



**3e Technologies International
3e-010F-A-2 and 3e-010F-C-2
Crypto Client Software**

Security Target

22000209-701

Version K

August, 2006

© 2006 3e Technologies International, Inc. All rights reserved.

3e Technologies International 3e-010F-A-2 and 3e-010F-C-2 Crypto Client Software Security Target Revision K.

This guide, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. The content of this guide is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by 3eTI. 3eTI assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

Except as permitted by license, no part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without prior written permission of 3eTI.

All registered names, product names and trademarks of other companies used in this guide are for descriptive purposes only and are the acknowledged property of the respective company.

Document ID Number: 22000209-701 Revision K
Total Page Count: 35

Contact 3e Technologies International, Inc.

3e Technologies International, Inc
700 King Farm Boulevard
Suite 600
Rockville, MD 20850 USA

Telephone: +1 (301) 670-6779

Fax: +1 (301) 670-6989

Website: <http://www.3eti.com/>

Email: <mailto:info@3eti.com>

UNCLASSIFIED

Table of Contents

Table of Contents	3
List of Tables and Figures	4
1. Security Target Introduction	5
1.1 Security Target, TOE and CC Identification	5
1.2 Common Criteria Conformance Claims	5
1.3 TOE Summary	5
1.4 Strength of Environment	5
1.5 Conventions, Terminology, Acronyms	5
2. TOE Description	10
2.1 Product Description	10
2.2 Security Environment TOE Boundary	11
2.3 TOE File List	12
3. Security Environment	12
3.1 Secure Usage Assumptions	13
3.2 Threats to Security	13
3.3 Organization Security Policies	16
3.4 Security Function Policies	16
4. Security Objectives	16
4.1 Security Objectives for the TOE	17
4.2 Security Objectives for the IT Environment	17
4.3 Security Objectives for the non-IT Environment	17
5. IT Security Requirements	17
5.1 TOE Security Functional Requirements	17
5.2 IT Environment Security Requirements	21
5.3 TOE Security Assurance Requirements	21
5.4 Strength of Function	22
6. TOE Summary Specification	22
6.1 TOE Security Functions	22
6.2 TOE Security Assurance Measures	24
6.3 Strength of Function	25
7. Rationale	26
7.1 Security Objectives Rationale	26
7.2 Security Requirements Rationale	28
7.3 Rationale for Assurance Requirements	33
7.4 Requirement Dependency Rationale	33
7.5 Rationale for Not Satisfying All Dependencies	33
7.6 Explicitly Stated Requirements Rationale	34
7.7 TOE Summary Specification Rationale	35
7.8 Strength of Function Rationale	35
7.9 Protection Profile Claims Rationale	35

List of Tables and Figures

Figure 1 - Example of 3eTI WLAN Access System (Wireless Client + AP + Security Server).....	10
Table 1 - TOE Assumptions.....	13
Table 2 - Threats.....	14
Table 3 - Basic Robustness Threats NOT Applicable to the TOE.....	15
Table 4 - Organizational Security Policies.....	16
Table 5 - Security Function Policies.....	16
Table 6 – TOE Security Objectives.....	17
Table 7 – IT Environment Security Objectives.....	17
Table 8 – Non-IT Environment Security Objectives.....	17
Table 9 - TOE Security Functional Requirements.....	18
Table 10 - Auditable Events.....	18
Table 11 - IT Environment Security Functional Requirements.....	21
Table 12- TOE Security Assurance Requirements.....	21
Table 13 - Security Objectives to Assumptions, Threats and Policies Mappings.....	26
Table 14 - Rationale for TOE Security Requirements.....	28
Table 15 - Rationale for Requirements on the TOE IT Environment.....	32
Table 16 - TOE Security Functional Requirement Dependencies.....	33
Table 17 - Unsupported Dependency Rationale.....	34
Table 18 - Rationale for Explicit Requirements.....	34

1. Security Target Introduction

This section (a) identifies the Security Target (ST) and Target of Evaluation (TOE); (b) specifies the ST conventions and ST conformance claims; and (c) describes the ST organization.

1.1 Security Target, TOE and CC Identification

ST Title: 3e Technologies International 3e-010F-A-2 and 3e-010F-C-2 Crypto-Client Software Security Target

ST Version: Version K

ST Author: Ryon Coleman

ST Publication Date: August, 2006

TOE Identification: The TOE for the 3e-010F-A-2 is identified as the FIPS 140-2 Validated™ Cryptomodule 3e-010F-A-2 Version 2.0 Build 18.

The TOE for the 3e-010F-C-2 is identified as the FIPS 140-2 Validated™ Cryptomodule 3e-010F-C-2 Version 2.0 Build 15.

Evaluation Assurance Level (EAL): Evaluation Assurance Level (EAL) 2 augmented with, ACM_SCP.1 (TOE CM Coverage), ALC_FLR.2 (Flaw Remediation), ACM_CAP.3 (Authorization Controls), and AVA_MSU.1 (Misuse – Examination of Guidance).

Strength of Function: SOF-Basic

Common Criteria Identification: Common Criteria for Information Technology Security Evaluation, Version 2.3, August, 2005. International Standard – ISO/IEC 15408:2004.

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

1.2 Common Criteria Conformance Claims

This TOE conforms to the following specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.3, August, 2005.
 - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.3, August, 2005.
 - Part 3 Conformant
 - Evaluation Assurance Level (EAL) 2 augmented with, ACM_SCP.1 (TOE CM Coverage), ALC_FLR.2 (Flaw Remediation), ACM_CAP.3 (Authorization Controls), and AVA_MSU.1 (Misuse – Examination of Guidance)

1.3 TOE Summary

The Target of Evaluation (TOE) is a cryptographic WLAN client comprised of either the 3e-010F-C-2 or 3e-010F-A-2 Crypto Client Software. The difference between the clients is in the drivers related to the supported hardware. The 3e-010F-C-2 supports Intel PRO/Wireless 2200BG and 2915ABG cards, and the 3e-010F-A-2 supports WLAN cards based on the Atheros AR5001X+, AR5002G and AR5002X chipsets. It is expected that the client will be a component of a larger system (e.g. the WLAN client communicating to a 3eTI Enterprise WLAN Access Point). The WLAN client software is in most cases installed into a laptop or mobile device. The Crypto Client provides standard 802.11a/b/g wireless access along with enhanced protection through a variety of cryptographic features, providing a high level of security for wireless environments.

1.4 Strength of Environment

The TOE, 3e Technologies International 3e-110 WLAN PC Card and 3e-010F Crypto-Client Software, is being evaluated for the basic robustness operating environment. The assurance requirements of the augmented EAL2 and the minimum strength of function of SOF-basic were specified to be consistent with that level of risk.

1.5 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the Security Target.

1.5.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
 - **Iteration**: allows a component to be used more than once with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).
 - **Assignment**: allows the specification of an identified parameter. Assignment is indicated by showing the value in square brackets, [Assignment_value].
 - **Selection**: allows the specification of one or more elements from a list. Selections are denoted by *italicized text*.
 - **Refinement**: allows the addition of details. Refinements are indicated using **bold**, for additions, and ~~strike-through~~, for deletions.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions and the application of interpretations.
- Explicitly stated Security Functional Requirements include _EXP in their demarcation.
- Security Functional Requirements including the "-NIAP-xxxx" (where x is, for example, an integer) extension are considered to be explicitly stated.

1.5.2 Terminology

The following terminology is used in the Security Target:

- **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 and the disclosure and modification of data.
- **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.
- **Assurance** -- A measure of confidence that the security features of an IT system are sufficient to enforce it's' security policy.
- **Asymmetric Cryptographic System** -- A system involving two related transformations; one determined by a public key (the public transformation), and another determined by a private key (the private transformation) with the property that it is computationally infeasible to determine the private transformation (or the private key) from knowledge of the public transformation (and the public key).
- **Asymmetric Key** -- The corresponding public/private key pair needed to determine the behavior of the public/private transformations that comprise an asymmetric cryptographic system.
- **Attack** -- An intentional act attempting to violate the security policy of an IT system.
- **Authentication** -- Security measure that verifies a claimed identity.
- **Authentication credentials** -- Information used to verify a claimed identity.
- **Authorization** -- Permission, granted by an entity authorized to do so, to perform functions and access data.
- **Authorized user** -- An authenticated user who may, in accordance with the TSP, perform an operation.
- **Availability** -- Timely, 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 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 contiguous perimeter that establishes the physical bounds (for hardware) or logical bounds (for software) of a cryptographic module.
- **Cryptographic key (key)** -- A parameter used in conjunction with a cryptographic algorithm that determines: (a) the transformation of plaintext data into cipher text data; (b) the transformation of cipher text data into plaintext data; (c) a digital signature computed from data; (d) the verification of a digital signature computed from data, or (e) a digital authentication code computed from data.
- **Cryptomodule** -- This Security Target uses the term "crypto module" in several cryptographic functional requirements. When used this term has very specific meaning. It describes:
 - a cryptographic module that is FIPS 140-2 validated (to comply with FCS_BCM_EXP);
 - the cryptographic functionality implemented in that module are FIPS-approved security functions that have been validated; and
 - the cryptographic functionality is available in a FIPS-approved mode for the crypto module.
- **Cryptographic Module** -- The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
- **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 ST and additional rules imposed by the vendor.
- **Defense-in-Depth (DID)** -- A security design strategy whereby layers of protection are utilized to establish an adequate security posture for an IT system.
- **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 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.
- **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.
- **Identity** -- A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
- **Integrity** -- A security policy pertaining to the corruption of data and TSF mechanisms.
- **Integrity label** -- A security attribute that represents the integrity level of a subject or an object. Integrity labels are used by the TOE as the basis for mandatory integrity control decisions.
- **Integrity level** -- The combination of a hierarchical level and an optional set of non-hierarchical categories that represent the integrity of data.
- **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.
- **Mandatory Access Control (MAC)** -- A means of restricting access to objects based on subject and object sensitivity labels.
- **Mandatory Integrity Control (MIC)** -- A means of restricting access to objects based on subject and object integrity labels.
- **Multilevel** -- The ability to simultaneously handle (e.g., share, process) multiple levels of data, while allowing users at different sensitivity levels to access the system concurrently. The system permits each user to access only the data to which they are authorized access.
- **Named Object** -- An object that exhibits all of the following characteristics: (a) the object may be used to transfer information between subjects of differing user identities within the TSF; (b) subjects in the TOE must be able to request a specific instance of the object; (c) the name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with different user identities to request the same instance of the object.

