3e Technologies International
3e-525A-3 Access System

Security Target

22000201-701

Revision S

August, 2006

3eTI Enterprise International 3e-525A-3 Access System Security Target, Revision S.

Document ID Number: 22000201-701 Revision S.
Total Page Count: 52

Contact: 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

1. Table of Contents

2. List of Tables and Figures

3. 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.

3.1 Security Target, TOE, and CC Identification

ST Title:	3eTI 3e-525A-3 Access System Security Target
ST Version:	22000201-701 Version S
ST Author:	Ryon Coleman
ST Publication Date:	August, 2006
TOE Identification:	**3eTI 3e-525A-3 Access System**. The TOE contains: 3e-525A-3 Hardware Version 1.0, Software Version 4.0.9.11. 3e-030-2 Software Version 3.0.7
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.

3.2 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)

3.3 TOE Summary

The Target of Evaluation (TOE) is a wireless LAN access system. The 3e-525A-3 Access System is a ruggedized access point intended for use in industrial and external environments. The TOE provides a secure, yet flexible, WLAN environment through the use of FIPS-validated components and support for industry standards.

3.4 Conventions, Terminology, Acronyms

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

3.4.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – The TOE Security Functional Requirements in sections 7.1 of the ST are derived from the CC Part 2 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). An asterisk "*" refers to all iterations of a component.
  - **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.
- Application notes provide additional information for the reader, but do not specify requirements. Application notes are denoted by *Application Note: italicized text.*
- Security Functional Requirements including the "-NIAP-xxxx" (where x is, for example, an integer) extension are considered to be explicitly stated.

3.4.2 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 resource use and data disclosure/modification.
- ***Access System*** --Equipment providing the interface between mobile clients and a wired network.
- ***Accountability*** -- Property allowing an IT system activity 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.
- ***Audit Server*** -- A central location where audit events/records are stored.
- ***Authentication*** -- Security measure that verifies a claimed identity.
- ***Authentication credentials*** -- Information used to verify a claimed identity.
- ***Authentication Server*** -- A central location where the users and administrators authentication credentials are stored.
- ***Authorization*** -- Permission, granted by an entity authorized to do so, to perform functions and access data.
- ***Authorized administrator(s)*** – This term is used to collectively describe users with the Administrator role and the Crypto-Officer.
- ***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) a cryptographic module that is FIPS 140-2 validated (to comply with FCS_BCM_EXP); (b) the cryptographic functionality implemented in that module are FIPS-approved security functions that have been validated; and (c) 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 a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.
- ***Embedded Cryptographic Module*** -- A Cryptographic Module that is built as an integral part of a larger and more general surrounding system (i.e., one that is not easily removable from the surrounding system).
- ***Enclave*** -- A collection of entities under the control of a single authority and having a homogeneous security policy. They may be logical, or may be based on physical location and proximity.
- ***Entity*** -- A subject, object, user, or another IT device, which interacts with TOE objects, data, or resources.
- ***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; and (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; and/or (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.

3.4.3 Acronyms

The acronyms used within this Security Target:

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

3.4.4 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 2 Validation "3e-525A-3 Access Point"
- 3eTI FIPS 140-2 Non-Proprietary Security Policy Level 1 Validation "3e-030-2 Security Server"

3.4.5 Security Target Overview and Organization

The Security Target contains the following additional sections:

- **TOE Description (Section 4)**: Provides an overview of the TOE security functions and boundary.
- **Security Environment (Section 5)**: Describes the threats, organizational security policies and assumptions that pertain to the TOE.
- **Security Objectives (Section 6)**: Identifies the security objectives that are satisfied by the TOE and the TOE environment.
- **IT Security Requirements (Section 7)**: Presents the security functional and assurance requirements met by the TOE.
- **TOE Summary Specification (Section 8)**: Describes the security functions provided by the TOE to satisfy the security functional requirements and objectives.
- **Rationale (Section 9)**: Presents the rationale for the security objectives, requirements, and TOE summary specifications as to their consistency, completeness and suitability.

4. TOE Description

The Target of Evaluation (TOE) is a wireless LAN access system. The 3e-525A-3 Access System is a ruggedized access point intended for use in industrial and external environments. The TOE provides a secure, yet flexible, WLAN environment comprised of two components: (a) the 3e-525A-3 Wireless Access Point (3e-WAP), and (b) the 3e-030-2 Security Server. (3e-SS). Figure 1 shows the concept of the TOE platform with Wireless Access Point and Security Server components.

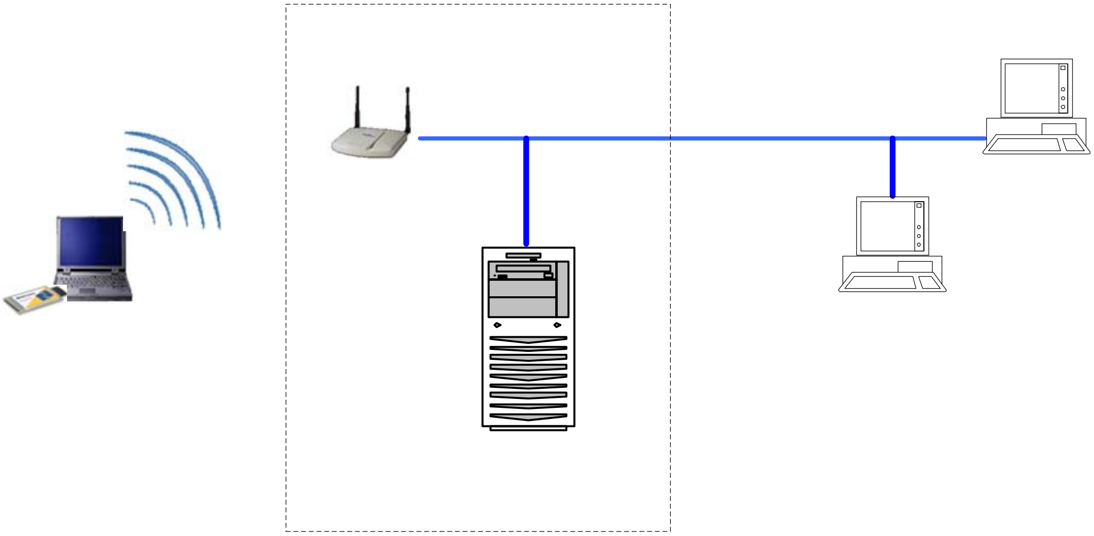

Figure 1 - TOE Platform

The 3e-WAP accommodates 802.11a/b/g WLAN access and uses Power over Ethernet (PoE) access to the Ethernet WAN to eliminate the need for internal access point power supply units (AC-DC converters) and 110-220V cabling installations. The wireless LANs can include any mobile devices such as handheld Personal Data Assistants (PDAs), mobile web pads, and wireless laptops which support the 802.11a/b/g standards for wireless networking.

The 3e-SS is a RADIUS-based server which provides EAP-TLS authentication of the clients connecting to the WLAN, ensuring only authorized connections are allowed. The Server is installed within the environment and connected to the 3e-WAP through the uplink port, allowing it to provide the authentication services for the mobile clients.

4.1 Product Description

The access system is a fully functional WLAN platform with augmented security functionality. While the system can provide standard 802.11a/b/g wireless access, the system can provide enhanced protection through a variety of cryptographic features, providing a high level of security for wireless environments. The 3e-WAP contains FIPS 140-2 Validated Level 2 secure encryption modules, with EAP-TLS provided by the 3e-SS software using the DKE Key exchange method when used in conjunction with 3e-010F clients. The 3e-WAP also includes 802.11i support.

Wireless Client

4.1.1 3e-525A-3 Wireless Access Point Description

The figure below shows the 3e-WAP part of the access system.

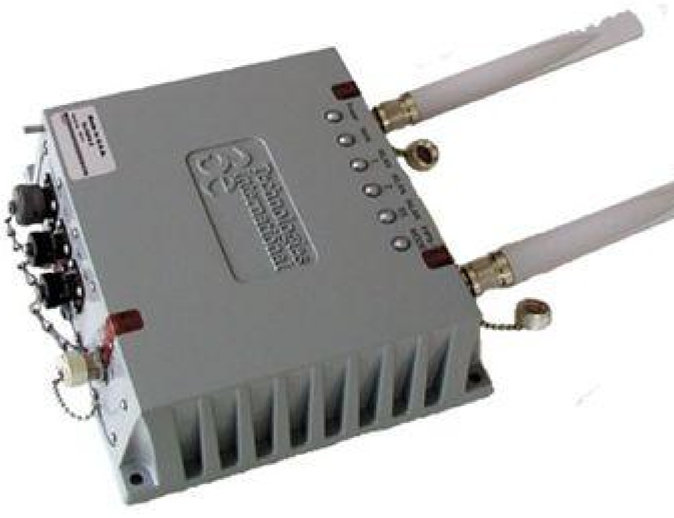

Figure 2 - 3e-525A-3 Wireless Access Point

For encryption on the WLAN, several different encryption mechanisms 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, or Dynamic Key Exchange. To support this mode, the wireless devices are required to have the 3e-010F Crypto-Client software installed. If you are using the access system in non-FIPS 140-2 mode, you can select None, Static 3DES, Static AES, Static WEP, or WPA. WPA uses TKIP or AES-CCMP so that legacy client WEP cards can be employed to secure the wireless band.

