold	Bolded text alerts the reader that additional text has been added to the CC. Example: The TSF shall export **(in ASCII format)** the **labeled** user data with the user data's associated security attributes.	Assignment Refinement
Italics	Italicized text informs the reader of an appended assignment or selection operation to be completed by the developer. Example: The TSF shall provide the following [ST Assignment: *list of additional SFP capabilities*].	Assignment Selection

Convention	Purpose	Operation
Parentheses	Parentheses and an iteration number inform the reader that the author has selected a new field of assignments or selections with the same requirement and that the requirement will be used multiple times. Example: Basic data exchange confidentially (Iteration 1) The TSF shall enforce the **[policies P.ADMIN ACCESS and P.USER ACCESS]** to be able to transmit objects in a manner protected from unauthorized disclosure. Basic data exchange confidentially (Iteration 2) The TSF shall enforce the **[policies P.ADMIN ACCESS and P.USER ACCESS]** to be able to receive objects in a manner protected from unauthorized disclosure.	Iteration
Underline	Underlined text informs the reader that a choice was made from a list provided by the CC selection operation statement. Example: The TSF shall be able to prevent modifications to the audit records.	Selection

Application notes provide support information that is considered relevant or useful for the construction, evaluation, or use of the target of evaluation (TOE). Application notes clarify the intent of a requirement, identify implementation choices, or define "pass-fail" criteria for a requirement. Application notes follow the relevant requirement component, are directive in nature, and may amplify the CC terminology stated in a specific requirement.

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.

ST Assignments: Assignments left to the ST author are annotated as "ST Assignment." When submitting a ST against this PP, ST authors should complete these assignments as appropriate for their particular product.

ST Selections: Selections left to the ST author are annotated as "ST Selection." When submitting a ST against this PP, ST authors should complete these selections as appropriate for their particular product.

Terminology

In the CC, Section 2.3 of Part 1 defines many terms. In addition to terms defined in the CC, the PP uses the following defined terms. The sensitive but unclassified (SBU) wireless local area network (WLAN) TOE consists of a wireless device (desktop or portable) with client software, a broadcast radio, and a receiving antenna.

Agent — An individual who is not an authorized user of the TOE.

Authorized administrator — Any person who has the authority and responsibility for the long-term health of the security attributes of the system, or the defined role. Administrators can initiate, modify, view, and delete security attributes.

Authorized users — Any person who is authorized to access the TOE and who has successfully authenticated to the TOE, or the defined role.

Enclave — The secure, fixed facility that shelters and supports an information technology (IT) environment on behalf of an organization. It contains an assortment of physical and electronic security mechanisms for authentication and access control.

Mobile client — An equipment item that is easily man-portable used to wirelessly connect with an organization's network.

Object — An entity within the TOE scope of control (TSC) that contains or receives information and upon which subjects perform operations.

Radio — a device that sends data over a radio frequency (RF) signal.

Subject — An entity within the (TSC) that causes operations to be performed.

System resources — Any system assets (data and software) required for the correct operation of 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 includes agents and authorized users who seek to exceed their authority.

User data — Data created by and for the authorized user that does not affect the operation of the TSP. User data are the files that a user might upload or download to other remote units or the secure enclave. User data is separate from the TSF data, which has security attributes associated with it and the system data.

User resources — Any data supplied by authorized users.

Document Organization

Section 1 provides the introductory material for the PP.

Section 2 describes the SBU WLAN (i.e., the TOE for this PP) and its general purpose.

Section 3 describes the expected environment for the Peer-to-Peer SBU WLAN. This section defines—

- Secure-use assumptions that describe the presumptive conditions for secure use in the selected environment
- Threats that are to be addressed by either the technical countermeasures implemented in the Peer-to-Peer SBU WLAN hardware or software or through the environmental controls
- Organizational policies that levy further requirements for secure operations.

Section 4 defines the security objectives for the Peer-to-Peer SBU WLAN and its environment.

Section 5 contains the functional and assurance requirements derived from the CC, Parts 2 and 3, respectively, that must be satisfied by the Peer-to-Peer SBU WLAN technology and development teams, respectively.

Section 6 provides a rationale to demonstrate explicitly that the information technology security objectives satisfy the policies and threats. Arguments are provided for the security objectives being necessary to support policies and counter threats. The section then explains how 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. Next, Section 6 provides arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the PP requirements.

Section 7, Reference, identifies background material.

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

1. Introduction

This Protection Profile (PP) supports future Department of Defense (DoD) procurements of commercial off-the-shelf (COTS) peer-to-peer wireless local area networks (WLAN) that will be used in sensitive but unclassified (SBU) environments.[1] This PP details the policies, assumptions, threats, security objectives, security functional requirements, and security assurance requirements for the SBU WLAN and its environment. These are the consolidated security requirements for the DoD for procurement of any SBU WLAN.

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

1.1 Identification

Title:	Peer-to-Peer Wireless Local Area Network (WLAN) For Sensitive But Unclassified Environments Protection Profile
Authors:	Brian Green and Erik Williams, Booz·Allen & Hamilton; Jandria Alexander, Kimberly Caplan, and Mike Hale, Tresys Technology.
Vetting Status:	Draft
CC Version	2.1
Evaluation Level:	Evaluation Assurance Level (EAL) 3
General Status:	Draft
Registration:	TBD
Keywords:	Sensitive but unclassified, SBU, radio, medium assurance, wireless, network, wireless local area network, wireless LAN, WLAN, LAN

1.2 Protection Profile Overview

This PP specifies the DoD's information security needs for a SBU WLAN configured as a peer-to-peer network. The architecture assumed is one in which all components on the network may directly communicate among themselves. No central hub or access point is required. This PP requires privacy and integrity of communications over the WLAN using commercially available cryptographic algorithms. Security administration is the

[1] Sensitive But Unclassified information is meant to be information of Medium Value, as defined in Section 1.3.4.3 of the X.509 Certificate Policy for the United States Department of Defense, version 5.0, dated 13 December 1999.

responsibility of the user of each component (i.e., client). The assurance requirements specified in the PP are EAL 3.