- **Non-Repudiation** -- A security policy pertaining to providing one or more of the following: (a) to the sender of data, proof of delivery to the intended recipient; (b) to the recipient of data, proof of the identity of the user who sent the data.
- **Object** -- An entity within the TSC that contains or receives information and upon which subjects perform operations.
- **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.
- **Operational key** -- Key intended for protection of operational information or for the production or secure electrical transmissions of key streams.
- **Peer TOEs** -- Mutually authenticated TOEs that interact to enforce a common security policy.
- **Public Object** -- An object for which the TSF unconditionally permits all entities "read" access. Only the TSF or authorized administrators may create, delete, or modify the public objects.
- **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), and AVA_MSU.1 (Misuse-Examination Guidance) as defined in CCIB-98-028, Part 3, Version 2.0
 - **Medium**: Security services and mechanisms that provide for layering of additional safeguards above good commercial practices. Medium robustness equates to EAL-4 plus; ALC_FLR (Flaw Remediation); ADV_IMP.2; ADV_INT.1; ATE_DPT.2; and AVA_VLA.3 (Moderately Resistant Vulnerability Analysis) as defined in CCIB-98-028, Part 3, Version 2.0. If cryptographic functions are included in the TOE, then the ST should be augmented with AVA_CCA_EXP.2 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.
- **Security attributes** -- TSF data associated with subjects, objects, and users that is used for the enforcement of the TSP.
- **Security level** -- The combination of a hierarchical classification and a set of non-hierarchical categories that represent the sensitivity on the information.
- **Sensitivity label** -- A security attribute that represents the security level of an object and that describes the sensitivity (e.g. Classification) of the data in the object. Sensitivity labels are used by the TOE as the basis for mandatory access control decisions.
- **Split key** -- A variable that consists of two or more components that must be combined to form the operational key variable. The combining process excludes concatenation or interleaving of component variables.
- **Subject** -- An entity within the TSC that causes operations to be performed.
- **Symmetric key** -- A single, secret key used for both encryption and decryption in symmetric cryptographic algorithms.
- **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.

- **User Data** -- Data created by and for the authorized user that does not affect the operation of the TSP. User data is separate from the TSF data, which has security attributes associated with it and the system data.
- **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.

1.5.3 Acronyms

The acronyms used within this Security Target:

CC	Common Criteria	RF	Radio Frequency
CM	Configuration Management	SBU	Sensitive But Unclassified
COTS	Commercial Off-The-Shelf	SF	Security Function
DoD	Department of Defense	SFP	Security Function Policy
EAL	Evaluation Assurance Level	SFR	Security Functional Requirement
FIPS	Federal Information Processing Standards	SoF	Strength of Function
GIG	Global Information Grid	ST	Security Target
HARA	High-Assurance Remote Access	TOE	Target of Evaluation
ISSE	Information System Security Engineers	TSC	TSF Scope of Control
IT	Information Technology	TSF	TOE Security Functions
PKI	Public Key Infrastructure	TSFI	TSF Interface
PP	Protection Profile	PUB	Publication
TSP	TOE Security Policy	WLAN	Wireless Local Area Network

1.5.4 References

- DoD Directive Number 8500.1 "Information Assurance", October 24, 2002.
- DoD Instruction Number 8500.2 "Information Assurance Implementation", February 6, 2003.
- U.S. Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments, Version 1.1, August 1, 2003.
- U.S. Government Wireless Local Area Network (WLAN) Client for Basic Robustness Environments Protection Profile, Version 1.0, November 2003.
- 3eTI Enterprise Access System for Basic Robustness Environments, Security Target, Version 1.1, April 2004.
- 3e-110 WLAN PC Card and 3e-010F Crypto Client Software for Basic Robustness Environments Security Target, Version 1.0, February 2004.
- NIST SP 800-37, Guidelines for the Security Certification and Accreditation of Federal IT Systems, June 2003 (or later version).
- 3eTI FIPS 140-2 Non-Proprietary Security Policy Level 1 Validation

1.5.5 Security Target Overview and Organization

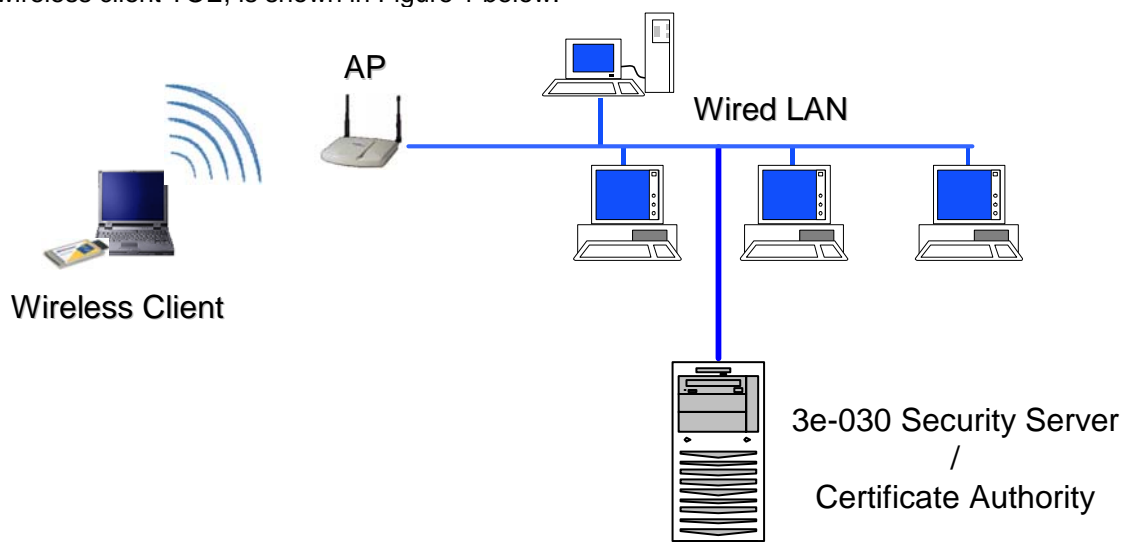
The Security Target contains the following additional sections:

- TOE Description (Section 2): Provides an overview of the TOE security functions and boundary.
- Security Environment (Section 3): Describes the threats, organizational security policies and assumptions that pertain to the TOE.
- Security Objectives (Section 4): Identifies the security objectives that are satisfied by the TOE and the TOE environment.
- IT Security Requirements (Section 5): Presents the security functional and assurance requirements met by the TOE.
- TOE Summary Specification (Section 6): Describes the security functions provided by the TOE to satisfy the security functional requirements and objectives.
- Rationale (Section 7): Presents the rationale for the security objectives, requirements, and TOE summary specifications as to their consistency, completeness and suitability.

2. TOE Description

The Target of Evaluation (TOE) is a cryptographic WLAN client. It is expected that the client will be a component of a larger system (e.g. the WLAN client communicating to a 3eTI Enterprise WLAN Access Point). For the purpose of this ST we will be discussing a typical wired to wireless configuration. However the reader should keep in mind that it does not preclude any other wireless configuration that may exist. This ST does not dictate a particular configuration. Instead the ST addresses the security requirements for the client that provides communication between the wireless user and the wired network and its resources. The security requirements of the TOE are administration, audit, and encryption.

A WLAN is an extension, or possibly a replacement, of a traditional wired network. The WLAN client is in most cases installed into the laptop or mobile device. Therefore, it must also be understood that the TOE alone does not provide all of the security functionality that is required in a Basic Robustness Environment. In the typical configuration, the client and access system establish a connection through which all data will traverse to the wired side of the network. As such, it is not intended to provide any direct network services to the users that connect through the access system. The client will rely mainly on the environment in which it resides to perform many of the management duties and providing secure access to the network. A more accurate example of the 3eTI wireless access system, including the wireless client TOE, is shown in Figure 1 below.



**Figure 1 - Example of 3eTI WLAN Access System
(Wireless Client + AP + Security Server)**

2.1 Product Description

The TOE is a WLAN client comprised of either the 3e-010F-C-2 or 3e-010F-A-2 Crypto Client Software. The difference between the clients is in the drivers related to the supported hardware. The 3e-010F-C-2 supports Intel PRO/Wireless 2200BG and 2915ABG cards, and the 3e-010F-A-2 supports WLAN cards based on the Atheros AR5001X+, AR5002G and AR5002X chipsets. Other than the drivers needed to work with the specific cards, the clients are identical. The TOE supports Windows 2000 and Windows XP (Home and Professional).

The Crypto Client provides standard 802.11a/b/g wireless access along with enhanced protection through a variety of cryptographic features, providing a high level of security for wireless environments.