The access system incorporates Power over Ethernet (PoE). The PoE interface on the 3e-WAP is compatible with commercial vendor “injected power” hub units. The 3e-WAP includes AES/3DES cryptographic modules for wireless encryption and HTTPS/TLS, for secure web communication. In addition, it contains the capability to use the traditional WEP algorithm, either as static WEP or managed under WPA. The access system has an Ethernet WAN interface for communication to the wired LAN backbone, Ethernet LAN local port for purposes of initial setup and configuration, and two wireless AP antennas for communicating on the 802.11a/b/g frequencies.

The 3e-WAP shall use the MontaVista Linux operating system. It supports the file system, networking TCP/IP stack, memory device, block device, firewall system, and console driver that enables the 3e-WAP primary functionality. IPtable is a service provided by the Linux kernel. It is used to do Network Address Translation (NAT) in Gateway mode. It is also used to perform network activity logging and other network related operations. The Linux kernel in the 3e-WAP provides the core service of the unit by bridging different network interfaces together.

Within the 3e-WAP, support for IPv6 is available in AP Mode. Packet processing that is done in these modes is layer 2, so IP version (which is a layer 3 concern) is irrelevant in the normal data path. No changes are necessary in the data processing path. IPv4 and IPv6 wireless clients can transparently send data through the AP without any special configuration. However, IPv6 support is required to manage the AP. The 3e-WAP supports static IPv6 addresses on the WAN and LAN ports so that an IPv6 client can configure it. The AP does not support the following features in IPv6 mode:

- DHCP server on the LAN port.
- DHCP client on the WAN port.
- Dynamic Key Exchange (DKE) server.
- 802.11i
- SNMP

A user selectable option shall be provided to enable IPv6 support. When IPv6 is enabled, the IPv4 stack and IPv6 stack are running simultaneous (commonly known as a “dual stack” approach).

The following services shall be provided by the application layer software on the 3e-WAP:

- DHCP server serving the LAN side.
- Web server serving as a management interface to the device (should only allow HTTPS connection).
- Printer server providing printing services on the USB printer
- Dynamic Key Exchange serving the authentication and key distribution of all wireless clients.
- Network Activity Logging to log every network activity of the unit (filters need to be applied so that the limited disk space will not be filled out in a very short period of time).
- SNMP agent serving as another management interface to the device (the service provided via this interface shall be a small subset of overall system management options). Different version of SNMP, including V1, V2, V3 and AES encryption)

Basic Functions

- Ethernet uplink WAN port
- Local Ethernet LAN port (for configuration only)
- USB port
- Wireless (802.11a/b/g) AP with operating range of 2000+ feet
- Power over Ethernet (PoE)
- Above average temperature range for extreme environments (with TEC option)
- AES, 3DES, WEP encryption or WPA with TKIP, depending on setup
- HTTPS/TLS secure Web
- DHCP client
- Bandwidth control
- Adjustable Radio Power
- MAC address filtering
- Load Balancing
- Rogue AP Detection

The following security modules have been implemented in the 3e-525A-3 Access System:

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

4.1.2 3e-030-2 Security Server Description

The 3e-030-2 Security Server (3e-SS) is comprised of three major subcomponents. They are the security server service, the security server manager, and the key/certificate file format converter.

The 3e-SS is installed on a Microsoft Windows 2000 Server or Windows 2003 Server system provided within the environment (the Windows server is not part of the TOE). The 3e-SS creates, distributes and manages “dynamic” per session keys for each user, each time they log into the network. It also authenticates each user (the 3e-010F Crypto-Client) by distributing and managing digital certificates.

The 3e-030-2 Security Server provides and enforces the following services:

- The EAP-TLS authentication from 3e-SS through the 3e-WAP to the 3e-010F Crypto Client
- Process dynamic key exchange after a successful authentication
- Deny users that are on the CRL (Certificate Revocation List)
- Audit/Log every attempt to authenticate and the results of authentication.
- Audit/Log service starting and stopping
- Audit/Log key zeroization, error detected during cryptographic key transfer
- Audit/Log cryptographic operation (i.e. key changing event) and certificate operation (i.e. changing authentication credentials, revocation validation, etc.)
- Audit/Log all modifications to the audit configuration that occur while the audit collection functions are operating
- Audit/log unsuccessful binding of user security attributes to a subject

- Audit/log changing encryption mode

The security server manager handles the interaction between user input and security server service via a GUI. These include:

- A signed certificate for the server and the corresponding private key file, and private key password
- The root certificate and the signed server certificate
- A shared secret between the 3e-SS and the 3e-WAP
- Certificate Revocation List (CRL) file
- Service port number

The key/certificate file format converter utility will convert the certificate generated from the Microsoft certificate server to standard X.509 format certificate for the root, server, and user's certificates.

4.2 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.

4.2.1 Physical Boundaries

The 3e-WAP is a ruggedized wireless access point that meets both military and enterprise environment requirements, and the entire box is included within the TOE. The hardware main board consists of an Intel Xscale IXP 425 processor, which processes encrypted and unencrypted traffic on both the wireless and wired networks to which the 3e-WAP interfaces. The processor runs at 533 MHz. There are 8M bytes of flash memory, and 64M bytes of RAM. Both external ports and internal ports are available on the hardware main board. External ports include one 10/100 Mbps WAN Ethernet port, one 10/100 Mbps LAN Ethernet port, one external USB host port, and a reset button. Internal ports include two mini-PCI interfaces for wireless adapters and one each of the following: JTAG interface, MII bus, I2C port, UART port, and 16-bit expansion port for expansion. There are LED indicators on the box. They are for AC power, WAN activities, PCI 1 active, PCI 2 active, and FIPS mode indicator.

The 3e-WAP supports multiple RFs (802.11a/b/g) and the following additional functionality: AES/3DES encryption, Unicast/Broadcast key setting, 802.1x packet awareness, standard WDS (Wireless Data Service), sniffing, i.e., receiving all the wireless packets in the same channel in the air and "passing" them up the network stack (i.e. encapsulating the packets) to the application layer OS and WPA and WPA2 (Wi-Fi Protected Access). The 3e-WAP includes a USB master controller which provides connectivity to external equipment such as a USB printer. Two types of Ethernet ports are provided by the 3e-WAP: one for WAN connection, and the other for protected LAN connection.

The 3e-SS is a software package which is installed on a Windows 2000 Server or Windows 2003 Server system. The operating system and computer on which the 3e-SS is installed are not included in the TOE, only the provided 3e-SS software. The physical boundary for the 3e-SS component of the TOE then is the environment needed for effective operation of the component itself. This would include a server with the installed operating system and a network connection to the 3e-WAP.

4.2.2 Logical Boundaries

The TOE Security Functions are Audit, Encryption, Identification and Authentication, Management, Information Flow Control and Protection of the TSF.

4.2.2.1 Audit

The access system generates auditable events for actions on the 3e-WAP and the 3e-SS. These events can be viewed within the 3e-WAP Management Interface or they can be exported to audit systems within the IT environment. The 3e-WAP and the 3e-SS each generate separate records for their own actions, though each contain information about the user/process associated with the event, result of the event and when the event occurred.

4.2.2.2 Encryption

This access system 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 access system use these evaluated modules/algorithms to ensure the security of all data passed through the 3e-WAP.

4.2.2.3 Identification and Authentication

The access system requires that administrators be properly identified and authenticated prior to performing any administrative tasks on the system. Furthermore, multiple authentication mechanisms are provided for access to wireless services provided by the access system. The type of authentication mechanism invoked depends on the origin of the source (i.e., remote user from the wireless environment, remote administrative user or Crypto-Officer from the wired environment, or administrative user or Crypto-Officer from a local console) requesting the service. The authentication of a user or client computer will be based on a set of authentication credentials assigned to each user or client computer.

4.2.2.4 Management

The access system provides a web-based interface to manage the configuration of the access point and an application interface to manage the cryptographic credentials stored in the Security Server. The management includes all security settings of the access point, controlling the types of communications which will be allowed to connect via the WLAN as well as the clients which will be allowed to connect.

4.2.2.5 Information Flow Control

The access system enforces information flow by requiring the establishment of an encrypted communications channel between components of the system. The access system may further restrict potential information flows by granting or denying access to the network based upon authentication by a remote server. The 3e-WAP and 3e-SS require a secure communication channel.