1.3 Related Protection Profiles

Infrastructure Wireless Local Area Network (WLAN) for Sensitive But Unclassified Environments Protection Profile [2].

2. TOE Description

The Target of Evaluation (TOE) is a peer-to-peer WLAN where devices communicate directly with one another. Peers communicate directly with one another using wireless communication protocols. The security requirements for a peer-to-peer WLAN are limited to data communications integrity, privacy, and nonrepudiation. Privacy and integrity of communication are implemented using cryptography. The TOE is limited to the hardware and/or software that provides the security services between the peers.

In a peer-to-peer WLAN, no access points exist to authenticate clients attempting to join the network. In addition, there is no central administrator for the entire network. Instead, the users of the peer-to-peer WLAN are responsible for administrating the network and must follow physical security and procedures to control access to the components and the cryptographic keys.

The TOE consists of the software and hardware (e.g., personal computer [PC] cards) on each client that constitute the WLAN application. The hardware platform (e.g., handheld PC, notebook computer) and the operating system are not part of the TOE.

The user on the WLAN will use a public key infrastructure (PKI) and Class 3 or Class 4, X.509 certificates to provide digital signature of transmitted data and to perform secure establishment of symmetric session keys between clients. The PKI used is considered to be outside the TOE but part of the TOE environment.

Figure 1 shows a simple peer-to-peer WLAN topology.

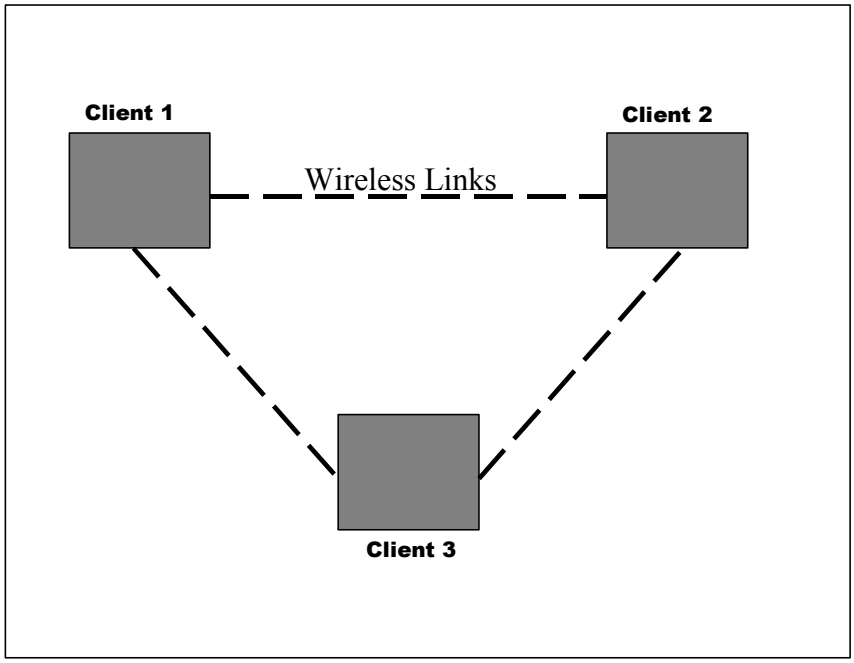

Figure 1. Peer-to-Peer WLAN Topology

3. TOE Security Environment

The peer-to-peer WLANs specified within this PP are intended for environments that process up to SBU traffic. In an SBU 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. In the peer-to-peer WLAN environment, the user organization controls the wireless infrastructure and does not rely on a service provider for WLAN operation.

Unlike an infrastructure WLAN configuration in which an access point is connected to an established wired network, the peer-to-peer WLAN location is typically temporary with clients in proximity to each other. The user of each client is responsible for ensuring the WLAN is used in an environment suitable for SBU processing.

Cryptographic modules suitable for protecting SBU information must comply with Federal Information Processing Standard Publication (FIPS PUB) 140-1, 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.

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, which are assumptions that support secure use of the WLAN. Threats are countered by the security objectives. Policies support the security objectives and are employed 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 2 identifies the conditions that are assumed to exist in the operational environment.

Table 2. TOE Assumptions

Name	Assumption
A.OPERATING_SYS	The underlying information technology (IT) environment of the TOE does not contain vulnerabilities that undermine the secure operation of the TOE.
A.ADMINISTRATION	Authorized users are trusted, competent, and trained to manage the security features of the TOE.
A.NO_USER_DATA	The TOE is strictly a conduit for information flow through radio frequency (RF) transmission and does not provide user data storage capability.
A.CO_LOCATED	TOE components (clients) are sufficiently co-located as required to accommodate communication ranges.
A.CONFIGURATION	The TOE will not be interconnected to a wired network.
A.ENVIRON	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low to medium.
A.PHYSICAL	Each TOE component is physically protected from unauthorized physical access.
A.PKI	Within the IT environment, a PKI provides valid Class 3 or 4, X.509 certificates.

3.2 Threats to Security

The threats listed in Table 3 are general. Threats are actions that may have an adverse affect on the peer-to-peer SBU WLAN or mission. Exposure of wireless communications in the RF transmission environment introduces unique threats to the WLAN. With WLANs, an adversary no longer requires physical access to the network in order to exploit a wireless system. The WLAN is susceptible to over-the-air signal intercept, spoofing, and jamming attacks. Given the assumptions, the threats identified exclude those that would be considered a sophisticated attack (i.e., intentional jamming, traffic analysis).