If encryption is desired for the WLAN, different encryption can be employed depending on the mode selected. In FIPS 140-2 mode (highly secure), encryption can be set for None, Static AES, Static 3DES, Dynamic Key Exchange and WPA2 Enterprise and Personal (AES-CCMP). In non-FIPS mode, you can select None, Static AES, Static 3DES, Dynamic Key Exchange, Static WEP, WPA-Enterprise and Personal (TKIP or AES-CCMP) and WPA2-Enterprise and Personal (TKIP or AES-CCMP).

The Configuration Utility provides an intuitive user interface to configure, manage and use various features. The administrator can configure up to 10 separate profiles. Each profile consists of various wireless configuration parameters (e.g., Security Mode (FIPS or non-FIPS mode), SSID, card type (802.11a/b/g), wireless authentication type, encryption (AES, 3DES, DKE, AES-CCMP) and related keys or certificate, power level, transmit rate, etc.).

The user interface also provides a Site Survey tool. The FIPS 140-2 mandated Self test suite can also be invoked from the GUI. The Radio state can also be controlled.

The following security modules have been implemented in the Crypto-Client:

- AES (128/192/256 bit)
- 3DES (192 bit)
- AES-CCMP
- TKIP
- WEP
- 802.1x/EAP-TLS for authentication
- WPA
- WPA2/802.11i

2.2 Security Environment TOE Boundary

The TOE includes both physical and logical boundaries. This section describes both the security functions provided by the TOE as well as the physical realization of the TOE.

2.2.1 Physical Boundaries

The TOE is a software package installed on a Windows 2000/XP Home/XP Pro computer. The operating system and computer are not included in the TOE, only the provided software (including the appropriate driver for the WLAN card).

2.2.2 Logical Boundaries

The TOE Security Functions are Audit, Encryption, Management and Information Flow Control.

2.2.2.1 Audit

The TOE can generate auditable events in cooperation with its IT environment. It is expected that the IT environment will provide the mechanisms for audit event storage and retrieval.

2.2.2.2 Encryption

This 3e-AS includes cryptographic modules which have been evaluated against applicable Federal Information Processing Standard Publication (FIPS PUB) standards. The entire product has been evaluated against FIPS 140-2, which defines security requirements for cryptographic modules, while the 3DES and AES encryption algorithms have been evaluated against FIPS 46-3 and FIPS 197, respectively. All cryptographic operations of the TOE use these evaluated modules/algorithms to ensure the security of all data passed.

2.2.2.3 Management

The TOE requires that administrators be properly identified and authenticated prior to performing any administrative tasks for the TOE. The TOE provides a Crypto-Officer and Administrator accounts which can configure the security settings (this is restricted to the Crypto-Officer account) and other settings on the client.

2.2.2.4 User Data Protection

The TOE protects all user data, such as cryptographic keys, stored within the system against malicious recovery by assuring that when the data is no longer needed that it is zeroized, and not just deallocated. This ensures that the data is not still available to other processes which may subsequently use the same resource. The TOE IT Environment ensures that any previous information content of a resource is made unavailable upon the allocation of the resource.

One of the ways that the TOE enforces information flow is by requiring the establishment of an encrypted communications channel. The TOE only allows connections which are specified by the Crypto-Officer, to assure the security needs of the organization are met.

2.2.2.5 Identification & Authentication

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

2.2.2.6 Protection of the TSF

The TOE performs a series of tests on startup to verify the integrity of the software using FIPS-approved integrity checking techniques. These tests are used to assure the correct security functionality when the TOE is active. The results of these tests are written into the audit records of the installed operating system (i.e. the Event Log). These tests are started automatically when the computer is turned on and the drivers necessary for WLAN connectivity are loaded by the operating system.

2.3 TOE File List

The list of files included below define what is included within the TOE.

3e-010F-A-2 Crypto Client

Installed Files on Windows XP/Windows 2000:

1. wathsupp.exe
2. ccsathcfg.exe
3. aepathssl32.dll
4. aepathlib32.dll
5. ccsathcrypt.dll
6. ccsathn51.sys
7. ccsathn51.inf
8. aepn50_A.dll
9. aepands5.sys
10. ccsathmsg.dll
11. uninstall_ath.exe
12. adapter_ath.exe
13. killproc.exe
14. CCSAthHelp.chm
15. msvcp60.dll (only on Windows 2000 if not present)

3e-010F-C-2 Crypto Client

Installed Files on Windows XP/Windows 2000:

1. wcx2supp.exe
2. ccscx2cfg.exe
3. aepcx2ssl32.dll
4. aepcx2lib32.dll
5. ccscx2crypt.dll
6. ccscx2n51.sys (Only on Windows XP)
7. ccxcx2n50.sys (Only on Windows 2000)
8. ccscx2n51.inf
9. aepn50_c.dll
10. aepcnds5.sys
11. ccscx2msg.dll
12. uninstall_cx2.exe
13. adapter_cx2.exe
14. killproc.exe
15. CCScx2Help.chm
16. msvcp60.dll (only on Windows 2000 if not present)

3. Security Environment

The TOE security environment describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed. The statement of the TOE security environment defines the following:

- Threats that the product is designed to counter
- Assumptions made on the operational environment and the method of use intended for the product,
- Organizational security policies with which the product is designed to comply.

3.1 Secure Usage Assumptions

This section describes the aspects of the operating environment in which the TOE is intended to be used—including personnel and physical assumptions of the environment. The TOE is assured of providing effective security measures in its intended environment only if it has been delivered, installed, and administered as intended.

Table 1 - TOE Assumptions

Name	Assumption Definition
A.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance.
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.

3.2 Threats to Security

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 ST. 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.

The threats listed in Table 2 are general. Exposure of wireless communications in the RF transmission environment introduces unique threats to the WLAN client. 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 nature of the basic robustness environment, the threats identified exclude those that would be considered a sophisticated attack (i.e., intentional jamming, traffic analysis).

Table 3 lists basic robustness threats that are not applicable to the TOE.

Table 2 - Threats

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 functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
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	Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered thereby causing potential security vulnerabilities.
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).

Table 3 - Basic Robustness Threats NOT Applicable to the TOE

Name	Threat Definition	Rationale for NOT Including this Threat
T.ACCIDENTAL_AUDIT_COMPROMISE	A user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	The storage/retrieval and review of audit records is provided by the IT environment. Hence, although this threat must be addressed within the IT environment, the functional requirements specified in this ST do not provide the functionality required to protect the audit records in the external environment. Although there may be some cases where one could argue that requiring encrypted RF communications and user authentication will assist in addressing this threat. The fundamental threat must be met by protecting communications path that the audit records travel for storage and review.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	As is noted previously, this TOE is a wireless network interface card, which is installed as part of a larger system. As a component of a larger system, the TOE is responsible for generating audit records in accordance with the audit policy specified by the system administrator. It is expected that these records will be stored outside of the TOE. The TOE IT environment will provide appropriate mechanisms to protect audit records after they have been generated.
T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.	The ST authors recognize that this threat, although appropriate for a basic robustness environment, but that it will not be addressed (either fully or partially) by the TOE. The TOE, in this case, is a wireless network interface card, which is installed as part of a larger system. As a component of larger system, the only unattended sessions within the TOE scope of control are network connections. The ST authors believe that this threat is more appropriately mitigated by the operating system in which the WLAN client is installed. The OS is capable of uniformly enforcing a policy for unattended network, serial interface and console sessions.
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.	As is noted previously, this TOE is a wireless network interface card, which is installed as part of a larger system. As a component of a larger system, the does not have access to information identifying authorized or unauthorized users.

Name	Threat Definition	Rationale for NOT Including this Threat
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.	As is noted previously, this TOE is a wireless network interface card, which is installed as part of a larger system. As a component of a larger system, the TOE is responsible for generating audit records in accordance with the audit policy specified by the system administrator. However the TOE is not expected to provide facilities to either store or review audit records. It is expected that the TOE IT environment will provide facilities to review, sort, select and other manage the audit records.

3.3 Organization Security Policies

The following table lists the Organizational Security Policies enforced by the TOE:

Table 4 - Organizational Security Policies

Name	Policy Definition
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHY	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).

For a WLAN client device, the TOE is a component of a larger system and as such, does not address all of the policies identified as part of a basic robustness environment. These policies are identified below.

Name	Policy Definition	Rationale for NOT Including this Policy
P.ACCESS_BANNER	The TOE displays 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.	As is noted previously, this TOE is a wireless network interface card, which is installed as part of a larger system. As such, the TOE IT environment (e.g. operating system) is responsible for the display of appropriate banner information.

3.4 Security Function Policies

Several of the functional requirements in section 5.1 reference Security Function Policies (SFPs). Each SFP is listed in the table below with an explanation that supplies additional information and interpretation.

Table 5 - Security Function Policies

Name	Policy Definition
P.WIRELESS ENCRYPTION SFP	The users/access system administrators shall specify that the TOE encrypt/decrypt user data as it transits to/from wireless network.

4. Security Objectives

This section defines the security objectives of the TOE and its supporting environment. Security objectives, categorized as either IT security objectives or non-IT security objectives, reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified. All of the identified threats and organizational policies are addressed under one of the categories below.

4.1 Security Objectives for the TOE

Table 6 – TOE Security Objectives

Name	TOE Security Objective
O.ADMIN_GUIDANCE	The TOE provides administrators with the necessary information for secure management.
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security relevant events.
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.CORRECT_TSF_OPERATION	The TOE will provide the capability to verify the correct operation of the TSF.
O.CRYPTOGRAPHY	The TOE uses NIST FIPS 140-2 validated cryptographic services.
O.DOCUMENTED_DESIGN	The design of the TOE is adequately and accurately documented.
O.MANAGE	The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE.
O.PARTIAL_FUNCTIONAL_TESTING	The TOE will undergo partial security functional testing that demonstrates the TSF satisfies some of its security functional requirements.
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.VULNERABILITY_ANALYSIS	The TOE has undergone vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.