4.2.2.6 Protection of the TSF

The access system protects the TSF by ensuring that no access is granted to TOE functions without authorization. Internal testing of the TOE hardware and software ensures that all security functions are running and available before the access system will accept any communications.

4.3 Security Server File List

3e-030-2 Security Server

<u>Installed Files on Windows 2000 Server or Windows 2003 Server:</u>

01 aesmain.exe
02 ca.js
03 cam.css
04 cam.hta
05 cam.ico
06 cam.js
07 crl.hta
08 crl.js
09 cv2k.exe
10 DoDAlarm.exe
11 DoDServer.exe
12 ldapfetch.exe
13 lib.js
14 libeay32.dll
15 log.hta
16 log.js
17 openssl.exe
18 openssl.js
19 page.js
20 PkiCom.dll
21 service.js
22 setup.js
23 ssleay32.dll
24 SSLogFile.exe
25 svc-setup.exe
26 uninstall-DoDPKI.exe
27 images/cam.ico
28 images/cam.jpg
29 images/cclog.ico
30 images/certificate.gif
31 images/certificate.ICO
32 images/certificate.png
33 images/checkmark.gif
34 images/close-3.gif
35 images/contact.gif
36 images/crl.gif
37 images/CRL.ico
38 images/CRL.png
39 images/crlcam.ico
40 images/down.gif
41 images/ldap.gif
42 images/ldap.jpg
43 images/lock.gif
44 images/minus.gif
45 images/plus.gif
46 images/up.gif

5. 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 TOE security environment defines (a) threats that the product is designed to counter; (b) assumptions made on the operational environment and the method of use intended for the product, and (c) organizational security policies with which the product is designed to comply.

5.1 Secure Usage Assumptions

This section describes operating environment aspects 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	Authorized Administrators, including Crypto-Officers, are non-hostile, appropriately trained, and shall follow and abide by the instructions provided by TOE guidance documentation.
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, in addition to the physical security provided by the enclosure of the TOE itself. The physical environment shall provide reliable power and air conditioning controls to insure reliable operation of the hardware.
A.HARDWARE	The software portion of TOE (3e-SS) shall be installed in a hardware system that is running Windows 2000 Server or Windows 2003 Server with a network interface card installed.

5.2 Threats to Security

The threats listed in Table 2: Threats are general threats. Threats are actions that may have an adverse affect on the Basic Robustness WLAN or mission. Exposure of wireless communications in the RF transmission environment introduces unique threats for the WLAN. The WLAN interconnected to a wired network could effectively create a hole in the wired infrastructure boundary because it exposes information to the RF medium where signals can be more readily detected and intercepted. With WLANs, an adversary no longer requires physical access to the network to exploit a wireless system. For basic robustness, the threats identified do not include those that would be considered a sophisticated attack (e.g., intentional jamming, traffic analysis). This is not to say that the 3eTI WLAN access system is not designed to withstand such attacks.

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.

In fact, the relationship between expertise and resources is somewhat more complicated. In general, if resources include factors other than just raw processing power (money, for example), then expertise should be considered to be at the same “level” (low, medium, high, for example) as the resources because money can be used to purchase expertise. Expertise in some ways is different, because expertise in and of itself does not automatically procure resources. However, it may be plausible that someone with high expertise can procure the requisite amount of resources by virtue of that expertise (for example, hacking into a bank to obtain money in order to obtain other resources).

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

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

The important general points we can make are:

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

Table 2 - Threats

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.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.POOR_DESIGN	Unintentional errors in requirements specification or TOE design 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).
T.UNATTENDED_ SESSION	A user may gain unauthorized access to an unattended session, thus gaining access to the resources protected by the TOE.
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, thus tampering with the TSF data.
T.UNAUTH_ADMIN_ACCESS	An unauthorized user or process may gain access to an administrative account, thus allowing tampering of the TSF data.
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 where TSF data has been modified.

The following table lists the Basic Robustness threats not applicable to the TOE:

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.

5.3 Organization Security Policies

Following are the Organizational Security Policies enforced by the TOE:

Table 4 - Organizational Security Policies

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

5.4 *Security Function Policies*

Several 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.SPECIFIED USERS SFP	The access system administrators shall specifically identify the set of wireless clients that can connect to the network through the remote access server. The TSF shall filter traffic at the wireless interfaces based upon the user authentication credentials stored in the authentication server. The traffic across the wired side of the network is not directly restricted by the information flow control policy.
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.

6. Security Objectives

This section defines TOE security objectives and its supporting environment. Security objectives, categorized as either IT 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.

6.1 Security Objectives for the TOE

Table 6 – TOE Security Objectives

Name	TOE Security Objective
O.ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure management.
O.AUDIT_GENERATION	The TOE provides the capability to detect and create records of security relevant events.
O.AUDIT_REVIEW	The TOE provides the capability to selectively view audit information.
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. This is accomplished through operational self-tests, which are FIPS 140-2 approved.
O.CRYPTOGRAPHY	The TOE uses NIST FIPS 140-2 validated cryptographic services.
O.DISPLAY_BANNER	The TOE will display an advisory warning prior to establishing an administrator session regarding use of the TOE prior to permitting the use of any TOE services that requires authentication.
O.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 Authorized Administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.MEDIATE	The TOE mediates the flow of information to and from wireless clients communicating via the TOE in accordance with its security policy.
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. This is proven by Audit Logging destruction of a cryptographic key.
O.SELF_PROTECTION	The TSF maintains a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.
O.VULNERABILITY_ ANALYSIS	The TOE has undergone vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.

6.2 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 will provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.

6.3 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.HARDWARE	The software portion of TOE shall be installed in a hardware system that is running Windows 2000 Server or Windows 2003 Server with a network interface card installed.
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 shall provide physical security commensurate with the value of the TOE and the data it contains.

7. IT Security Requirements

7.1 TOE Security Functional Requirements

This section specifies the TOE Security Functional Requirements (SFRs). This section organizes the SFRs by CC class. The TOE SFRs in sections 7.1 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. The following table 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
	FAU_GEN.2-NIAP-0410 - User identity association
	FAU_SAR.1 Audit review
	FAU_SAR.2 Restricted audit review
	FAU_SAR.3 Selectable audit review
	FAU_SEL.1-NIAP-0407 - Selective audit
Cryptographic Support (FCS)	FCS_BCM_EXP.1 - Baseline Cryptographic Module
	FCS_CKM.1 - Cryptographic key generation
	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 (1) - Subset information flow control (Specified Users Policy)
	FDP_IFC.1 (2) - Subset information flow control (Wireless Encryption Policy)
	FDP_IFF.1-NIAP-0407 (1) - Simple security attributes (Specified Users SFP)
	FDP_IFF.1-NIAP-0407 (2) - Simple security attributes (Wireless Encryption SFP)
	FDP_ITT.1 Basic internal transfer protection
	FDP_RIP.1 (1) - Subset residual information protection
Identification and Authentication (FIA)	FIA_AFL.1-NIAP-0425 - Administrator Authentication failure handling
	FIA_ATD.1 - User attribute definition
	FIA_UAU.1 - Timing of authentication
	FIA_UID.1 - Timing of identification
	FIA_USB.1-NIAP-0415 - User-subject binding
Security Management (FMT)	FMT_MOF.1 (1) - Management of security functions behavior (Cryptographic Function)
	FMT_MOF.1 (2) - Management of security functions behavior (Audit Record Generation)
	FMT_MSA.1 - Management of security attributes
	FMT_MSA.2 - Secure security attributes
	FMT_MSA.3-NIAP-0409 - Static attribute initialization
	FMT_MTD.1 (1) - Management of TSF Data
	FMT_MTD.1 (2) - Management of TSF Data
	FMT_MTD.1 (3) - Management of TSF Data
	FMT_REV.1 - Revocation
	FMT_SMF.1 (1) - Specification of Management Functions (Cryptographic Function)
	FMT_SMF.1 (2) - Specification of Management Functions (TOE Audit Record Generation)
	FMT_SMF.1 (3) - Specification of Management Functions (Authorized WLAN User List)
	FMT_SMF.1 (4) - Specification of Management Functions (Cryptographic Key Data)
	FMT_SMR.1 (1) - Security roles
Protection of TSF (FPT)	FPT_RVM.1 - Non-bypassability of the TSP
	FPT_SEP.1 - TSF domain separation
	FPT_TST_EXP.1 - TSF testing
	FPT_TST_EXP.2 - TSF testing of Cryptographic Modules
TOE Access (FTA)	FTA_SSL.3 - TSF-initiated termination
	FTA_TAB.1 - Default TOE access banners

7.1.1 Security Audit (FAU) Requirements

7.1.1.1 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 events for the *minimum* level of audit; and (c) [all auditable events as shown in the following table];