Table 3. Threats

Name	Threat
T.SIGNAL_DETECT	An unauthorized user detects and intercepts signals transmitted from the TOE to obtain user data.
T.JAM_INTERFERE	Non-TOE generated signals in the area unintentionally interfere and disrupt TOE transmissions.
T.HACK_ACCESS	An unauthorized user gains access to parts of the TOE as a result of missing and weak identification controls.
T.SPOOFING	An attacker uses RF signal paths to masquerade as a valid user or to deliver spurious messages.
T.HACK_MSG_CONTENT	A hacker modifies information intercepted from the RF communication link between two unsuspecting entities before passing it on, thereby deceiving the intended recipient.

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 identifies the organizational security policies applicable to the peer-to-peer SBU WLAN.

Table 4. Organizational Security Policies

Name	Policy
P.ACCOUNT	Authorized users must be held accountable for security-relevant actions.
P.COMPLY	The implementation and use of the TOE must comply with all applicable laws, regulations, and guidelines imposed on the organization for an SBU environment.
P.USAGE	The TOE must be used for only authorized purposes.
P.GUIDANCE	Guidance must be provided for the secure installation and use of the system.
P.CRYPTO	Encryption used to protect user data and the associated cryptographic module must comply, at a minimum, with FIPS 140-1 (Level 2).
P.PKI	Class 3 or 4, X.509 certificates shall be used to establish session keys and to digitally sign transmitted data.

4. Security Objectives

4.1 Security Objectives for the TOE

Table 5 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.

Table 5. Security Objectives for the TOE

Name	TOE Security Objective	Corresponding Threat or Policy
O.ACCESS	The TOE shall control access to information that is subject to the TOE security policy, based on the identity of the individuals, such that this policy cannot be bypassed in the TOE.	T.HACK_ACCESS
O.IDENTITY	The TOE will uniquely identify each user of the system. The TOE will associate each user-requested action with the identity of the user who initiated the session (i.e., log on). The TOE will restrict the actions a user may perform before the TOE verifies the identity of the user.	T.SPOOFING T.HACK_ACCESS
O.CRYPTO	The TOE shall use Class 3 or 4, X.509 certificates and support cryptographic functions in a secure manner with sufficient strength for SBU information. The certificates shall be used to establish session keys and to digitally sign transmitted data.	P.CRYPTO P.PKI
O.DATA_PRO	Encryption will be used to provide confidentiality and integrity of TOE security functions (TSF) and user data in transit between parts of the TOE.	T.SIGNAL_DETECT T.HACK_ACCESS T.HACK_MSG_CONTENT T.SPOOFING P.CRYPTO

Name	TOE Security Objective	Corresponding Threat or Policy
O.EXCHANGE	The TOE will ensure that the system correctly exchanges security-attribute information with distributed components of the TOE.	T.SPOOFING
O.MANAGE	The TOE will provide adequate management features for its security functions.	P.USAGE
O.ENVIRONMENT	The TOE must protect itself against compromise by having a structure that neither reveals security information nor operates in an insecure manner when exposed to signal interference.	T.JAM_INTERFERE
O.DOC	Guidance documentation provided to authorized users will detail the proper installation and use of the TOE to minimize the security risks within the environment.	P.GUIDANCE
O.EAL	The TOE must be tested, structurally shown to be resistant to obvious vulnerabilities, and documented with sufficient design, test, configuration, and life-cycle documentation.	P.COMPLY

4.2 Security Objectives for the Environment

The assumptions identified in Section 3.1 are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures. Table 6 identifies the security objectives for the environment.

Table 6. Security Objectives for the Environment

Name	TOE Security Objective	Corresponding Assumption, Threat, or Policy
OE.ADMIN	Authorized users are trustworthy and follow all administrator guidance.	A.ADMINISTRATION P.USAGE

Name	TOE Security Objective	Corresponding Assumption, Threat, or Policy
OE.OPERATING_SYS	The IT environment must be implemented, installed, and operated in a manner that does not undermine the secure operation of the TOE.	A.OPERATING_SYS
OE.TRAIN	Authorized users are trained to perform assigned duties and follow TOE security practices and procedures (e.g., safeguarding passwords).	A.ADMINISTRATION P.USAGE
OE.INSTALL	Those responsible for the administration of the TOE will ensure the TOE is delivered, installed, managed, and operated in a manner that maintains IT security objectives.	A.NO_USER_DATA A.CO_LOCATED A.CONFIGURATION
OE.PHYSICAL	TOE users must ensure that the TOE is protected from unauthorized physical access.	A.PHYSICAL
OE.LOWEXP	Those responsible for the administration of the TOE will ensure that the TOE is used in an environment in which the threat of malicious attacks is considered low.	A.ENVIRON
OE.PKI	Those responsible for the administration of the TOE will ensure that the TOE uses a PKI that provides valid Class 3 or 4, X.509 certificates.	A.PKI
OE.COMPLY	Those responsible for the administration of the TOE will ensure that the TOE is compliant with applicable laws and regulations imposed on the organization.	P.COMPLY

Name	TOE Security Objective	Corresponding Assumption, Threat, or Policy
OE.ACCOUNT	Those responsible for the administration of the TOE will maintain records of users assigned WLAN components.	P.ACCOUNT

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 an EAL containing assurance components from Part 3 of the CC.

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This section provides information related to the TOE's Security Functional Requirements (SFR). The first subsection addresses strength of function claims. The second subsection identifies standards compliance methods for the cryptographic SFRs included in this PP. The third subsection specifies the SFRs.

5.1.1 Strength of Function Claims

The statement of the TOE security requirements must include a minimum strength level for the TOE security functions realized by a probabilistic or permutational mechanism, except for cryptographic functions. In the case of this PP, this minimum level shall be SOF-basic.

5.1.2 Identification of Standards Compliance Methods

For this PP, cryptographic operations and key management functions must meet FIPS 140-1 (Level 2). The designated approval authority of the TOE-user organization will specify the methodology used to show compliance to FIPS 140-1 standards. Authorized certificates used by a PP-compliant TOE must be DoD PKI Class 3 or 4, X.509 certificates.