4.2 Security Objectives for the IT 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 7 – IT Environment Security Objectives

Name	TOE Environment Security Objective
OIE.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.
OIE.SELF_PROTECTION	The TOE IT environment 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 its their interfaces.

4.3 Security Objectives for the non-IT Environment

The following security objectives are intended to be satisfied by the non-IT environment of the TOE.

Table 8 – Non-IT Environment Security Objectives

Name	TOE Environment Security Objective
OE.NO_EVIL	Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.
OE.PHYSICAL	The IT environment will provide physical security, commensurate with the value of the TOE and the data it contains.

5. IT Security Requirements

5.1 TOE Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE, organized by CC class. The TOE Security Functional Requirements in this section of the ST are derived from the CC Part 2 Functional Requirements. These requirements consist of functional components from Part 2 of the CC as well as explicitly stated components derived from Part 2 of the CC, and assurance components from Part 3 of the CC. Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 9 - TOE Security Functional Requirements

Functional Class	Functional Components
Security Audit (FAU)	FAU_GEN.1-NIAP-0410 - Audit data generation
Cryptographic Support (FCS)	FCS_BCM_EXP.1 - Baseline Cryptographic Module
	FCS_CKM_EXP.2 - Cryptographic key establishment
	FCS_CKM.4 - Cryptographic key destruction
	FCS_COP_EXP.1 - Random Number Generation
	FCS_COP_EXP.2 - Cryptographic operation
User Data Protection (FDP)	FDP_IFC.1 - Subset information flow control (Wireless Encryption SFP)
	FDP_IFF.1-NIAP-0407 - Simple security attributes (Wireless Encryption SFP)
Identification & Authentication (FIA)	FIA_ATD.1 - User attribute definition
	FIA_UAU.2 - User authentication before any action
	FIA_UID.2 - User identification before any action
	FMT_SMF.1 (1) - Specification of Management Functions (Cryptographic Function)
	FMT_SMF.1 (2) - Specification of Management Functions (Cryptographic Key Data)
Protection of TSF (FPT)	FPT_TST_EXP.1 - TSF testing
	FPT_TST_EXP.2 - TSF testing of Cryptographic Modules

5.1.1 Security Audit (FAU) Requirements

5.1.1.1 FAU_GEN.1-NIAP-0410 - Audit data generation

FAU_GEN.1.1-NIAP-0410 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 listed in the following Table;
- c) No additional events

Table 10 - Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1-NIAP-0410	None	None
FCS_BCM_EXP.1	None	None
FCS_CKM_EXP.2	Error(s) detected during cryptographic key transfer	None
FCS_COP_EXP.1	None	None
FCS_COP_EXP.2	None	None
FMT_SMF.1(1)	Changing the TOE encryption algorithm including the selection not to encrypt communications	Encryption algorithm selected (or none)
FMT_SMF.1(2)	Changes to the cryptographic key data	None – the TOE SHALL NOT record cryptographic keys in the audit log.
FPT_TST_EXP.1	Execution of the self test	Success or Failure of test
FPT_TST_EXP.2	Execution of the self test	Success or Failure of test

FAU_GEN.1.2-NIAP-0410 The TSF shall record within each audit record at least the following information:

- a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [information specified in column three of the table in FAU_GEN.1.1-NIAP-0410].

5.1.2 Cryptographic Support (FCS) Requirements

5.1.2.1 FCS_BCM_EXP.1.1 - Baseline Cryptographic Module

FCS_BCM_EXP.1.1 All cryptomodules shall be FIPS PUB 140-2 validated, and perform the specified cryptographic functions in a FIPS-approved mode of operation.

FCS_BCM_EXP.1.2 The cryptomodule implemented shall have a minimum overall rating of FIPS PUB 140-2 Level 1.

5.1.2.2 FCS_CKM_EXP.2 - Cryptographic Key Establishment

FCS_CKM_EXP.2.1 The TSF shall provide the following cryptographic key establishment technique: Cryptographic Key Establishment using Manual Loading. The cryptomodule shall be able to accept key data as input and is prevented, by design, from outputting any cryptographic keys or CSPs in accordance with a specified manual cryptographic key distribution method using FIPS-approved Key Management techniques that meets the FIPS 140-2 Key Management Security Levels 1, Key Entry and Output.

5.1.2.3 FCS_CKM.4 - Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [cryptographic key zeroization method] that meets the following: [

- a) The Key Zeroization Requirements in FIPS PUB 140-2 Key Management Security Levels 1;
- c) Zeroization of all private cryptographic keys, plaintext cryptographic keys, key data, and all other critical cryptographic security parameters shall be immediate and complete; and
- d) The zeroization shall be executed by overwriting the key/critical cryptographic security parameter storage area three or more times with an alternating pattern.
- e) The TSF shall overwrite each intermediate storage area for private cryptographic keys, plaintext cryptographic keys, and all other critical security parameters three or more times with an alternating pattern
- f) upon the transfer of the key/CSPs to another location].

5.1.2.4 FCS_COP_EXP.1 – Random Number Generation

FCS_COP_EXP.1.1 The TSF shall perform all Random Number Generation used by the cryptographic functionality of the TSF using a FIPS-approved Random Number Generator implemented in a FIPS-approved cryptomodule running in a FIPS-approved mode.

5.1.2.5 FCS_COP_EXP.2 - Cryptographic operation

FCS_COP_EXP.2.1 A cryptomodule shall perform encryption and decryption using a FIPS-140-2 Approved algorithm operating in one or more FIPS 140-2 supporting minimum FIPS approved key sizes.

5.1.3 User Data Protection (FDP) Requirements

5.1.3.1 FDP_IFC.1 - Subset information flow control (Wireless Encryption SFP)

FDP_IFC.1.1 The TSF shall enforce the [Wireless Encryption SFP] on: [subjects: client, access point/system; information: network packets; operations: receive packet and transmit packet].

5.1.3.2 FDP_IFF.1-NIAP-0407 - Simple security attributes (Wireless Encryption SFP)

FDP_IFF.1.1-NIAP-0407 The TSF shall enforce the [Wireless Encryption SFP] based on the following types of subject and information security attributes: [encryption/decryption flag; direction of travel at the network interface].

FDP_IFF.1.2-NIAP-0407 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- If the encryption/decryption flag does NOT indicate that the TOE should perform encryption then all packets may pass without modification.
- If the direction of travel is from the operating system to the network interface and the encryption/decryption flag indicates the TOE should perform encryption, then the TOE must encrypt user data via FCS_COP_EXP.2.1 and if successful transmit the packet via the wireless interface.

- The direction of travel is from the network interface to the operating system and the encryption/decryption flag indicates the TOE should perform decryption then the TOE must decrypt user data via FCS_COP_EXP.2.1 and if successful pass that information to the operating system.
- [no additional information flow Wireless Encryption SFP Rules].

FDP_IFF.1.3-NIAP-0407 The TSF shall enforce the following information flow control rules: [no additional information flow control SFP rules].

FDP_IFF.1.4-NIAP-0407 The TSF shall provide the following [no additional SFP capabilities].

FDP_IFF.1.5-NIAP-0407 The TSF shall explicitly authorize an information flow based on the following rules: [no explicit authorization rules].

FDP_IFF.1.6-NIAP-0407 The TSF shall explicitly deny an information flow based on the following rules: [no explicit denial rules].

5.1.4 Identification and Authentication (FIA) Requirements

5.1.4.1 FIA_ATD.1 - User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following **minimum** list of security attributes belonging to individual users: [Username, Roles, and Authentication Credentials]. The Authentication Mechanisms (or Credentials) are shown in the Strength of Function section.

5.1.4.2 FIA_UAU.2 – User Authentication Before Any Action

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

5.1.4.3 FIA_UID.2 - User Identification Before Any Action

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.

5.1.5 Security Management (FMT) Requirements

5.1.5.1 FMT_SMF.1 (1) - Specification of Management Functions (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_EXP.2) in conformance with the Wireless Encryption SFP].

5.1.5.2 FMT_SMF.1 (2) - Specification of Management Functions (Cryptographic Key Data)

FMT_SMF.1.1(2) The TSF shall be capable of performing the following security management functions: [set, modify, and delete the cryptographic keys and key data in support of the Wireless Encryption SFP and enable/disable verification of cryptographic key testing].

5.1.6 Protection of TSF (FPT) Requirements

5.1.6.1 FPT_TST_EXP.1 - TSF Testing

FPT_TST_EXP.1.1 The TSF shall run a suite of self-tests during initial start-up, to demonstrate the correct operation of the software portions of the TSF.

FPT_TST_EXP.1.2 The TSF shall provide the capability to use a TSF-provided cryptographic function to verify the integrity of all TSF data except the following: audit data *and any cached data*. This is accomplished through a FIPS 140-2 Integrity Check.

FPT_TST_EXP.1.3 The TSF shall provide the capability to use a TSF-provided cryptographic function to verify the integrity of stored TSF executable code.

5.1.6.2 FPT_TST_EXP.2 - TSF testing of Cryptographic Modules

FPT_TST_EXP.2.1 The TSF shall run the self-test suite provided by the FIPS 140-2 cryptomodule during initial start-up (power on) and upon request, to demonstrate the correct operation of the cryptographic components of the TSF.