Table 10 - Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents	Enumeration
FAU_SEL.1-NIAP-0407	All modifications to the audit configuration that occur while the audit collection functions are operating	The identity of the Administrator/Crypto-Officer performing the function	1
FCS_CKM.4	Destruction of a cryptographic key	If available - the authentication credentials of subjects that share the destroyed key.	2
FDP_IFF.1-NIAP-0407 *	Decisions to permit requested information flows	None	3
FIA_AFL.1-NIAP-0425	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g., disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal	This event is logged in the System Log only.	4
FIA_UAU.1	Unsuccessful use of the authentication mechanism	None	5
FIA_UID.1	Unsuccessful use of the user identification mechanism, including the user identity provided	None	6
FIA_USB.1-NIAP-0415	Unsuccessful binding of user security attributes to a subject Maps to same auditable events as FDP_IFF.1-NIAP-0407	None	7
FMT_MOF.1(2)	Start or Stop of audit record generation	None	8
FMT_MSA.1	Changing the list of WLAN Devices authorized to communicate with the TOE	User Authentication Credentials added or deleted	9
FMT_MSA.3	Changing the default behavior of the Specified Client Policy	None	10
FMT_MTD.1(2)	Changes to the cryptographic key data	None – the TOE SHALL NOT record cryptographic keys in the audit log.	12
FMT_SMR.1(1)	Modifications to the group of users that are part of a role	This event is logged in the System Log only.	13
FPT_TST_EXP.1	Execution of the self test	Refer to System Log for Pass/Fail status	15
FPT_TST_EXP.2	Execution of the self test	Refer to System Log for Pass/Fail status	16
FTA_SSL.3	TSF Initiated Termination Management Console initiated termination is logged in the 3e-SS User inactivity causing Termination is logged in the 3e-WAP	This event is logged in the System Log only.	17

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].

7.1.1.2 FAU_GEN.2-NIAP-0410 - User Identity Association

FAU_GEN.2.1-NIAP-0410 **For audit events resulting from actions of identified users**, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

7.1.1.3 FAU_SAR.1 – Audit Review

FAU_SAR.1.1 The TSF shall provide [authorized administrators] with the capability to read [list of auditable events provided in FAU_GEN.1.1-NIAP-0410] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

7.1.1.4 FAU_SAR.2 – Restricted Audit Review

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

7.1.1.5 FAU_SAR.3 – Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to perform *sorts* of audit data based on [log events which contain unique serial numbers, valid date and time, event type, MAC address of client, IP address of access point].

7.1.1.6 FAU_SEL.1-NIAP-0407 - Selective Audit

FAU_SEL.1.1-NIAP-0407 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) *event type*
b) *[no additional attributes].*

7.1.2 Cryptographic Support (FCS) Requirements

7.1.2.1 FCS_BCM_EXP.1.1 - Baseline Cryptographic Module

FCS_BCM_EXP.1.1 All cryptomodules shall be FIPS PUB 140-2 validated, and shall 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.

7.1.2.2 FCS_CKM.1 - Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA, AES and 3DES] and specified cryptographic key sizes [128, 192 and 256 bits for AES and 192 bits for 3DES] that meet the following: [FIPS 186-2 for RSA, FIPS 197 for AES and FIPS 46-3 for 3DES].

7.1.2.3 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 as input and be able to output keys in the following circumstances [Diffie-Hellman algorithms, or AES key wrap algorithms] 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.

7.1.2.4 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 Level 1;
b) zeroization of some private cryptographic keys, plaintext cryptographic keys, key data, and all other critical cryptographic security parameters shall be immediate and complete; and
c) zeroization mechanism: Key Zeroization in the 3e-WAP and in the 3e-SS is performed by writing an all zero pattern "00000…" into the Key Data Field being zeroized at least one time.]

7.1.2.5 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.

7.1.2.6 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.

7.1.3 User Data Protection (FDP) Requirements

7.1.3.1 FDP_IFC.1 (1) - Subset Information Flow Control (Specified Users SFP)

FDP_IFC.1.1 (1) The TSF shall enforce the [Specified Users SFP] on [subjects: access system; information: network packets; operations: receive packet and transmit packet].

7.1.3.2 FDP_IFC.1 (2) - Subset Information Flow Control (Wireless Encryption SFP)

FDP_IFC.1.1 (2) The TSF shall enforce the [Wireless Encryption SFP] on: [subject: wireless access system; information: network packets and encryption/decryption flag; and operations: encrypt network packets, decrypt network packets].

7.1.3.3 FDP_IFF.1-NIAP-0407 (1) - Simple Security Attributes (Specified Users SFP)

FDP_IFF.1.1-NIAP-0407 (1) The TSF shall enforce the [Specified Users SFP] based on the following types of subject and information security attributes: [authentication credentials].

FDP_IFF.1.2-NIAP-0407 (1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

a) the subject is an access system, the operation is transmit packet, and the authentication credentials of the user is allowed based upon the authentication credentials specified in the authentication server;

b) the subject is an access system, the operation is receive packet, and the authentication credentials of the user are allowed based upon the authentication credentials specified in the authentication server;

c) [no additional information flow Specified Users SFP Rules].

FDP_IFF.1.3-NIAP-0407 (1) The TSF shall enforce the following information flow control rules: [no additional information flow control SFP rules].

FDP_IFF.1.4-NIAP-0407 (1) The TSF shall provide the following [no additional SFP capabilities].

FDP_IFF.1.5-NIAP-0407 (1) The TSF shall explicitly authorize an information flow based on the following rules: [no explicit authorization rules].

FDP_IFF.1.6-NIAP-0407 (1) The TSF shall explicitly deny an information flow based on the following rules: [no explicit denial rules].

7.1.3.4 FDP_IFF.1-NIAP-0407 (2) - Simple Security Attributes (Wireless Encryption SFP)

FDP_IFF.1.1-NIAP-0407 (2) The TSF shall enforce the [Wireless Encryption SFP] based on the following types of subject and information security attributes: [encryption/decryption flag; subject type].

FDP_IFF.1.2-NIAP-0407 (2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

a) if the encryption/decryption flag does NOT indicate that the TOE should perform encryption then all packets may pass without modification;

b) if the subject type is wireless access system, the operation is transmit the network packet, and the encryption/decryption flag indicates the TOE should perform encryption, then the TOE must encrypt user data via FCS_COP_EXP.2.1 to permit the information flow;

c) if the subject type is wireless access system, the operation is pass the network packet, and the encryption/decryption flag indicates the TOE should perform decryption then the TOE must decrypt user data via FCS_COP_EXP.2.1 to permit the information flow;

d) [no additional information flow Wireless Encryption SFP Rules].

FDP_IFF.1.3-NIAP-0407 (2) The TSF shall enforce the following information flow control rules: [ST AUTHOR - selection: [no additional information flow control SFP rules].

FDP_IFF.1.4-NIAP-0407 (2) The TSF shall provide the following [no additional SFP capabilities].

FDP_IFF.1.5-NIAP-0407 (2) The TSF shall explicitly authorize an information flow based on the following rules: [no explicit authorization rules].

FDP_IFF.1.6-NIAP-0407 (2) The TSF shall explicitly deny an information flow based on the following rules: [no explicit denial rules].

7.1.3.5 FDP_ITT.1 – Basic Internal Transfer Protection

FDP_ITT.1.1 The TSF shall enforce the [Wireless Encryption SFP and/or Specified Users SFP] to prevent the *disclosure, modification, loss of use of user data* when it is transmitted between physically-separated parts of the TOE.

Application Note: *Wired connection between the 3e-SS and the 3e-WAP is trusted.*

7.1.3.6 FDP_RIP.1 (1) - Subset Residual Information Protection

FDP_RIP.1.1(1) The TSF shall ensure that any previous information content of a resource is made unavailable upon *the deallocation of the resource from* the following objects: [Critical Security Parameters (CSPs) listed in the following Tables].