5.1.3 TOE Security Functional Requirements

The SFRs for the TOE consist of the following components from Part 2 of the CC, summarized in Table 7. All dependencies among the SFRs are satisfied by the inclusion of the relevant requirement within the TOE security requirements.[2]

Table 7. TOE Security Functional Requirements

Functional Component		Dependencies
FCO_NRO.1	Selective proof of origin	FIA_UID.1
FCS_CKM.1	Cryptographic key generation	FCS_COP.1; FCS_CKM.4; FMT_MSA.2
FCS_CKM.4	Cryptographic key destruction	FCS_CKM.1; FMT_MSA.2
FCS_COP.1	Cryptographic operation	FCS_CKM.1; FCS_CKM.4; FMT_MSA.2
FDP_IFC.2	Complete information flow control	FDP_IFF.1

[2] FMT_MSA.2 is dependent on ADV_SPM.1. FMT_MSA.1, FMT_MSA.2, and FMT_MSA.3 all are dependent on FMT_SMR.1. Section 6 provides the rationale excluding ADV_SPM.1 and FMT_SMR.1.

Functional Component		Dependencies
FDP_IFF.1	Simple security attributes	FDP_IFC.1; FMT_MSA.3
FDP_ITT.1	Basic internal transfer protection	FDP_IFC.1
FDP_ITT.3	Integrity monitoring	FDP_IFC.1; FDP_ITT.1
FIA_ATD.1	User attribute definition	None
FIA_UID.2	User identification before any action	None
FIA_USB.1	User-subject binding	FIA_ATD.1
FMT_MSA.1	Management of security attributes	FDP_IFC.1; FMT_SMR.1
FMT_MSA.2	Secure security attributes	ADV_SPM.1; FDP_IFC.1; FMT_MSA.1; FMT_SMR.1
FMT_MSA.3	Static attribute initialization	FMT_MSA.1; FMT_SMR.1
FPT_ITT.1	Basic internal TSF data transfer protection	None
FPT_SEP.1	TSF domain separation	None
FPT_RVM.1	Nonbypassability of the TSP	None

5.1.3.1 FCO_NRO.1 Selective proof of origin

Hierarchical to: No other components.

FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted **data** at the request of the recipient.

FCO_NRO.1.2 The TSF shall be able to relate the **digital signature** of the originator of the information and the **transmitted data** of the information to which the evidence applies.

FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to the recipient given **a valid X.509 certificate.**

Dependencies:
FIA_UID.1 Timing of identification

5.1.3.2 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a **FIPS 140-1 compliant** cryptographic key generation algorithm] and specified cryptographic key sizes **of 128 bits** that meet the following: **FIPS 140-1 standards**.

Dependencies:

FCS_COP.1 Cryptographic operation
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.1.3.3 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a cryptographic key destruction method that meets the following:
a) FIPS PUB 140-1;
b) zeroization of all plaintext cryptographic keys and all other critical security parameters within the device shall be immediate and complete; and
c) upon each issuance of the zeroization, the destruction shall be executed by overwriting the key/critical security parameter storage area three or more times with an alternating pattern.

Dependencies:

FCS_CKM.1 Cryptographic key generation
FMT_MSA.2 Secure security attributes

5.1.3.4 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform **data encryption** in accordance with a specified cryptographic algorithm **RC4** and cryptographic key sizes **128 bits** that meet the following: **FIPS 140-1**.

Dependencies:

FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.1.3.5 FDP_IFC.2 Complete information flow control

Hierarchical to: FDP_IFC.1

FDP_IFC.2.1 The TSF shall enforce the **WIRELESS SFP** on **all clients and data flows between them** and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.

Dependencies:
FDP_IFF.1 Simple security attributes

5.1.3.6 FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1 The TSF shall enforce the **WIRELESS SFP** based on the following types of subject and information security attributes: **fields in the X.509 certificate**.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:**a) for each operation, there shall be a rule, or rules, where the security attributes of the subject correspond to the information flow control attributes of the object, and**
b) for each operation, there shall be a default rule that is used when the subject security attributes do not correspond to the object security attributes.

FDP_IFF.1.3 The TSF shall enforce the following additional information flow control SFP rules: **None**.

FDP_IFF.1.4 The TSF shall provide the following additional SFP capabilities: **None**.

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules:**None**.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: **None**.

Dependencies:

FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

Application Note:
The ST author defines the WIRELESS SFP by making assignments for the FDP_IFF.1.x requirements.

5.1.3.7 FDP_ITT.1 Basic internal transfer protection

Hierarchical to: No other components.

FDP_ITT.1.1 The TSF shall enforce the **WIRELESS SFP** to prevent the disclosure, loss of user data when it is transmitted between physically separated parts of the TOE.

Dependencies:

FDP_IFC.1 Subset information flow control

5.1.3.8 FDP_ITT.3 Integrity monitoring

Hierarchical to: No other components.

FDP_ITT.3.1 The TSF shall enforce the **WIRELESS SFP** to monitor user data transmitted between physically separated parts of the TOE for the following errors: **integrity errors**.

FDP_ITT.3.2 Upon detection of a data integrity error, the TSF shall **record the error in the audit logs, delete the data in error, and request retransmission**.

Dependencies:

FDP_IFC.1 Subset information flow control
FDP_ITT.1 Basic internal transfer protection

5.1.3.9 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following **minimum** list of security attributes belonging to individual users: **X.509 certificates**.

Dependencies: No dependencies

5.1.3.10 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

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

Dependencies: No dependencies

5.1.3.11 FIA_USB.1 User-subject binding

Hierarchical to: No other components.

FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

Dependencies:
FIA_ATD.1 User attribute definition

5.1.3.12 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the **WIRELESS SFP** to restrict the ability to modify **the value of the object** security attributes to **authorized administrators and owners of the object**.

Dependencies:

FDP_IFC.1 Subset information flow control
FMT_SMR.1 Security roles

5.1.3.13 FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

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

Dependencies:

ADV_SPM.1 Informal TOE security policy model
FDP_IFC.1 Subset information flow control
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

5.1.3.14 FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the **WIRELESS SFP** to provide restrictive default values for security attributes that are used to enforce the *SF*P.