5.2 IT Environment Security Requirements

The IT environment security requirements define functional and/or assurance requirements to be satisfied by the IT environment. The IT environment includes the authentication server, the management console, and the audit collection server, and authorized IT entities (e.g., a certificate authority server, NTP server).

Table 11 - IT Environment Security Functional Requirements

Functional Class	Functional Components
Protection of TSF (FPT)	FPT_RVM.1 Non-Bypassability of the TSP
	FPT_SEP.1 TOE IT Environment Domain Separation
	FPT_STM.1 Reliable time stamps

5.2.1 Protection of TSF (FPT) Requirements

5.2.1.1 FPT_RVM.1 – Non-bypassability of the TSP

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

5.2.2 TOE IT Environment Domain Separation

5.2.2.1 FPT_SEP.1 – TOE IT Environment Domain Separation

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

5.2.3 Reliable Time Stamps

5.2.3.1 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.

5.3 TOE Security Assurance Requirements

The TOE security assurance requirements summarized in the table below identify the management and evaluative activities required to address the threats and policies identified in this document. Section 7.3 provides a justification for the chosen security assurance requirements and the selected assurance level EAL2 augmented with, ACM_SCP.1 (CM Coverage), ALC_FLR.2 (Flaw Remediation), and AVA_MSU.1 (Misuse – Examination of guidance). The Security Assurance Requirements for the TOE are taken from Part 3 of the Common Criteria. None of the assurance components are refined. The assurance components are listed in Table 13.

Table 12- TOE Security Assurance Requirements

Assurance Class	Assurance Components
Configuration Management (ACM)	ACM_CAP.3 Authorization controls as modified by NIAP Interpretation I-0412
	ACM_SCP.1 TOE CM coverage
Delivery and Operation (ADO)	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Development (ADV)	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Guidance Documents (AGD)	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance

Assurance Class	Assurance Components
Life cycle support (ALC)	ALC_FLR.2 Flaw reporting procedures
Tests (ATE)	ATE_COV.1 Evidence of Coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Vulnerability assessment (AVA)	AVA_MSU.1 Examination of guidance
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

5.4 Strength of Function

The overall strength of function requirement is SOF-basic. The strength of function requirement applies to FIA_UAU.2. The SOF claim for FIA_UAU.2 is SOF-basic. The strength of the “secrets” mechanism is consistent with the objective of the TOE’s management O.MANAGE and O.VULNERABILITY_ANALYSIS. Strength of Function shall be demonstrated for the non-certificate based authentication mechanisms to be SOF-basic, as defined in Part 1 of the CC. Specifically, the local authentication mechanism must demonstrate adequate protection against attackers possessing a low-level attack potential. Strength of Function has been documented in the Crypto Client FIPS 140-2 Security Policy as follows:

Authentication Mechanism	Strength of Mechanism
Userid and password	Minimum 6 characters => $72^6 = 1.39E11$
Static Key (TDES or AES)	TDES (192-bits) or AES (128, 192, or 256-bits)
CA signature	128-bit
AES CCM Passphrase	Minimum 8 characters => $72^8 = 7.22E14$
EAP-TLS	CA signature => 128-bit

A SOF-Basic analysis is provided as follows:

Pass-word length	Combination of characters using Alpha+numeric+special characters = 94	Attempts to crack per sec	Attempt to crack retry rate	Seconds to Crack	Days to Crack	Years to Crack
6	$94^6 = 689,869,781,056$	500	2 ms	1,379,739,562	15,969	43.8
6	689,869,781,056	1,000	1 ms	689,869,781	7,984	21.8
6	689,869,781,056	5,000	200 us	137,973,956	1,597	4.3
6	689,869,781,056	10,000	10 us	68,986,978	798	2.2

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

Each of the security function descriptions is organized by the security requirements corresponding to the security function. Hence, each function is described by describing how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions are suitable to satisfy the necessary requirements.

6.1.1 Security Audit

6.1.1.1 FAU_GEN.1-NIAP-0410

The TOE collects audit data and provides an interface for authorized administrators to review generated audit records. All audit records include the date/time of the event, the identity associated with the event (such as the service, computer or user), the success/failure of the event and a definition of the event (by code or explanation).

The start and stop of the audit service is noted in the audit record. Additional information about recorded events can be found in Table 10 - Auditable Events.

Auditing is automatically started when the computer starts and can not be disabled. Audit records are accessible through the operating system where the TOE is installed (audit records are not stored within the TOE itself).

6.1.2 Cryptographic Support

6.1.2.1 FCS_BCM_EXP.1

The TOE has undergone FIPS 140-2 Level 1 validation and is in the NIST FIPS 140-2 prevalidation queue.

6.1.2.2 FCS_CKM_EXP.2

The TOE has undergone FIPS 140-2 Level 1 validation and is in the NIST FIPS 140-2 prevalidation queue.. The TOE supports the manual input of the cryptographic keys used for secure encryption on the wireless network by the Crypto-Officer. Only the Crypto-Officer can enter the keys, and these keys are the only ones allowed to be used.

6.1.2.3 FCS_CKM.4

Zeroization Mechanism: Key Zeroization is performed by writing an all five pattern "55555..." into the Key Data Field being zeroized exactly one time, followed by writing an all A pattern "AAAAA..." into the Key Data Field being zeroized exactly one time, followed by writing an all five pattern "55555..." into the Key Data Field being zeroized exactly one time, followed by writing an all zero pattern "00000..." into the Key Data Field being zeroized exactly one time.

6.1.2.4 FCS_COP_EXP.1

As part of the FIPS 140-2 Level 1 validation effort, the random number generator has been evaluated to the FIPS 186-2 specification and has been given certificate #67.

6.1.2.5 FCS_COP_EXP.2

The TOE has undergone FIPS 140-2 Level 1 validation and is in the NIST FIPS 140-2 prevalidation queue.. The AES algorithm has been validated against FIPS 197 for key lengths of 126- 192- and 256-bit. The 3DES algorithm as been validated against FIPS 46-3 for 192-bit keys.

6.1.3 User Data Protection

6.1.3.1 FDP_IFC.1 & FDP_IFF.1-NIAP-0407

The TOE secures the transmission of wireless data through the implementation of the Wireless Encryption information flow control policy.

The Wireless Encryption SFP is used to specify the level of protection of data being transmitted on the wireless network. The Policy requires that the specified encryption algorithm (either AES or 3DES) be used to encrypt/decrypt traffic if protection of the wireless system is enabled. This policy ensures that traffic which is to be protected is properly encrypted before it can be sent on the wireless network. The authentication/authorization of the client is set by the administrator, and can be based on certificates (EAP-TLS), WEP or WPA shared secrets, RADIUS, MAC address or none (if no encryption is specified for the network).

6.1.4 Identification and Authentication

6.1.4.1 FIA_ATD.1

To provide security for the configuration of the TOE, all administrators must first authenticate to the TOE before any access is granted to the management interface. There is one Crypto-Officer account as well as up to 5 administrator accounts, each of which are assigned a password. The username and password must be entered correctly to provide access to the configuration. The Authentication Mechanisms (or Credentials) are shown in the Strength of Function section.

6.1.4.2 FIA_UAU.2 & FIA_UID.2

The TOE provides authentication services for administrative access to the configuration settings of the TOE. All access to the configuration is blocked until the user has successfully logged into the administrative application. The user must authenticate as either the Crypto-Officer or the Administrator. The Crypto-Officer has full access to all security settings, while the Administrator has more restricted access and can not change the security settings of the TOE.

6.1.5 Security Management

6.1.5.1 FMT_SMF.1(2)

The Crypto-Officer is able to specify the cryptographic keys used to protect the traffic on the WLAN. This information can only be set by the Crypto-Officer, who may also review the keys and change them at any time (though they must also be changed on the Wireless Access Point to maintain WLAN connectivity).

The TOE provides an administrator with the ability to manage the security functions through a locally installed application. The TOE has two accounts, each with a separate role: the Crypto-Officer and the Administrator. The Crypto-Officer role has full access to the entire security configuration while the Administrator role has more limited access and can not change any security settings. Through the management interface, the Crypto-Officer can initialize and configure all security settings such as the encryption settings for wireless traffic.

6.1.6 Protection of the TSF

6.1.6.1 FPT_TST_EXP.1

The TOE performs a series of tests on startup to verify the integrity of the software using FIPS-approved integrity checking techniques. These tests are used to assure the correct security functionality when the TOE is active. The results of these tests are written into the audit records of the installed operating system (i.e. the Event Log). These tests are started automatically when the computer is turned on and the drivers necessary for WLAN connectivity are loaded by the operating system.

These tests are only performed on the software itself, and not the configuration, audit records, or any other data that may be generated by the use of the TOE.

Tests can be performed at any time by restarting the computer where the TOE is installed.

6.1.6.2 FPT_TST_EXP.2

To ensure the proper operation of the TOE, startup self-tests are performed automatically on the TOE software when the computer starts. These tests include AES-MAC integrity checks to ensure the software, including the driver, cryptomodule and all other components, has not been tampered (or damaged), which are run as the software is loaded into memory by the operating system. The cryptomodule also performs KATs on the encryption algorithms and a continuous RNG test to ensure randomness of the RNG.

Tests can be performed at any time by restarting the computer where the TOE is installed.

6.2 TOE Security Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL2+ assurance requirements: (a) Configuration Management, (b) Delivery and Operations, (c) Development, (d) Guidance Documents, (e) Life-Cycle Support, (f) Tests, (g) Vulnerability Assessment.