Table 11 - List of Zeroizable Static Critical Security Parameters in 3e-WAP

Type	ID	Storage Location	Form	Zeroizable	Zeroization Mechanism	Function
Plaintext Keys						
PMK 256 bit	"pairwise master key"	RAM	Plaintext (inaccessible)	Y	By changing the mode to FIPS-11i or static key encryption	Master key used to derive PTK
GMK 256 bit	"group master key"	RAM	Plaintext (inaccessible)	Y	By changing the mode to FIPS-11i or static key encryption	Master key used to derive GTK
AES Dynamic Broadcast 128,192, or 256 bit	"dynamic broadcast AES key"	RAM	Plaintext (inaccessible)	Y	By changing the mode to FIPS-11i or static key encryption	Client Access

Type	ID	Storage Location	Form	Zeroizable	Zeroization Mechanism	Function
3DES Dynamic Broadcast 192 bit	“dynamic broadcast 3DES key”	RAM	Plaintext (inaccessible)	Y	By changing the mode to FIPS-11i or static key encryption	Client Access
AES Dynamic Unicast 128,192, or 256 bit	“dynamic unicast AES key”	RAM	Plaintext (inaccessible)	Y	By changing the mode to FIPS-11i or static key encryption	Client Access
3DES Dynamic Unicast 192 bit	“dynamic unicast 3DES key”	RAM	Plaintext (inaccessible)	Y	By changing the mode to FIPS-11i or static key encryption	Client Access
RNG Seed Key 160 bit	“RNG seed key”	RAM	Plaintext (inaccessible)	Y	Zeroized immediately following use (after function is called & returned)	To generate the RNG
AES post-authentication 128 bit	“post - authentication AES key”	RAM	Plaintext (inaccessible)	Y	Zeroized after the unicast key (encrypted by this AES key) is decrypted by the module	N/A
AES-CCM Dynamic Broadcast 128 bit (GTK)	“dynamic broadcast AES-CCM key use for FIPS-11i”	RAM	Plaintext (inaccessible)	Y	By changing encryption mode to DKE or static key encryption	Client Access
KCK 128 bit	“key MIC key”	RAM	Plaintext (inaccessible)	Y	By changing encryption mode to DKE or static key encryption	To generate MIC in 802.11i key message
KEK 128 bit	“key encryption key”	RAM	Plaintext (inaccessible)	Y	By changing encryption mode to DKE or static key encryption	To encrypt GTK in 802.11i key message
AES-CCM Dynamic Unicast 128 bit (TK)	“dynamic unicast AES-CCM key use for FIPS-11i”	RAM	Plaintext (inaccessible)	Y	By changing encryption mode to DKE or static key encryption	Client Access
802.11i pre-shared passphrase 8 to 63 chars	“802.11i pre-shared passphrase”	RAM	Plaintext (inaccessible)	Y	By changing the mode to FIPS-11i or static key encryption	Used to generate PMK
RSA Private Key	“HTTPS/TLS RSA private key”	FLASH	Plaintext (inaccessible)	Y	Setting the module to factory default	N/A
HMAC-SHA-1 key (1)	“firmware integrity check key for firmware load test”	FLASH	Plaintext (inaccessible, hard-coded)	Y	Zeroized by upgrading firmware	N/A
HMAC-SHA-1 key (3)	SNMP packet authentication key	FLASH	Plaintext	Y	Setting the module to factory default	N/A
TLS Session Key	“HTTPS/TLS session key”	RAM	Plaintext (inaccessible)	Y	When the module is powered down.	N/A
Diffie-Hellman Private Exponent, 1024-bit	“diffie-hellman prime”	RAM	Plaintext	Y	Zeroized after the unicast key (encrypted by the established AES key) is decrypted	N/A

Type	ID	Storage Location	Form	Zeroizable	Zeroization Mechanism	Function
					by the module	
Web-GUI logon password for the Crypto-Officer	“CO web-GUI logon password”	FLASH	Hashed using SHA-1	Y	Setting the module to factory default	CO logon credential.
Web-GUI logon password for the Administrator	“Admin web-GUI logon password”	FLASH	Hashed using SHA-1	Y	Setting the module to factory default	Admin logon credential.
Encrypted Keys: These keys are stored encrypted in the module and as such do not require zeroization.						
AES Static 128,192, or 256 bit	“static AES key”	FLASH	Encrypted AES using “system config AES key”	N/A	N/A	Client Access
AES Static 128,192, or 256 bit	“static AES key”	FLASH	Encrypted AES using “system config AES key”	N/A	N/A	Wireless Bridging
3DES Static 192 bit	“static 3DES key”	FLASH	Encrypted AES using “system config AES key”	N/A	N/A	Client Access
3DES Static 192 bit	“static 3DES key”	FLASH	Encrypted AES using “system config AES key”	N/A	N/A	Wireless Bridging
HMAC-SHA-1 key (2)	“backend HMAC key”	FLASH	Encrypted AES using “system config AES key”	N/A	N/A	N/A
802.11i TLS Key Encryption Key	“backed AES key”	FLASH	Encrypted AES using “system config AES key”	Y	Setting the module to factory default	To encrypt Transport TLS Session Key
Downloaded configuration file password	“downloaded config file pwd”	FLASH	Encrypted AES using “system config AES key”	N/A	N/A	To protect the configuration file

Table 12 - List of Zeroizable Static Critical Security Parameters in 3e-SS

Type	ID	Storage Location	Form	Zeroizable	Zeroization Mechanism	Function
Plaintext Keys						
HMAC-SHA-1 key 128 bit	“Software Integrity Check Key”	Hard Disk/ RAM	Plaintext (inaccessible, hard-coded)	N/A	N/A	Calculate system file HMAC; hashing Crypto-Officer password
AES Static 256 bit	“System Configuration AES Key”	Hard Disk/RAM	Plaintext (inaccessible, hard-coded)	N/A	N/A	Protect system configuration files
TLS Session Key	“TLS Session Key”	RAM	Plaintext (inaccessible)	Y	Zeroized immediately after the key is sent to AP	N/A
Diffie-Hellman Session Key	“DH Session Key”	RAM	Plaintext (inaccessible)	Y	Zeroized immediately after the key is used to encrypt TLS Session Key	To encrypt Transport TLS Session Key
Encrypted Keys: These keys are stored encrypted in the module and as such do not require zeroization.						

Type	ID	Storage Location	Form	Zeroizable	Zeroization Mechanism	Function
AES Key 128 bit	"AES Key Wrapper Key"	Hard Disk/ RAM	Encrypted AES using "System Configuration AES Key"	N/A	N/A	To encrypt Transport TLS Session Key
Other						
HMAC-SHA-1 secret(1)	"Key Wrapper EAP message authenticator secret"	Hard Disk/ RAM	Encrypted AES using "System Configuration AES Key"	N/A	N/A	Generate and verify EAP message MAC
HMAC-SHA-1 secret (2)	"DKE EAP message authenticator secret"	Hard Disk/ RAM	Encrypted AES using "System Configuration AES Key"	N/A	N/A	Generate and verify EAP message MAC
Crypto Officer Password	"Crypto Officer Password"	Hard Disk/ RAM	HMAC hashed using "Software Integrity Check Key"	N/A	N/A	CO password
RSA Certificate	"Server Certificate"	Hard Disk	Plaintext (inaccessible)	N/A	N/A	N/A
RSA Private Key	"Server Private Key"	Hard Disk	Plaintext (Encrypted 3DES CBC using password. Inaccessible.)	N/A	N/A	N/A

7.1.4 Identification and Authentication (FIA) Requirements

7.1.4.1 FIA_AFL.1-NIAP-0425 – Administrator Authentication Failure Handling

FIA_AFL.1.1-NIAP-0425 The TSF shall detect when **a fixed integer number (3) of** unsuccessful authentication attempts occur related to [remote administrators logging on to the WLAN access system].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the administrator from performing activities remotely that require authentication until an action is taken by a local Administrator].

7.1.4.2 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 data].

7.1.4.3 FIA_UAU.1 - Timing of Authentication

FIA_UAU.1.1 The TSF shall allow [the passing of authentication data to and from the authentication server] on behalf of the user to be performed before the user is authenticated.

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

7.1.4.4 FIA_UID.1 - Timing of Identification

FIA_UID.1.1 The TSF shall allow [the passing of authentication data to and from the authentication server] on behalf of the user to be performed before the user is identified.

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

7.1.4.5 FIA_USB.1-NIAP-0415 - User-Subject Binding

FIA_USB.1.1–NIAP-0415 The TSF shall associate the **following** user security attributes with subjects acting on behalf of that user: [authentication credentials and MAC address or username (as applicable)].

7.1.4.6 FIA_USB.1.2

The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].

7.1.4.7 FIA_USB.1.3

The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].

7.1.5 Security Management (FMT) Requirements

7.1.5.1 FMT_MOF.1 (1) - Management of Security Functions Behavior

FMT_MOF.1.1(1) The TSF shall restrict the ability to *modify the behavior* of the **cryptographic** functions [access system configuration] to [the Crypto-Officer and Administrators].

7.1.5.2 FMT_MOF.1 (2) - Management of Security Functions Behavior

FMT_MOF.1.1(2) The TSF shall restrict the ability to *enable, disable, determine, and modify the behavior* of the **audit record generation** functions [specify auditable events, specify event notifications] to [the Crypto- Officer].

7.1.5.3 FMT_MSA.1 - Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the [Specified Users SFP and Wireless Encryption SFP] to restrict the ability to *modify* the [value of the object security attributes] to [authorized administrators].

7.1.5.4 FMT_MSA.2 - Secure Security Attributes

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

Application Note: *A "password complexity" function is provided.*

7.1.5.5 FMT_MSA.3-NIAP-0409 - Static Attribute Initialization

FMT_MSA.3.1-NIAP-0409 The TSF shall enforce the [Specified Users SFP and Wireless Encryption SFP] to provide *restrictive* default values for the **information flow policy** attributes used to enforce the SFP.