FMT_MSA.3.2 The TSF shall allow the **authorized user** to specify alternative initial values to override the default values when an object or information is created.

Dependencies:

FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

5.1.3.15 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure and modification when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies

5.1.3.16 FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

5.1.3.17 FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

5.2 TOE Security Assurance Requirements

The TOE security assurance requirements, summarized in Table 8, detail the management and evaluative activities required to develop the peer-to-peer SBU WLAN for use in the operational environment. Section 6 provides a justification for the chosen security assurance requirements and the selected EAL 3 assurance level.

Table 8. TOE Assurance Requirements

Assurance Class	Assurance Components
Configuration Management	Authorization controls (ACM_CAP.3) TOE CM coverage (ACM_SCP.1)
Delivery and Operations	Delivery procedures (ADO_DEL.1) Installation, generation, and startup procedures (ADO_IGS.1)
Development	Informal functional specification (ADV_FSP.1) Security enforcing high-level design (ADV_HLD.2) Informal correspondence demonstration (ADV_RCR.1)
Guidance documents	Administrator guidance (AGD_ADM.1) User guidance (AGD_USR.1)
Life-Cycle Support	Identification of security measures (ALC_DVS.1)
Tests	Analysis of coverage (ATE_COV.2) Testing: high-level design (ATE_DPT.1) Functional testing (ATE_FUN.1) Independent testing—sample (ATE_IND.2)
Vulnerability Assessment	Examination of guidance (AVA_MSU.1) Strength of TOE security function evaluation (AVA_SOF.1) Developer vulnerability analysis (AVA_VLA.1)

5.2.1 Authorization Controls (ACM_CAP.3)

Developer action elements:

ACM_CAP.3.1D. The developer shall provide a reference for the TOE.

ACM_CAP.3.2D. The developer shall use a Configuration Management (CM) system. The developer shall demonstrate that the identified CM system is employed for all TSF development.

ACM_CAP.3.3D. The developer shall provide CM documentation to the evaluation team that describes the CM system, including the implementation and how the CM system has been used to control the development of the TSF.
Content and presentation of evidence elements:

ACM_CAP.3.1C. The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.3.2C. The TOE shall be labeled with its reference.

ACM_CAP.3.3C. The CM documentation shall include a configuration list and a CM plan.

ACM_CAP.3.4C. The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.3.5C. The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.3.6C. The CM system shall uniquely identify all configuration items.

ACM_CAP.3.7C. The CM plan shall describe how the CM system is used.

ACM_CAP.3.8C. The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.3.9C. The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.3.10C. The CM system shall provide measures such that only authorized changes are made to the configuration items.

Evaluator action items:

ACM_CAP.3.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2 TOE CM Coverage (ACM_SCP.1)

Developer action elements:

ACM_SCP.1.1D. The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_SCP.1.1C. The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation.

ACM_SCP.1.2C. The CM documentation shall describe how configuration items are tracked by the CM system.

Evaluator action items:

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

5.2.3 Delivery Procedures (ADO_DEL.1)

Developer action elements:

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

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

Content and presentation of evidence elements:

ADO_DEL.1.1C. The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action items:

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

5.2.4 Installation, Generation, and Startup Procedures (ADO_IGS.1)

Developer action elements:

ADO_IGS.1.1D. The developer shall document procedures necessary for the secure installation, generation, and startup of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C. The documentation shall describe the steps necessary for secure installation, generation, and startup of the TOE.

Evaluator action items:

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

5.2.5 Informal Functional Specification (ADV_FSP.1)

Developer action elements:

ADV_FSP.1.1D. The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C. The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C. The functional specification shall be internally consistent.

ADV_FSP.1.3C. The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions, and error messages, as appropriate.

ADV_FSP.1.4C. The functional specification shall completely represent the TSF.

Evaluator action items:

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

ADV_FSP.1.2F. The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.2.6 Security Enforcing High-Level Design (ADV_HLD.2)

Developer action elements:

ADV_HLD.2.1D. The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.2.1C. The presentation of the high-level design shall be informal.

ADV_HLD.2.2C. The high-level design shall be internally consistent.

ADV_HLD.2.3C. The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C. The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C. The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions

provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C. The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C. The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C. The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions, and error messages, as appropriate.

ADV_HLD.2.9C. The high-level design shall describe the separation of the TSF into TSP-enforcing and other subsystems.

Evaluator action items:

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

ADV_HLD.2.2E. The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.2.7 Informal Correspondence Demonstration (ADV_RCR.1)

Developer action elements:

ADV_RCR.1.1D. The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C. For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action items:

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

Application Note: For this PP, this applies to ensure that the functional specification and high-level design are consistent with each other.

5.2.8 Administrator Guidance (AGD_ADM.1)

Developer action elements:

AGD_ADM.1.1D. The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C. The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C. The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C. The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C. The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C. The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C. The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C. The administrator guidance shall be consistent with all other documents supplied for evaluation.

AGD_ADM.1.8C. The administrator guidance shall describe all security requirements on the IT environment that are relevant to the administrator.

Evaluator action items:

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

5.2.9 User Guidance (AGD_USR.1)

Developer action elements:

AGD_USR.1.1D. The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C. The user guidance shall describe the functions and interfaces available to the nonadministrative users of the TOE.

AGD_USR.1.2C. The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C. The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C. The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C. The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C. The user guidance shall describe all security requirements on the IT environment that are relevant to the user.

Evaluator action items:

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

5.2.10 Identification of Security Measures (ALC_DVS.1)

Developer action elements:

ALC_DVS.1.1D. The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C. The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C. The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action items:

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

ALC_DVS.1.2E. The evaluator shall confirm that the security measures are being applied.