6.2.1 Configuration Management

The configuration management measures applied by 3eTI ensure that configuration items are uniquely identified and the TOE is uniquely labeled. These activities are documented in 3eTI Standard Operating Procedures (SOPs) as follows:

- 00000112-001 Design Release and Change Control Procedure
- 00000121-001 Project-Related Document Control Procedure
- 00000139-002 Software Configuration Management Procedure

Assurance Requirements: ACM_CAP.3, ACM_SCP.1.

6.2.2 Delivery and Operations

3eTI provides delivery documentation and procedures to identify the TOE, facilitate detection of unauthorized modifications of the TOE and to provide installation and generation instructions at start-up. 3eTI's delivery procedures describe the methods to be used for the secure installation, generation, and start-up of the TOE. Crypto-Officer and Administrator guidance and operation procedures are also included. These procedures are documented in the 3e-010F-A-2 User's Guide and the 3e-010F-C-2 User's Guide.

Assurance Requirements: ADO_DEL.1, ADO_IGS.1.

6.2.3 Development

3eTI provides design documentation that identifies and describes the external interfaces and the decomposition of the TOE into subsystems. The design documentation consists of the following documents and various references from these documents:

- 3e-010F-A-2 Internal Specification Sheet (satisfies ADV_FSP.1, ADV_RCR.1)
- 3e-010F-C-2 Internal Specification Sheet (satisfies ADV_FSP.1, ADV_RCR.1)
- 22000209-702 3e-010F-A-2 & 3e-010F-C-2 Client Software Functional Specification (satisfies ADV_FSP.1)
- 22000209-703 3e-010F-A-2 & 3e-010F-C-2 Client Software High Level Design (satisfies ADV_FSP.1)

Assurance Requirements: ADV_FSP.1, ADV_HLD.1, ADV_RCR.1.

6.2.4 Guidance Documents

3eTI provides guidance documentation to instruct the Crypto-Officer, Administrator, and Users in operating the TOE safely and securely. The guidance documentation is contained in the 3e-010F-A-2 User's Guide and the 3e-010F-C-2 Security Server User's Guide.

Assurance Requirements: AGD_ADM.1, AGD_USR.1.

6.2.5 Life-Cycle Support

TOE users need to understand how to submit security flaw reports to the developer. 3eTI provides flaw remediation guidance to the user through the following SOP's (Standard Operating Procedures):

- 00000106-001 Defect Management Procedure
- 00000112-001 Design Release and Change Control Procedure

Assurance Requirements: ALC_FLR.2.

6.2.6 Tests

3eTI provides test documentation that describes how each of the TOE security functions is tested, as well as the actual results of applying the tests. The test documentation consists of the following documents:

- 29000201-715 3e-525A-3 Access System & 3e-010F-C-2 and 3e-010F-A-2 Crypto-Clients Test Plan

Assurance Requirements: ATE_COV.1, ATE_FUN.1, ATE_IND.2.

6.2.7 Vulnerability Assessment

3eTI provides examination of guidance and vulnerability analyses of the entire TOE in support of CC requirements. The objective of the examination of guidance is to ensure that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. Examination of guidance has been performed on the 3e-010F-A-2 User's Guide and the 3e-010F-C-2 Security Server User's Guide.

3eTI performs systematic vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE. The vulnerability analysis is documented in:

- 22000209-720 3e-010F-A-2 & 3e-010F-C-2 Client Software Vulnerability Analysis

Assurance Requirements: AVA_MSU.1, AVA_SOF.1; AVA_VLA.1.

6.3 Strength of Function

The Strength of Function claim is SOF-Basic based on the overall TOE. Authentication by a password, specifically regarding FIA_UAU.2 is realized by a probabilistic or permutational mechanism. The methods used to provide difficult-to-guess passwords are probabilistic. Strength of Function has been documented in the Crypto Client FIPS 140-2 Security Policy as follows:

Authentication Mechanism	Strength of Mechanism
Userid and password	Minimum 6 characters => $72^6 = 1.39E11$
Static Key (TDES or AES)	TDES (192-bits) or AES (128, 192, or 256-bits)
CA signature	128-bit
AES CCM Passphrase	Minimum 8 characters => $72^8 = 7.22E14$
EAP-TLS	CA signature => 128-bit

A SOF-Basic analysis is provided as follows:

Pass-word length	Combination of characters using Alpha+numeric+special characters = 94	Attempts to crack per sec	Attempt to crack retry rate	Seconds to Crack	Days to Crack	Years to Crack
6	$94^6 = 689,869,781,056$	500	2 ms	1,379,739,562	15,969	43.8
6	689,869,781,056	1,000	1 ms	689,869,781	7,984	21.8
6	689,869,781,056	5,000	200 us	137,973,956	1,597	4.3
6	689,869,781,056	10,000	10 us	68,986,978	798	2.2

7. Rationale

This section describes the rationale for the Security Objectives and Security Functional Requirements as defined in Sections 3 and 4, respectively. This section also describes the rationale for not satisfying all of the dependencies and the rationale for the strength of function (SOF) claim.

7.1 Security Objectives Rationale

7.1.1 TOE, IT Environment and non-IT Environment Security Objectives Rationale

This section shows that all threats and organizational security policies are completely covered by security objectives. In addition, each objective counters or addresses at least one, organizational security policy, or threat.

Table 13 - Security Objectives to Assumptions, Threats and Policies Mappings

	O.ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.CONFIGURATION_IDENTIFICATION	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.DOCUMENTED_DESIGN	O.MANAGE	O.PARTIAL_FUNCTIONAL_TESTING	O.RESIDUAL_INFORMATION	O.VULNERABILITY_ANALYSIS	OIE.TIME_STAMPS	OIE.SELF_PROTECTION	OE.NO_EVIL	OE.PHYSICAL
A.NO_EVIL													X	
A.PHYSICAL														X
T.ACCIDENTAL_ADMIN_ERROR	X													
T.ACCIDENTAL_CRYPTO_COMPROMISE					X			X				X		
T.POOR_DESIGN						X			X					
T.POOR_IMPLEMENTATION			X				X		X					
T.POOR_TEST			X	X			X		X					
T.RESIDUAL_DATA								X						
T.TSF_COMPROMISE							X	X				X		
P.ACCOUNTABILITY		X						X		X				
P.CRYPTOGRAPHY					X									

7.1.1.1 T.ACCIDENTAL_ADMIN_ERROR

An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

O.ADMIN_GUIDANCE helps to mitigate this threat by ensuring that 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.

7.1.1.2 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 contributes to the mitigation of this threat by ensuring that neither the TOE or the TOE IT environment will insert critical data (including data related to encryption) and executable code as padding in network packet objects. In addition, **FCS_CKM_EXP.2** and **FCS_CKM.4** ensure that FIPS 140-2 procedures are followed when cryptographic keys are handled and destroyed. **OIE.SELF_PROTECTION** ensures that the TOE IT environment will protect the TOE and itself from users.

7.1.1.3 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.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 responsible for TOE development understand the overall design of the TOE. This in turn decreases the likelihood of design flaws and increases the chances 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.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. **O.VULNERABILITY_ANALYSIS** ensure that the TOE has been analyzed for obvious vulnerabilities and that any vulnerabilities found have been removed or otherwise mitigated.

7.1.1.4 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 plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE design. This ensures that changes to the TOE are performed in structure manner and tracked. **O.PARTIAL_FUNCTIONAL_TESTING ATE_COV.1** ensures that the developers testing of the TOE is sufficiently addressing all TOE Security Functional requirements. **ATE_IND.2** contributes to removing this threat by ensuring that the security relevant portions of the TOE have been tested against the security functional requirements. **O.VULNERABILITY_ANALYSIS** ensures that the TOE has been analyzed for obvious vulnerabilities and that the TOE is resistant to casually mischievous users.

7.1.1.5 T.POOR_TEST

Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered thereby causing potential security vulnerabilities.

O.PARTIAL_FUNCTIONAL_TESTING contributes to removing this threat by ensuring that the security relevant portions of the TOE have been tested against the security functional requirements. **O.CORRECT_TSF_OPERATION** ensures that users can verify the continued correct operation of the TOE after it has been installed in its target environment. **O.VULNERABILITY_ANALYSIS** ensures that the TOE has been analyzed and tested to demonstrate that it is resistant to obvious vulnerabilities.

7.1.1.6 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 contributes to the mitigation of this threat by ensuring that network packet objects are cleared prior to use. In addition, **FCS_CKM_EXP.2** and **FCS_CKM.4** ensure that FIPS 140-2 is followed and objects used to store cryptographic keys are overwritten when those keys are no longer needed.

7.1.1.7 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 mitigates this threat by restricting access to administrative functions and TSF data to the administrator. **O.RESIDUAL_INFORMATION** and **OIE.SELF_PROTECTION** requires that the TOE IT environment be able to protect itself and the TOE 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.

7.1.1.8 P.ACCOUNTABILITY

The authorized users of the TOE shall be held accountable for their actions within the TOE.

O.AUDIT_GENERATION ensures that the TOE is capable of generating records of audit events. **O.MANAGE** ensures that the administrator can enable or disable the audit function. **OIE.TIME_STAMPS** plays a role in supporting this policy by requiring the TOE IT environment provide a reliable time stamp (configured locally by the Administrator or via an external NTP server). The audit mechanism is required to include the current date and time in each audit record.

7.1.1.9 P.CRYPTOGRAPHY

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).

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 140-2.

7.1.2 Non-IT Environment Security Objectives Rationale

7.1.2.1 A.NO_EVIL

Administrators are non-hostile, appropriately trained and follow all administrator guidance.

The **OE.NO_EVIL** objective ensures that only non-hostile, competent administrators (following guidance) manage the TOE.