FMT_MSA.3.2-NIAP-0409 The TSF shall allow the [the Crypto-Officer] to specify alternative initial values to override the default values when an object or information is created.

7.1.5.6 FMT_MTD.1 (1) - Management of TSF Data

FMT_MTD.1.1(1) The TSF shall restrict the ability to *modify, delete, clear,* [*and create*] the [security relevant TSF data except for audit records, user security attributes, and critical security parameters] to [authorized administrators].

7.1.5.7 FMT_MTD.1 (2) - Management of TSF Data

FMT_MTD.1.1(2) The TSF shall restrict the ability to [*initialize*] [the authentication data] to [Authorized Administrators].

7.1.5.8 FMT_MTD.1 (3) - Management of TSF Data

FMT_MTD.1.1(3) The TSF shall restrict the ability to *modify* [*and initialize*] [the critical security parameters] to [the Crypto-Officer and Administrators].

7.1.5.9 FMT_REV.1 - Revocation

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the *users* within the TSC to [the Crypto-Officer for administrators and users, and administrators for users].

FMT_REV.1.2 The TSF shall enforce the rules: [for validation of authentication credentials]. Rules are defined by FMT_MTD.1.1(2) and FMT_MTD.1.1(3).

7.1.5.10 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 (FCS_COP_EXP.1), or query and set no encryption/decryption of network packets].

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

FMT_SMF.1.1(2) The TSF shall be capable of performing the following security management functions: [enable or disable Security Audit (FAU_GEN.1-NIAP-0410)].

7.1.5.12 FMT_SMF.1 (3) - Specification of Management Functions (Authorized User List)

FMT_SMF.1.1(3) The TSF shall be capable of performing the following security management functions: [The TSF shall support the Specified Users SFP by providing the ability to modify, and delete entries in the database of authentication credentials in the authentication server with which the TOE may communicate].

7.1.5.13 FMT_SMF.1 (4) - Specification of Management Functions (Cryptographic Key Data)

FMT_SMF.1.1(4) 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].

7.1.5.14 FMT_SMR.1 (1) - Security Roles

FMT_SMR.1.1(1) The TSF shall maintain the roles: [Crypto-Officer, Administrator and user].

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

7.1.6 Protection of TSF (FPT) Requirements

7.1.6.1 FPT_RVM.1 - Non-Bypassability of the TSP

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

7.1.6.2 FPT_SEP.1 - TSF Domain Separation

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

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

7.1.6.3 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 hardware and 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, *none*.

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.

7.1.6.4 FPT_TST_EXP.2 - TSF Testing of Cryptographic Modules

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

7.1.7 TOE Access (FTA) Requirements

7.1.7.1 FTA_SSL.3 - TSF-Initiated Termination

FTA_SSL.3.1 The TSF shall terminate an interactive **administrator** session after a [10 minute time period of user inactivity].

7.1.7.2 FTA_TAB.1 - Default TOE access banners

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

7.2 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 authorized IT entities including a certificate authority server, as well as the hardware on which the Security Server software (files listed in section 4.3) reside.

Table 13 - IT Environment Security Functional Requirements

Functional Class	Functional Components
Protection of TSF (FPT)	FPT_STM.1 - Reliable time stamps

7.2.1 Protection of TSF (FPT) Requirements

7.2.1.1 FPT_STM.1 - Reliable Time Stamps

FPT_STM.1.1 The **IT Environment** shall be able to provide reliable time stamps for its own use.

7.3 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 9.3 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), ACM_CAP.3 (Authorization Controls), 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 14.

Table 14- TOE Security Assurance Requirements

Assurance Class	Assurance Components
Configuration Management (ACM)	ACM_CAP.3 Authorization controls
	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 Security enforcing 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 Analysis 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

7.4 Strength of Function

The Strength of Function claim is SOF-Basic. The overall strength of function requirement is SOF-basic. The strength of function requirement applies to FIA_UAU.1. The SOF claim for FIA_UAU.1 is SOF-basic. The strength of the “secrets” mechanism is consistent with the objective of the TOE’s logical access O.TOE_ACCESS 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 FIPS 140-2 Security Policy as follows:

Authentication Mechanism	Strength of Mechanism
Userid and password	Minimum 8 characters => 72^8 = 7.22E14
Static Key (TDES or AES)	TDES (192-bits) or AES (128, 192, or 256-bits)
HMAC SHA-1 shared secret	Minimum 10 characters => 72^10 = 3.74E18
CA signature	128-bit
AES CCM pre-shared key	Minimum 8 characters => 72^8 = 7.22E14
EAP-TLS	CA signature => 128-bit

8. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

8.1 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.

8.1.1 Audit

8.1.1.1 FAU_GEN.1-NIAP-0410

The TOE collects audit data based on the events described in Table 10. These events are considered to be security relevant, and therefore warrant recording their occurrence. The TOE generates records for two separate classes of events: authentication/access to the system, and actions taken directly on the system by network clients. 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). An “Auditing – Log” screen provides a listing of all audit records. Access to the Management interface can also be reviewed from the Web Access Log screen. Every start and stop of the audit service is noted in the audit record.

8.1.1.2 FAU_GEN.2-NIAP-0410

All actions performed by the TOE are associated with users or with the unique MAC address of a client. User associated events are those performed through the Management interface, such as changing the settings of the TOE. MAC address associated events are those that deal with traffic sent by clients of the TOE, such as successful shared secret authentication. Since all actions performed by the TOE are associated with a unique identifier, this information is maintained in the audit record, allowing the events stored there to be traced directly to the user or system for which they were performed.

8.1.1.3 FAU_SAR.1 & FAU_SAR.3

The TOE provides the ability to review audit records through the Management interface. This interface allows the review of all generated events, as well as the ability to perform queries for records for specific events. Queries can be done based on the Start or End time of the event, the MAC address or for a specific record. The records for the Management interface can be reviewed apart from the total record through the Web Access Log.

8.1.1.4 FAU_SAR.2

The TOE allows a user with Administrative or Crypto-Officer privileges to review audit records. This is assigned through the roles of these accounts. The audit records are not accessible through any other interface, and access to this interface requires the explicit creation of an administrator account (or knowledge of the Crypto-Officer account).

8.1.1.5 FAU_SEL.1-NIAP-0407

The TOE provides the Crypto-Officer with the ability to modify the types of events which will be audited. The Crypto-Officer can modify the events to be audited based on the following event properties: object identity, user identity, and event type.

8.1.2 Encryption

8.1.2.1 FCS_BCM_EXP.1

The 3e-WAP portion of the TOE has undergone FIPS 140-2 Level 2 validation and has been given certificate #640. The 3e-SS portion of the TOE has undergone FIPS 140-2 Level 1 validation and is in the NIST prevalidation queue. When the TOE is operated in FIPS-mode, all cryptographic operations performed by the TOE are FIPS-compliant, utilizing only FIPS-approved algorithms.

8.1.2.2 FCS_CKM.1

As part of the FIPS 140-2 Level 2 and Level 1 validation efforts, the AES and 3DES cryptographic algorithms for the TOE have also been evaluated. The AES algorithm has been evaluated against FIPS 197 and given certificate #415 and #238. The 3DES algorithm has been evaluated against FIPS 46-3 and given certificate #292. These validations assure the proper generation of cryptographic keys for use in the algorithm. The AES algorithm can use keys of 128, 192 and 256 bits in length. The 3DES algorithm can use keys of 192 bits in length.

8.1.2.3 FCS_CKM_EXP.2

The 3e-WAP portion of the TOE has undergone FIPS 140-2 Level 2 validation and has been given certificate #640. The 3e-SS portion of the TOE has undergone FIPS 140-2 Level 1 validation and is in the NIST prevalidation queue. This ensures that keys can only be manually input into the TOE for the following algorithms: Diffie-Hellman algorithms, or AES key wrap algorithms, for use as keys in the TOE.

8.1.2.4 FCS_CKM.4

The TOE performs Key Zeroization by writing an all zero pattern “00000…” into the Key Data Field being zeroized at least one time. This occurs immediately when the data is determined to no longer be needed. The fields which are zeroized can be found in Table 11 and Table 12. The 3e-WAP portion of the TOE has undergone FIPS 140-2 Level 2 validation and has been given certificate #640. The 3e-SS portion of the TOE has undergone FIPS 140-2 Level 1 validation and is in the NIST prevalidation queue.

8.1.2.5 FCS_COP_EXP.1

As part of the FIPS 140-2 Level 2 and Level 1 validation efforts, the random number generator has been evaluated to the FIPS 186-2 specification and has been given certificates #210 and #22.

8.1.2.6 FCS_COP_EXP.2

The 3e-WAP portion of the TOE has undergone FIPS 140-2 Level 2 validation and has been given certificate #640. The 3e-SS portion of the TOE has undergone FIPS 140-2 Level 1 validation and is in the NIST 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.