5.2.11 Analysis of Coverage (ATE_COV.2)

Developer action elements:

ATE_COV.2.1D. The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

ATE_COV.2.1C. The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C. The analysis of the test coverage shall demonstrate that the correspondence between the TSF, as described in the functional specification, and the tests identified in the test documentation are complete.

Evaluator action items:

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

5.2.12 Testing: High-Level Design (ATE_DPT.1)

Developer action elements:

ATE_DPT.1.1D. The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

ATE_DPT.1.1C. The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

Evaluator action items:

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

5.2.13 Functional Testing (ATE_FUN.1)

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 of evidence elements:

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

ATE_FUN.1.2C. The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C. The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C. The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C. The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action items:

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

5.2.14 Independent Testing—Sample (ATE_IND.2)

Developer action elements:

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

Content and presentation of evidence 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 items:

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 test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E. The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

Application Note: The choice of the subset tested and the sample tests executed is entirely at the discretion of the evaluator.

5.2.15 Examination of Guidance (AVA_MSU.1)

Developer action elements:

AVA_MSU.1.1D. The developer shall provide guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.1.1C. The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences, and their implications for maintaining secure operation.

AVA_MSU.1.2C. The guidance documentation shall be complete, clear, consistent, and reasonable.

AVA_MSU.1.3C. The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.1.4C. The guidance documentation shall list all requirements for external security measures (including external procedural, physical, and personnel controls).

Evaluator action items:

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

AVA_MSU.1.2E. The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.1.3.E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.2.16 Strength of TOE Security Function Evaluation (AVA_SOF.1)

Developer action elements:

AVA_SOF.1.1D. The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C. For each mechanism with a strength of TOE security function claim, the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C. For each mechanism with a specific strength of TOE security function claim, the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action items:

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

AVA_SOF.1.2E. The evaluator shall confirm that the strength claims are correct.

Application Note: For this PP, this requirement applies to the authentication mechanism described for FIA_UAU.2.

5.2.17 Developer Vulnerability Analysis (AVA_VLA.1)

Developer action elements:

AVA_VLA.1.1D. The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2D. The developer shall document the disposition of obvious vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.1.1C. The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action items:

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

6. Rationale

This section presents the mapping to show complete coverage of the Policies, Threats, and Assumptions by the Security Objectives and complete coverage of the Security Objective by the functional and assurance requirements.

6.1 Security Objectives Rationale

The security objectives rationale demonstrates that the stated security objectives (in Section 4) are traceable to all of the aspects identified in the TOE security environment (described in Section 3) and are suitable to cover them.

Table 5 in Section 4 showed that all security objectives for the TOE are traced back to aspects of the identified threats (in Section 3.2) and/or aspects of the organizational security policies to be met by the TOE (in Section 3.3). Table 6 in Section 4 showed that all security objectives for the environment are traced back to aspects of the organizational security policies and/or assumptions to be met by the TOE's environment. Table 9 presents the justification that the security objectives are suitable to counter the threats and that they cover the (OSP) and assumptions described in Section 3.

Table 9. Security Objectives Justification

Threat	Security Objective(s)	Justification
T.SIGNAL_DETECT	O.DATA_PRO	An unauthorized user detects and intercepts signals transmitted from the TOE to obtain user data. The TOE will not be able to prevent signals from being intercepted; however, O.DATA_PRO protects the user data from being disclosed such that an unauthorized user would not be able to obtain recognizable user data.
T.JAM_INTERFERE	O.ENVIRONMENT	Non-TOE generated signals in the area unintentionally interfere and disrupt TOE transmissions. O.ENVIRONMENT mitigates the threat by ensuring the TOE protects its assets and operation in case unintentional interference occurs.

Threat	Security Objective(s)	Justification
T.HACK_ACCESS	O.ACCESS O.IDENTITY O.DATA_PRO	An unauthorized user gains access to parts of the TOE as a result of missing and weak identification controls. O.ACCESS and O.IDENTITY ensure that only authorized users have access to parts of the TOE as dictated by the security policy. O.DATA_PRO protects the transmission of information between the clients.
T.SPOOFING	O.DATA_PRO O.IDENTITY O.EXCHANGE	An attacker uses RF signal paths to masquerade as a valid user or to deliver spurious messages. O.IDENTITY prohibits an unauthorized user from masquerading as a valid user because the user must be identified to the TOE. O.DATA_PRO requires all transmissions to be encrypted, thus eliminating the threat of an attacker to interject recognizable messages in to the network. O.EXCHANGE ensures that spurious messages will not disrupt the exchange of information between parts of the TOE.
T.HACK_MSG_CONTENT	O.DATA_PRO	A hacker modifies information intercepted from the RF communication link between two unsuspecting entities before passing it on, thereby deceiving the intended recipient. O.DATA_PRO requires all transmission to be encrypted, thus eliminating a hacker's ability to modify a message without detection.

Threat	Security Objective(s)	Justification
P.ACCOUNT	OE.ACCOUNT	Users must be held accountable for security-relevant actions. Each user of a client is responsible for the physical security of the client and the proper setup of the client to allow the client to communicate peer-to-peer. Accountability is achieved by establishing who "owns" the client. OE.ACCOUNT provides procedural measures to record which user is assigned to a particular client.
P.COMPLY	O.EAL OE.COMPLY	The implementation and use of the TOE must comply with all applicable laws, regulations, and guidelines imposed on the organization for an SBU environment. O.EAL establishes the assurances in the TOE that are necessary for use in an SBU environment. OE.COMPLY ensures that the maintainers of the TOE comply with applicable laws and regulations. This objective is met through procedural means and checked by security reviews and assessments.
P.USAGE	OE.TRAIN O.MANAGE OE.ADMIN	The TOE must be used for only authorized purposes. OE.TRAIN and OE.ADMIN ensures that authorized users are trained on the appropriate use of the system, they are trusted not to misuse the TOE, and they follow guidance. O.MANAGE requires that the TOE provide management features to allow users to carry out their duties for administering the system.