7.1.2.2 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.

The **OE.PHYSICAL** objective provides for the physical security of the TOE.

7.2 Security Requirements Rationale

7.2.1 TOE Security Requirements Rationale

Table 14 - Rationale for TOE Security Requirements

	O.ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.CONFIGURATION_IDENTIFICATION	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.DOCUMENTED_DESIGN	O.MANAGE	O.PARTIAL_FUNCTIONAL_TESTING	O.RESIDUAL_INFORMATION	O.VULNERABILITY_ANALYSIS
FAU_GEN.1-NIAP-0410		X								
FCS_BCM_EXP.1					X					
FCS_CKM_EXP.2					X			X		
FCS_CKM.4					X			X		
FCS_COP_EXP.1					X					
FCS_COP_EXP.2					X					

	O.ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.CONFIGURATION_IDENTIFICATION	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.DOCUMENTED_DESIGN	O.MANAGE	O.PARTIAL_FUNCTIONAL_TESTING	O.RESIDUAL_INFORMATION	O.VULNERABILITY_ANALYSIS
FDP_IFC.1					X					
FDP_IFF.1-NIAP-0407					X					
FIA_ATD.1							X			
FIA_UAU.2							X			
FIA_UID.2							X			
FMT_SMF.1 (1)							X			
FMT_SMF.1 (2)							X			
FPT_TST_EXP.1				X						
FPT_TST_EXP.2				X						
ACM_CAP.3			X							
ACM_SCP.1			X							
ADO_DEL.1	X									
ADO_IGS.1	X									
ADV_FSP.1						X				
ADV_HLD.1						X				
ADV_RCR.1						X				
AGD_ADM.1	X									
AGD_USR.1	X									
ALC_FLR.2			X							
ATE_COV.1							X			
ATE_FUN.1							X			
ATE_IND.2							X			
AVA_MSU.1	X									
AVA_SOF.1										X
AVA_VLA.1										X

7.2.1.1 O.ADMIN_GUIDANCE

The TOE will provide administrators with the necessary information for secure management.

ADO_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 **ADO_IGS.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_ADM.1** requirement ensures that the developer provides the administrator with guidance on how to operate the TOE in a secure manner. This includes describing the interfaces used in managing the TOE, and any security parameters that are configurable by the administrator. The documentation also provides a description of how to setup and review the auditing features of the TOE. **AGD_USR.1** is intended for non-administrative users. If the TOE provides facilities/interfaces for this type of user, this guidance will describe how to use those interfaces securely. **AVA_MSU.1** ensures that the guidance documentation can be followed unambiguously to ensure the TOE is not misconfigured in an insecure state due to confusing guidance.

7.2.1.2 O.AUDIT_GENERATION

The TOE will provide the capability to detect and create records of security-relevant events.

FAU_GEN.1-NIAP-0410 defines the set of events that the TOE must be capable of recording. This requirement ensures that the Security 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.

7.2.1.3 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.

ACM_CAP.3 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. **ACM_SCP.1** 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 those discovered 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.

7.2.1.4 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_EXP.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_EXP.2** 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.

7.2.1.5 O.CRYPTOGRAPHY

The TOE shall use NIST FIPS 140-2 validated cryptographic services.

The FCS requirements satisfy this objective by levying requirements that ensure the cryptographic standards include the NIST FIPS publications (where possible) and NIST approved ANSI standards. The intent is to have the satisfaction of the cryptographic standards be validated through a NIST FIPS 140-2 validation.

FCS_BCM_EXP.1 is an explicit requirement that specifies the NIST FIPS rating level that the cryptographic module must satisfy. The level specifies the degree of testing of the module. The higher the level, the more extensive the module is tested. **FCS_CKM_EXP.2** Cryptographic Key Handling and Storage requires that FIPS PUB 140-2 be satisfied when performing key entry and output. **FCS_CKM.4** mandates the standards (FIPS 140-2) that must be satisfied when the TOE performs Cryptographic Key Zeroization. **FCS_COP_EXP.1** requires that for any cryptomodule implemented in the TOE use a FIPS-approved random number generator when it is necessary to generate random numbers. **FCS_COP_EXP.2** requires that for data decryption and encryption that the NIST approved Advanced Encryption Standard - Rijndael (AES) algorithm be used, and that the algorithm meets the FIPS PUB 140-2, FIPS PUB 197 standard. **FDP_IFC.1** and **FDP_IFF.1-NIAP-0407** identify the policy that the TOE must implement to encrypt/decrypt user data.

7.2.1.6 O.DOCUMENTED_DESIGN

The design of the TOE is adequately and accurately documented.

ADV_FSP.1 requires that the security relevant interfaces to the TSF be completely specified. In this TOE, a complete specification of the network interface is critical in understanding what functionality is presented to untrusted users and how that functionality fits into the enforcement of security policies. Having a complete understanding of what is available at the TSF interface allows one to analyze this functionality in the context of design flaws. **ADV_HLD.1** requires that a high-level design of the TOE be provided. This level of design describes the architecture of the TOE in terms of subsystems. It identifies which subsystems are responsible for making and enforcing security relevant (e.g., anything relating to an SFR) decisions and provides a description, at a high level, of how those decisions are made and enforced. Having this level of description helps to provide a general understanding of the TOE and how it functions. **ADV_RCR.1** is used to ensure that the decomposition of the TOE's design are consistent with one another. This is important, since design decisions that are analyzed and made at one level (high level design) that are not correctly or completely realized at a lower level (the functional specification) may lead to a design flaw. This requirement helps in the design analysis to ensure design decisions are realized at across the design. A complete and accurate description of the TOE design is critical to understanding the TOE design. It is this understanding, gained is from the design analysis, which the evaluator relies upon during testing and vulnerability analysis activities.

7.2.1.7 O.MANAGE

The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE.

FMT requirements are used to satisfy the management objective as well as other objectives that specify the control of functionality. The requirement's rationale for this objective focuses on the administrator's capability to perform management functions in order to control the behavior of security functions.

FIA_ATD.1 ensures that the TOE has accounts with authentication credentials for administration which will require authentication to be able to manage the settings on the client. **FIA_UAU.2** and **FIA_UID.2** require that users authenticate specifically to the TOE before any access to the management functions is allowed. No access to the security settings is allowed without a successful login. **FMT_SMF.1(1)** and **FMT_SMF.1(2)** ensure that the administrator has the ability to control the use of encryption when the TOE is communicating with external systems.

7.2.1.8 O.PARTIAL_FUNCTIONAL_TESTING

The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.

In order to satisfy O.FUNCTIONAL_TESTING, the ATE class of requirements is necessary.

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 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.

7.2.1.9 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.

FCS_CKM_EXP.2 places requirements on how cryptographic keys are managed within the TOE. This requirement places restrictions 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) 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 that the content of these keys cannot possibly be disclosed when a resource is reallocated to a user.

7.2.1.10 O.VULNERABILITY_ANALYSIS

The TOE will undergo some vulnerability analysis to demonstrate that the design and implementation of the TOE does not contain any obvious flaws.

AVA_VLA.1 requires the developer to perform a search for obvious vulnerabilities in all the TOE deliverables. The developer must then document the disposition of those obvious vulnerabilities. The evaluator then builds upon this analysis during vulnerability testing. This component provides the confidence that obvious security flaws have been either removed from the TOE or otherwise mitigated. **AVA_SOF.1** requires that any permutational or probabilistic mechanism in the TOE be analyzed and be found to be resistant to attackers possessing a "low" attack potential. This provides confidence those security mechanisms vulnerable to guessing type attacks are resistant to casual attack.

7.2.2 IT Environment Security Requirements Rationale

Table 15 - Rationale for Requirements on the TOE IT Environment

	OIE.SELF_PROTECTION	OIE.TIME_STAMPS
FPT_RVM.1	X	
FPT_SEP.1	X	
FPT_STM.1		X

7.2.2.1 OIE.SELF_PROTECTION

The TOE IT environment 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 its their interfaces.

FPT_SEP.1 ensures that the TOE IT environment provides a domain that protects itself and the TOE from untrusted users. Since the TOE is a component of a larger system, it cannot protect itself and must rely on the IT environment. If the IT environment cannot protect both itself and the TOE, then the TOE cannot be relied upon to enforce its security policies. The inclusion of **FPT_RVM.1** ensures that the TOE is able to make policy decisions on all packets passing between the TOE IT environment and the Wireless LAN. Without this non-bypassability requirement, the TOE could not be relied upon to completely enforce the security policies, since an interface(s) may otherwise exist that would provide a user with access to Wireless LAN regardless of the defined policies. Since the TOE is a component of a larger system, the TOE by itself cannot enforce FPT_RVM.

7.2.2.2 OIE.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.

7.3 Rationale for Assurance Requirements

The Security Assurance Requirements components in this ST are derived from Part 3 of the CC.

EAL2 augmented was chosen to ensure a confidence in security services used to protect information in a Basic Robustness Environment. The assurance selection was based on (a) recommendations documented in the GIG and (b) 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 with, ACM_SCP.1 (TOE CM Coverage), ALC_FLR.2 (Flaw Remediation), and AVA_MSU.1 (Misuse – Examination of Guidance).) was believed to best achieve this goal. The sponsor concluded that EAL2 augmented is applicable since this ST 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 ST 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.

7.4 Requirement Dependency Rationale

The table below provides a mapping of security functional requirements and illustrates that all dependencies have been included within this ST.