8.1.3 Information Flow Control

8.1.3.1 FDP_IFC.1 (1) & FDP_IFF.1-NIAP-0407(1)

The TOE protects access to network resources based on successful authentication/authorization to the TOE. Once the client system has successfully authenticated, the client will be able to send and receive wireless network packets across the TOE wireless LAN. 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).

8.1.3.2 FDP_IFC.1 (2) & FDP_IFF.1-NIAP-0407(2)

The TOE protects traffic on the WLAN through the use of FIPS-validated cryptographic functions. Based on the configuration specified by the administrator, the system can be set to use 3DES, AES or no encryption for the communications. All traffic sent across the WLAN must match the configured encryption algorithm to protect the transmitted data.

8.1.3.3 FDP_ITT.1

To ensure the non-disclosure and integrity of all data sent between separate components of the TOE, the components must first be authenticated to each other. This is done through the establishment of certificates on each component, which allow the separate components to establish identity, and hence authorization. After mutual authentication, all traffic between components is automatically encrypted and digitally signed by default with AES to ensure that internal data is not subject to loss or modification.

8.1.3.4 FDP_RIP.1

The TOE protects all critical data 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. Active keys (those in plaintext or otherwise in use and available) are always zeroized on a power cycle unless they are encrypted. Keys stored in an encrypted manner may be deleted, but since the key is not in the clear, negating the need to zeroize. Other keys are zeroized when the system is reset to factory default. This ensures that the data is not still available to other processes which may subsequently use the same resource. See Table 11 and Table 12 for a list of the critical data which is zeroized.

8.1.4 Identification and Authentication

8.1.4.1 FIA_AFL.1-NIAP-0425

The TOE authentication sequence to the Management interface includes a counter for unsuccessful attempts. When a user or administrator fails to enter the correct credentials after a specified number of attempts (the default is 3), the account will be locked. The account must then be unlocked by a Crypto-Officer (in the case of an administrator locking their account).

8.1.4.2 FIA_ATD.1

User accounts in the traditional sense have the following attributes: username, role, and authentication data. These accounts are then used to access the Management Interface. User accounts with respect to client computers accessing the WLAN resources of the TOE have only authentication credentials assigned. These credentials can take many forms, from a shared key (e.g., those used for WEP and WPA-PSK) to individually assigned certificates (used for EAP-TLS). The client must present the authentication credentials prior to gaining general access to the WLAN resources.

8.1.4.3 FIA_UAU.1 & FIA_UID.1

Due to the nature of a WLAN environment, certain data must be passed along the WLAN to allow the client system to be authenticated. Client authentication data is passed without, and prior, to a successful authorization to the network resources, and are used in determining whether authorization should be granted. Upon a successful authentication attempt, the client will be authorized to access the network, but if the authentication attempt is unsuccessful, no further traffic is allowed from the client (except for other authentication attempts).

The Strength of Function claim is SOF-Basic. Strength of Function has been documented in the FIPS 140-2 Security Policy as follows:

Authentication Mechanism	Strength of Mechanism
Userid and password	Minimum 8 characters => 72^8 = 7.22E14
Static Key (TDES or AES)	TDES (192-bits) or AES (128, 192, or 256-bits)
HMAC SHA-1 shared secret	Minimum 10 characters => 72^10 = 3.74E18
CA signature	128-bit
AES CCM pre-shared key	Minimum 8 characters => 72^8 = 7.22E14
EAP-TLS	CA signature => 128-bit

8.1.4.4 FIA_USB.1-NIAP-0415

All actions within the TOE are tied to the users/clients accessing the TOE resources through unique bindings. This allows each action or process to be uniquely identified with a specific user or client connected to the TOE. The primary mechanism of this binding is the authentication credentials of the client (or user), with a secondary binding (which would never conflict) via the MAC address or the username. For client access to TOE resources it would be authentication data and MAC address, while for Management interface access it would be username and password.

8.1.4.5 FTA_SSL.3

To ensure protection of the TOE configuration on systems where a session is accidentally left active, all administrative sessions to configure/access the TOE are subject to a 10 minute timeout period of user inactivity. A user is required to re-enter all authentication credentials upon return to a timed-out session.

8.1.4.6 FTA_TAB.1

When any user connects to the Management Interface, a proper-usage banner shall be presented, warning the user of unauthorized use of the resources.

8.1.5 Management

8.1.5.1 FMT_MOF.1 (1) & FMT_MOF.1 (2) & FMT_SMR.1

The TOE provides three roles: Crypto-Officer, Administrator, and user. The user role is the implicit role for anyone accessing the system as a client through the WLAN. The user role has no administrative ability on the TOE, only the ability to access the WLAN resources.

The Crypto-Officer and Administrator roles have many common management functions, with the Crypto-Officer role having extra privileges not available to the Administrator role. The following functions are unique to the Crypto-Officer:

- Initialization and management of security modules and cryptographic keys
- Audit configuration (what to audit, notifications)
- User management (creation, deletion, reset of users, timeout settings, lockout settings). “Creation” and “Deletion” refer to “creation and deletion of administrators and/or users”

All other management functions in the TOE can be performed by any authorized administrator as well as the Crypto-Officer.

8.1.5.2 FMT_MSA.1

The TOE restricts the ability to modify authentication credentials used to provide WLAN authorization to prevent unauthorized access to TOE resources. This access is restricted only to authorized administrators who are able to configure the users/clients which can access the TOE. The types of credentials which can be modified are pre-shared keys (such as those used in WEP or WPA-PSK) or certificates (for EAP-TLS). Users are not allowed to modify this data for network access.

8.1.5.3 FMT_MSA.2 & FMT_MSA.3-NIAP-0409

The TOE provides a default set of restrictive values which enable a high level of security upon initial configuration. The documentation provided by the TOE, along with proper training of the Crypto-Officer ensures that only secure values can be used. The TOE also provides visual confirmation of running in FIPS-mode, allowing the Crypto-Officer to instantly know whether these settings are enabled for the highest security. The Crypto-Officer is able to fully configure the security settings of the TOE, and therefore can override specific settings to tailor the configuration to fit any environment.

The default settings require an encrypted network and therefore means the Crypto-Officer must specifically add authorized users to the database prior to any access. The default access given to a new account is the user role, providing a restrictive environment.

8.1.5.4 FMT_MTD.1(1) & FMT_MTD.1(3)

The TOE provides two administrative roles with different levels of access to the system configuration of the TOE. The Crypto-Officer role has access to all configuration parameters within the TOE, including all critical security parameters such as the audit configuration, all cryptographic settings and administrative user management. The Crypto-Officer has the ability to initialize and modify the critical security parameters. The Administrator role does not have the ability to manage or review any of these specific settings, though all other functions available within the TOE are available to this role.

Any authorized administrator can create client user accounts with certificates for authentication, though only the Crypto-Officer can establish this mechanism for authentication. An authorized adminitstrator has the ability to modify, delete, clear, and create security relevant data.

8.1.5.5 FMT_MTD.1(2)

Any authenticated administrator can configure the client settings with respect to certificate (EAP-TLS)-based authentication. The authorized administrator is capable of initiating the certificate requests to the Certificate Authority which can then be loaded into the certificate database for client authentication.

8.1.5.6 FMT_REV.1

When users/clients must have their ability to access TOE resources revoked, the Crypto-Officer is able to remove the authentication credentials (certificates) from the account database, preventing any successful authentication by that user/client.

When administrator access must be revoked, the Crypto-Officer can delete the existing administrator account for that person, blocking future access to the Management interface.

Once revoked, the creation of a new user or administrator will not create the same identity, even with the use of the same information.

8.1.5.7 FMT_SMF.1(1) & FMT_SMF.1(4)

The TOE provides the Crypto-Officer with the ability to configure the cryptographic settings of the WLAN environment. This is done through the Management interface. The available cryptographic options for the WLAN include the selection whether to encrypt traffic, the encryption algorithm to use, and the type of authentication to the WLAN (EAP-TLS or pre-shared keys). The Crypto-Officer also has the ability to establish and initialize the keys to be used for the encryption of traffic across the WLAN. Key zeroization mechanisms are clearly defined in the FIPS 140-2 Vendor Evidence documentation.

8.1.5.8 FMT_SMF.1(2)

The TOE provides the Crypto-Officer with the ability to manage the audit settings of the TOE. The Crypto-Officer can specify the types of events to audit. The TOE allows only the Crypto-Officer to manage the audit settings. All access to the audit functions is through the Management interface.

8.1.5.9 FMT_SMF.1(3)

The TOE provides Authorized Administrators with the ability to manage the clients which are allowed to connect to the WLAN environment through the Security Server console. Through this console, the Authorized Administrator can request certificates from a specified Certificate Authority which can then be assigned to each client to connect to the WLAN. These certificates are then used as authentication credentials for client access to the network. The Security Server console provides full administration of these accounts, allowing the Authorized Administrators to create and delete the clients.