Threat	Security Objective(s)	Justification
P.GUIDANCE	O.DOC	Guidance must be provided for the secure installation and use of the system. O.DOC provides the guidance documentation required for proper installation and use of the TOE
P.CRYPTO	O.CRYPTO O.DATA_PRO	Encryption used to protect user data and the associated cryptographic module must comply, at a minimum, with FIPS 140-1 (level 2). O.DATA_PRO requires all transmission to be encrypted and O.CRYPTO ensures that the TOE uses appropriate cryptographic functions.
P.PKI	O.CRYPTO	Class 3 or 4, X.509 certificates shall be used to establish session keys and to digitally sign transmitted data. O.CRYPTO ensures that the TOE uses appropriate PKI certificates to create session keys and for digital signatures.
A.OPERATING_SYS	OE.OPERATING_SYS	The underlying IT environment of the TOE does not contain vulnerabilities that undermine the secure operation of the TOE. Through procedural means, OE.OPERATING_SYS objective requires the maintainers of the TOE to properly install, configure, and operate the underlying IT environment.

Threat	Security Objective(s)	Justification
A.ADMINISTRATION	OE.ADMIN OE.TRAIN	Authorized users are trusted, competent, and trained to manage the security features of the TOE. Because the authorized user is responsible for administering the client, the users are trusted not to misuse the TOE and follow guidance, which would describe the proper steps and procedures for using the TOE (OE.ADMIN). OE.TRAIN ensures that authorized users are trained on security features of the system.
A.NO_USER_DATA	OE.INSTALL	The TOE is strictly a conduit for information flow through RF transmission and does not provide user data storage capability. Proper installation and use of the TOE will prevent the TOE from being used outside its intended purpose. OE.INSTALL ensures that the maintainers of the TOE installed, managed, and operated in a manner that maintains IT security objectives
A.CO_LOCATED	OE.INSTALL	TOE components (clients and access point) are sufficiently co-located as required to accommodate communication ranges. OE.INSTALL ensures that the maintainers of the TOE installed, managed, and operated in a manner that maintains IT security objectives.
A.CONFIGURATION	OE.INSTALL	The TOE may or may not be interconnected to a wired network OE.INSTALL ensures that the maintainers of the TOE installed, managed, and operated in a manner that maintains IT security objectives.
A.ENVIRON	OE.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

Threat	Security Objective(s)	Justification
		OE.LOWEXP ensures that the TOE is used in a low risk nonhostile environment.
A.PHYSICAL	OE.PHYSICAL	The TOE components are physically protected from unauthorized physical access. OE.PHYSICAL requires the components be physically safeguarded by the individuals to whom they are assigned.
A.PKI	OE.PKI	Within the IT environment, there is a PKI that provides valid Class 3 or 4, X.509 certificates. OE.PKI requires that valid Class 3 or 4, X.509 certificates be used by the TOE.

6.2 Security Requirements Rationale

The security requirements rationale demonstrates that the set of security requirements (in Section 5) is suitable to meet and is traceable to the security objectives (specified in Section 4). The set of IT security requirements is internally consistent because the requirements were all derived from Parts 2 and 3 of the CC, operations were performed in accordance to the CC, and the security requirements were chosen and written to apply to the same concepts expressed in the security objectives. The IT security requirements together form a mutually supportive whole because they were derived from the TOE security objectives, include FPT_RVM.1 and FPT_SEP.1 to prevent bypassing and tampering of the TSF, and include security management requirements to properly manage the security functions.

6.2.1 TOE Assurance Requirements

This PP has been developed for an SBU environment with a low level of risk to assets. It is intended that peer-to-peer WLAN products used in these environments will be generally available and not require modification to meet the security needs of the environment. Given consideration to best commercial practices for COTS products and assurance requirements for the various assurance levels, it was determined that EAL 3 was the most appropriate.

6.2.2 Dependencies Not Met

FMT_MSA.2 is dependent on ADV_SPM.1. ADV_SPM.1 is an assurance requirement that is required at EAL 4. Because this PP is targeting EAL 3, the ADV_SPM.1 requirement was excluded. In addition, the rules for defining the SFP will be sufficiently defined by the developer within their ST when completing operations for FDP_IFF.1.

All the security management functional requirements included in this PP are dependent on FMT_SMR.1. FMT_SMR.1 requires the TOE to support roles and thus restrict actions taken by authorized users. Given the nature of the peer-to-peer WLAN configuration and use, the TOE defined in this PP allows the authorized users to perform security management functions such that the requirement for FMT_SMR.1 was not needed.

6.2.3 Strength of Function Rationale

The minimum strength of function level SOF-basic was chosen because the TOE environment assumes a nonhostile environment in which the threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low. The strength of function level is consistent with the security objectives of the TOE because the security objectives are derived from the TOE environment, which describes a low risk environment.

6.2.4 Traceability

Table 10 shows how the requirements for the TOE map to the security objectives.

Table 10. Mapping of Requirements to Security Objectives

Security Objectives / TOE Security Functional Requirements	O.ACCESS	O.IDENTITY	O.CRYPTO	O.DATA_PRO	O.EXCHANGE	O.MANAGE	O.ENVIRONMENT	O.DOC	O.EAL
FCS_NRO.1			■	■					
FCS_CKM.1			■						
FCS_CKM.4			■						
FCS_COP.1			■	■					
FDP_IFC.2	■								
FDP_IFF.1	■								
FDP_ITT.1					■				
FDP_ITT.3					■				
FIA_ATD.1		■							
FIA_UID.2		■	■						
FIA_USB.1		■							
FMT_MSA.1	■					■			
FMT_MSA.2			■			■			
FMT_MSA.3	■					■			
FPT_ITT.1							■		
FPT_SEP.1							■		
FPT_RVM.1							■		
AGD_ADM.1								■	

AGD_USR.1									
EAL 3 Assurance Requirements (See Table 8)									+

6.2.5 Suitability

In this section, each security requirement is shown to be suitable to satisfy the security objectives.