Table 16 - TOE Security Functional Requirement Dependencies

Requirement Number	Functional Requirements	Dependencies	Dependency	Dependency Met
1	FAU_GEN.1-NIAP-0410	FPT_STM.1	18	X
2	FCS_BCM_EXP.1	No dependencies	-	X
3	FCS_CKM_EXP.2	FMT_MSA.2	-	Rationale
4	FCS_CKM.4	FDP_ITC.1 or FCS_CKM.1	-	Rationale
		FMT_MSA.2	-	
5	FCS_COP_EXP.1	FDP_ITC.1 or FCS_CKM.1	-	Rationale
		FCS_CKM.4	4	X
		FMT_MSA.2	-	Rationale
6	FCS_COP_EXP.2	FDP_ITC.1 or FCS_CKM.1	-	X
		FCS_CKM.4	4	X
		FMT_MSA.2	-	X
7	FDP_IFC.1	FDP_IFF.1	8	X
8	FDP_IFF.1-NIAP-0407	FDP_IFC.1	7	X
		FMT_MSA.3	-	Rationale
9	FIA_ATD.1	No dependencies	-	X
10	FIA_UAU.2	FIA_UID.1	11	X
11	FIA_UID.2	FIA_UAU.1	10	X
12	FMT_SMF.1(1)	No dependencies	-	X
13	FMT_SMF.1(2)	No dependencies	-	X
14	FPT_TST_EXP.1	No dependencies	-	X
15	FPT_TXT_EXP.2	No dependencies	-	X
16	FPT_RVM.1	No dependencies	-	X
17	FPT_SEP.1	No dependencies	-	X
18	FPT_STM.1	No dependencies	-	X

7.5

7.6 Rationale for Not Satisfying All Dependencies

Each functional requirement, including explicit 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. Table identifies the functional requirement, its correspondent dependency and the analysis and rationale for not supporting the dependency in this ST.

Table 17 - Unsupported Dependency Rationale

Requirement	Unsatisfied Dependencies	Dependency Analysis and Rationale
FCS_CKM_EXP.2	FCS_CKM.1	In the context of FCS_CKM_EXP.2, the FCS_CKM.1 requirement allows the ST author to specify key generation standards for cryptographic keys used by the TOE. Since the WLAN client TOE is not expected to generate keys, this requirement has been omitted. Note: this ST specifies manual key entry.
	FMT_MSA.2	The FMT_MSA.2 requirement simply states that "The TSF shall ensure that only secure values are accepted for security attributes". In the context of FCS_CKM_EXP.2, it is not clear what security attributes/secure values are associated with handling cryptographic keys. Therefore this requirement has been omitted.
FCS_CKM.4	FCS_CKM.1	In the context of FCS_CCP_EXP.1, the FCS_CKM.1 requirement allows the ST author to specify key generation standards using FIPS PRNG functionality for cryptographic keys used by the TOE. Since the WLAN client TOE is not expected to generate keys, this requirement has been omitted. Note: this ST specifies manual key entry.
	FMT_MSA.2	The FMT_MSA.2 requirement simply states that "The TSF shall ensure that only secure values are accepted for security attributes". In the context of FCS_CKM.4, key zeroization clears keys and secure values for loading do not apply to the zeroization. Therefore this requirement has been omitted.
FCS_COP_EXP.1	FCS_CKM.1	In the context of FCS_CCP_EXP.1, the FCS_CKM.1 requirement allows the ST author to specify key generation standards using FIPS PRNG functionality for cryptographic keys used by the TOE. Since the WLAN client TOE is not expected to generate keys, this requirement has been omitted. Note: this ST specifies manual key entry.
	FMT_MSA.2	The FMT_MSA.2 requirement simply states that "The TSF shall ensure that only secure values are accepted for security attributes". In the context of FCS_CKM_EXP.2, it is not clear what security attributes/secure values are associated with handling cryptographic keys. Therefore this requirement has been omitted.
FCS_COP_EXP.2	FCS_CKM.1	In the context of FCS_CCP_EXP.1, the FCS_CKM.1 requirement allows the ST author to specify key generation standards using FIPS PRNG functionality for cryptographic keys used by the TOE. Since the WLAN client TOE is not expected to generate keys, this requirement has been omitted. Note: this ST specifies manual key entry.
	FMT_MSA.2	The FMT_MSA.2 requirement simply states that "The TSF shall ensure that only secure values are accepted for security attributes". In the context of FCS_CKM.4, key zeroization clears keys and secure values for loading do not apply to the zeroization. Therefore this requirement has been omitted.
FDP_IFC.1	FMT_MSA.3	The FDP_IFC.1 requirement specifies the Wireless Encryption SFP. The FMT_MSA.3 allows the ST author to specify secure default values for that policy. However, since the FMT_SMF.1(1) provides the ability to set the policy. The ability to set a secure initial default value (e.g. decrypt by default) is not necessary.
FDP_IFF.1-NIAP-0407	FMT_MSA.3	The FDP_IFF.1-NIAP-0407 requirement specifies the Simple Security Attributes Wireless Encryption SFP. The FMT_MSA.3 allows the ST author to specify secure default values for that policy. However, since the FMT_SMF.1(1) provides the ability to set the policy. The ability to set a secure initial default value (e.g. decrypt by default) is not necessary.

7.7 Explicitly Stated Requirements Rationale

Table 18 - Rationale for Explicit Requirements

Explicit Requirement	Identifier	Rationale
FCS_BCM_EXP.1	Baseline Cryptographic Module	This explicit requirement is necessary since the CC does not provide a means to specify a cryptographic baseline of implementation. This explicit requirement is also necessary because it describes requirements for a FIPS 140-2 validated cryptomodule rather than the entire TSF.
FCS_CKM_EXP.2	Cryptographic Key Establishment	This explicit requirement is necessary because it describes requirements for a FIPS 140-2 validated cryptomodule rather than the entire TSF. The TOE has undergone FIPS 140-2 Level 1 validation and is in the NIST FIPS 140-2 prevalidation queue.
FCS_COP_EXP.1	Random Number Generation	This explicit requirement is necessary since the CC cryptographic operation components are focused on specific algorithm types and operations requiring specific key sizes.
FCS_COP_EXP.2	Cryptographic Operation (Encryption/Decryption Using AES)	This explicit requirement is necessary because it describes requirements for a FIPS 140-2 validated cryptomodule rather than the entire TSF.

Explicit Requirement	Identifier	Rationale
FPT_TST_EXP.1	TSF Testing	This explicit requirement is necessary because, as identified in the US Government ST Guidance for Basic Robustness, there are several issues with the CC version of FPT_TST.1. First, the wording of FPT_TST.1.1 appears to make sense only if the TOE includes hardware; it is difficult to imagine what software TSF "self-tests" would be run. Secondly, some TOE data are dynamic (e.g., data in the audit trail, passwords) and so interpretation of "integrity" for FPT_TST.1.2 is required, leading to potential inconsistencies amongst Basic Robustness TOEs. Therefore, the explicit requirements are used in this ST.
FPT_TST_EXP.2	Testing of Cryptographic Modules	This explicit requirement is necessary because the basic self test requirement does not specify the required elements for testing of cryptographic functions, as called out in this explicit requirement.
FAU_GEN.1-NIAP-0410	Audit Data Generation	Used from CC Basic Robustness Guide
FDP_IFF.1-NIAP-0407	Simple Security Attributes (Wireless Encryption SFP)	Used from CC Basic Robustness Guide

When a SFR has the "-NIAP-xxxx" extension it is considered to be explicitly stated. These explicitly stated requirements are derived from the CC Basic Robustness Guide.

7.8 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

7.9 Strength of Function Rationale

Part 1 of the CC defines "strength of function" in terms of the minimum efforts assumed necessary to defeat the expected security behavior of a TOE security function. There are three strength of function levels defined in Part 1: SOF-basic, SOF-medium and SOF-high. SOF-basic is the strength of function level chosen for this ST. SOF-basic states, "a level of the TOE strength of function where analysis shows that the function provides adequate protection casual breach of TOE by attackers possessing a low attack potential." The rationale for choosing SOF-basic was to be consistent with the TOE objective O.VULNERABILITY_ANALYSIS and assurance requirements included in this ST. Specifically, AVA_VLA.1 requires that the TOE be resistant obvious vulnerabilities, this is consistent with SOF-basic, which is the lowest strength of function metric. Authentication by a password, specifically regarding FIA_UAU.2 is realized by a probabilistic or permutational mechanism. The methods used to provide difficult-to-guess passwords are probabilistic. The SOF claim for this IT security function is SOF-basic. The Strength of Function claim is SOF-basic based on the overall TOE. Strength of Function has been documented in the Crypto-Client FIPS 140-2 Security Policy as follows:

Authentication Mechanism	Strength of Mechanism
Userid and password	Minimum 6 characters => $72^6 = 1.39E11$
Static Key (TDES or AES)	TDES (192-bits) or AES (128, 192, or 256-bits)
CA signature	128-bit
AES CCM Passphrase	Minimum 8 characters => $72^8 = 7.22E14$
EAP-TLS	CA signature => 128-bit

A SOF-Basic analysis is provided as follows:

Pass-word length	Combination of characters using Alpha+numeric+special characters = 94	Attempts to crack per sec	Attempt to crack retry rate	Seconds to Crack	Days to Crack	Years to Crack
6	$94^6 = 689,869,781,056$	500	2 ms	1,379,739,562	15,969	43.8
6	689,869,781,056	1,000	1 ms	689,869,781	7,984	21.8
6	689,869,781,056	5,000	200 us	137,973,956	1,597	4.3
6	689,869,781,056	10,000	10 us	68,986,978	798	2.2

7.10 Protection Profile Claims Rationale

There is no claimed PP conformance for this ST.