O.ACCESS

The TOE shall control access to information that is subject to the TOE security policy, based on the identity of the individuals, such that this policy cannot be bypassed in the TOE.

In FDP_IFC.2 the WIRELESS SFP requires that all information flow occur only between subjects on the WLAN.

Identifying user data is stored in X.509 certificates, which may be stored on the client device or in a user token. The specific rules for the information flow policy are to be specified in the ST. (FDP_IFF.1)

FMT_MSA.3 is included because it is a dependency for FDP_IFF.1. This requirement specifies that the WIRELESS SFP must be initially restrictive, not allowing information flow to occur unless the authorized user specifies that it should be allowed.

FMT_MSA.1 is a dependency for FMT_MSA.3. It requires that only the authorized user be able to modify the security attributes for each user.

O.IDENTITY

The TOE will uniquely identify each system user through the user's possession of a valid X.509 certificate. The TOE will associate each user-requested action with the identity of the user who initiated the session (i.e., log on). The TOE will restrict the actions a user may perform before the TOE verifies the identity of the user.

The FIA_ATD.1 requirement specifies that the TSF shall maintain X.509 certificates and other security attributes to identify the users.

FIA_UID.2 requires that users be successfully identified to the TSF before being allowed to perform any action.

FIA_USB.2 requires that subjects acting on behalf of users be associated with the users' security attributes.

O.CRYPTO

The TOE shall use Class 3 or 4, X.509 certificates and support cryptographic functions in a secure manner with sufficient strength for SBU information. The certificates shall be used to establish session keys and to digitally sign transmitted data.

FCO_NRO.1 requires digital signatures to be affixed to all transmitted data to enforce nonrepudiation of origin. Thus, the sender of information cannot deny having sent it.

FIA_UID.1 is a dependency of FCO_NRO.1. It supports the nonrepudiation requirement by assuring that all users are uniquely identified to the TSF before sending any data. Users are implicitly identified through the possession of a Class 3 or Class 4 X.509 certificate. This PP includes FIA_UID.2, which is hierarchical to FIA_UID.1.

FCS_CKM.1 requires that a key generation algorithm be used to generate 128-bit cryptographic keys that will be used for all transmitted data.

FCS_CKM.4 requires that all keys be destroyed in accordance with standards and methods to be specified in the ST.

FCS_COP.1 requires that the RC4 algorithm use the 128-bit keys to encrypt all transmitted data.

FMT_MSA.2 is a dependency requiring that only secure values be accepted for cryptographic keys.

O.DATA_PRO

Encryption will be used to provide confidentiality and integrity of TSF and user data in transit between parts of the TOE.

FCO_NRO.1 is required to provide integrity. Integrity of data in WLAN communication is important because of the nature of it being transmitted over the air. Radio interference from other sources could cause integrity errors.

FCO_COP.1 is required to provide data encryption. Encryption is especially important in a WLAN as a result of the exposure of data transmitted over the air. Radio signals are easily intercepted. A greater danger of interception exists in a WLAN than in a traditional wired LAN.

O.EXCHANGE

The TOE will ensure that the system correctly exchanges security-attribute information with distributed components of the TOE.

FDP_ITT.1 requires protection of security attribute data transmitted between components of the TOE (e.g., between an access point and a client). Data should be protected from disclosure and modification.

FDP_ITT.3 requires that all transmitted security attribute data be monitored and checked for integrity errors. Integrity errors could occur when data transmitted using radio signals encounters interference over the air.

O.MANAGE

The TOE will provide adequate management features for its security functions.

FMT_MSA.1 allows only the authorized administrator to modify security attributes associated with users of the TOE.

FMT_MSA.2 ensures that only secure values are accepted for security attributes.

FMT_MSA.3 requires that default values are initialized in security attributes and allows only the authorized administrator to override the defaults.

O.ENVIRONMENT

The TOE must protect itself against compromise by having a structure that neither reveals security information nor operates in an insecure manner when exposed to signal interference.

FPT_ITT.1 requires that TSF data be protected from disclosure and modification when it is transmitted between components of the TOE.

FPT_SEP.1 requires that the TSF maintain a domain for its own protection, not allowing modification of its code or data.

FPT_RVM.1 requires that the TSF protection mechanisms always be invoked, and never bypassed.

O.DOC

Guidance documentation provided to authorized users and administrators will detail the proper installation and use of the TOE to minimize the security risks within the environment.

AGD_ADM.1 requires that the TOE vendor prepare guidance documentation for the authorized administrator.

AGD_USR.1 requires that the TOE vendor prepare guidance documentation for the user.

O.EAL

The TOE must be structurally tested; be shown to be resistant to obvious vulnerabilities; and be documented with sufficient design, test, configuration, and life-cycle documentation.

The Assurance requirements for EAL 3 listed in Table 8 require that the TOE be designed and tested to conform to EAL 3. The EAL 3 requirements satisfy the security objective for a structurally tested (shown to be resistant to obvious vulnerabilities) and documented TOE.

7. References

1. X.509 Certificate Policy for the United States Department of Defense, Version 5.0, 13 December 1999.
2. Infrastructure Wireless Local Area Network (WLAN) Protection Profile for Sensitive But Unclassified Environments, Version 0.1, March 2001.
3. Draft U.S. DoD Remote Access Protection Profile for High Assurance Environments, version 0.98, 24 May 2000.
4. Common Criteria for Information Technology Security Evaluation, Version 2.1. CCIMB-99-021, 032, 033. August 1999.
5. High-Assurance Remote Access (HARA) Architecture, Version 1.1, 15 May 2000.
6. Global Information Grid (GIG) Policy 6-8510, Information Assurance Guidance, 16 June 2000.
7. Common Methodology for Information Technology Security Evaluation, Version 1.0, CEM-99/045, August 1999.

Appendix A. Acronyms

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
ISSE	Information System Security Engineers
IT	Information Technology
OSP	
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
SoF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
WLAN	Wireless Local Area Network