8.1.6 Protection of the TSF

8.1.6.1 FPT_RVM.1

The TOE prevents bypassing of the TSF by requiring that all actions be bound to a set of authentication credentials. This ensures that a user must first authenticate successfully to the TOE before access to the wireless network or the management interface is granted.

Prior to any access to the WLAN, a client must be properly authorized; this can either be through a pre-shared key or through certificate authentication (EAP-TLS), or through specific MAC address. In any of these cases, no clients are allowed access to the WLAN outside of the TOE's control.

All access to the Management Interface shall require the administrator to first authenticate to the server. There are no functions available to unauthenticated users, assuring that no administrative functions can be accessed without successful authentication.

8.1.6.2 FPT_SEP.1

The WLAN portion of the TOE is a self-contained hardware unit, providing complete separation from all outside processes. Only physical access to this portion of the TOE can potentially violate domain separation, and this is protected by the IT Environment.

The database portion of the TOE is a software component residing on a secured server within the IT environment. This portion of the TOE executes as a kernel-mode (privileged) process, fully enabling operating system protection from other processes.

8.1.6.3 FPT_TST_EXP.1

The TOE performs a series of tests on startup to verify the integrity of the hardware and software that make up WLAN portion the TOE. These tests are used to assure the correct security functionality when the TOE is active. These tests provide their results in the form of audit records and in the lights which are on located on the outside of the hardware. Once the hardware has started, the software performs another series of tests to verify the integrity of the operating system and applications used to perform the network and security operations. The software checks use FIPS-approved methods to verify integrity. Tests can be performed at any time by restarting the TOE.

8.1.6.4 FPT_TST_EXP.2

The TOE executed FIPS 140-2-approved checks on the integrity of the cryptographic components within the TOE. These tests can be performed at any time by restarting the TOE. Continuous tests are performed on the random number generator, as well as known answer tests on the algorithms.

8.2 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.

8.2.1 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 Process]
- 00000139-002 [Software Configuration Management Procedure]

Assurance Requirements: ACM_CAP.3, ACM_SCP.1.

8.2.2 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-525A-3 User' Guide and the 3e-030-2 Security Server User's Guide, and in 00000310-001 {Delivery Procedure].

Assurance Requirements: ADO_DEL.1, ADO_IGS.1.

8.2.3 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-525A-3 Internal Specification Sheet (satisfies ADV_FSP.1, ADV_RCR.1)
- 3e-030-2 Internal Specification Sheet (satisfies ADV_FSP.1, ADV_RCR.1)
- 22000201-702 [3e-525A-3 Access System Functional Specification] (satisfies ADV_FSP.1)
- 22000201-703 [3e-525A-3 Access System High Level Design Doc] (satisfies ADV_HLD.1)

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

8.2.4 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-525A-3 User' Guide and the 3e-030-2 Security Server User's Guide.

Assurance Requirements: AGD_ADM.1, AGD_USR.1.

8.2.5 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 Process] and 00000112-001 [Design Release and Change Control Procedure].

Assurance Requirements: ALC_FLR.2.

8.2.6 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. See 3eTI document 22000201-715 [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.

8.2.7 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-525A-3 User' Guide and the 3e-030-2 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:

- 3e-525A-3 Vulnerability Analysis
- 3e-030-2 Vulnerability Analysis

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

8.3 Strength of Function

The Strength of Function claim is SOF-Basic. Authentication by a password, specifically regarding FIA_UAU.1 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. Strength of Function has been documented in the FIPS 140-2 Security Policy as follows:

Authentication Mechanism	Strength of Mechanism
Userid and password	Minimum 8 characters => 72^8 = 7.22E14
Static Key (TDES or AES)	TDES (192-bits) or AES (128, 192, or 256-bits)
HMAC SHA-1 shared secret	Minimum 10 characters => 72^10 = 3.74E18
CA signature	128-bit
AES CCM pre-shared key	Minimum 8 characters => 72^8 = 7.22E14
EAP-TLS	CA signature => 128-bit

9. Rationale

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

9.1 Security Objectives Rationale

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

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

Table 15 - Security Objectives to Assumptions, Threats and Policies Mappings

	O.ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.AUDIT_REVIEW	O.CONFIGURATION_ IDENTIFICATION	O.CORRECT_ TSF_OPERATION	O.CRYPTOGRAPHY	O.DISPLAY_BANNER	O.DOCUMENTED_DESIGN	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_ TESTING	O.RESIDUAL_ INFORMATION	O.SELF_PROTECTION	OIE.TIME_STAMPS	O.TOE_ACCESS	O.VULNERABILITY_ANALYSIS	OE.NO_EVIL	OE.PHYSICAL	OE.HARDWARE
A.NO_EVIL																	X		
A.PHYSICAL																		X	
A.HARDWARE																			X
T.ACCIDENTAL_ADMIN_ ERROR	X								X								X		
T.ACCIDENTAL_ CRYPTO_ COMPROMISE												X	X						
T.MASQUERADE															X				
T.POOR_DESIGN				X				X								X			
T.POOR_IMPLEMENTATION				X							X					X			
T.POOR_TEST					X						X								
T.RESIDUAL_DATA												X							
T.TSF_COMPROMISE									X			X	X						
T.UNATTENDED_ SESSION															X				
T.UNAUTHORIZED_ ACCESS										X									
T.UNAUTH_ADMIN_ACCESS	X								X						X		X		
T.UNIDENTIFIED_ ACTIONS			X																
P.ACCESS_BANNER							X												
P.ACCOUNTABILITY		X							X					X	X				
P.CRYPTOGRAPHY						X						X							
P.ENCRYPTED_CHANNEL						X													
P.NO_AD_HOC_NETWORKS										X									

9.1.1.1 A.NO_EVIL

Authorized Administrators, including the Crypto-Officers, are non-hostile, appropriately trained and will follow and abide by the instructions provided by the TOE guidance documentation. The OE.NO_EVIL objective ensures that only non-hostile, competent administrators (following guidance) manage the TOE.

9.1.1.2 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, in addition to the physical security provided by the enclosure of the TOE itself. The physical environment provides reliable power and air conditioning controls to insure reliable operation of the hardware. The OE.PHYSICAL objective provides for the physical security of the TOE.

9.1.1.3 A.HARDWARE

The software portion of TOE (3e-SS) will be installed in a hardware system that is running Windows 2000 Server or Windows 2003 Server, with a network interface card installed. The OE.HARDWARE objective assures that the proper environment is available for the installation of all components of the TOE.

9.1.1.4 T.ACCIDENTAL_ADMIN_ ERROR

An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms. OE.NO_EVIL helps to mitigate this threat by ensuring that incorrect configuration would not be purposeful, only accidental, and unlikely due to proper training and guidance. O.ADMIN_GUIDANCE help to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is insecure. O.MANAGE also contributes to mitigating this threat by providing administrators the capability to view configuration settings. For example, if the Administrator/Crypto-Officer made a mistake when configuring the set of permitted user authentication credentials, providing them the capability to view the lists of authentication credentials affords them the ability to review the list and discover any mistakes that might have been made.

9.1.1.5 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 any residual data is removed from network packet objects and ensuing that cryptographic material is not accessible once it is no longer needed. O.SELF_PROTECTION ensures that the TOE will have adequate protection from external sources and that all TSP functions are invoked.

9.1.1.6 T.MASQUERADE

A user may masquerade as an authorized user or the authentication server to gain access to data or TOE resources. O.TOE_ACCESS mitigates this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanism this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE.

9.1.1.7 T.POOR_DESIGN

Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program. O.CONFIGURATION_IDENTIFICATION plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE's design documentation and the ability to report and resolve security flaws. O.DOCUMENTED_DESIGN counters this threat, to a degree, by requiring that the TOE be developed using sound engineering principles. The use of a high level design and the functional specification ensure that developers responsible for TOE development understand the overall design of the TOE. This in turn decreases the likelihood of design flaws and increases the chance that accidental design errors will be discovered. ADV_RCR.1 ensures that the TOE design is consistent across the High Level Design and the Functional Specification. O.VULNERABILITY_ANALYSIS ensures that the TOE has been analyzed for obvious vulnerabilities and that any vulnerabilities found have been removed or otherwise mitigated, this includes analysis of any probabilistic or permutational mechanisms incorporated into a TOE.

9.1.1.8 T.POOR_IMPLEMENTATION

Unintentional errors in TOE design implementation 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's 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 provide evidence and demonstration that all security functions perform as specified through independent sample testing. O.VULNERABILITY_ANALYSIS ensures that the TOE has been analyzed and tested to demonstrate that it is resistant to obvious vulnerabilities.

9.1.1.9 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 ATE_COV.1 ensures that the developers provide evidence and demonstration that all security functions perform as specified through independent sample testing. 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.

9.1.1.10 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 contributes to the mitigation of this threat by ensuring that any residual data is removed from network packet objects and ensuing that cryptographic material is not accessible once it is no longer needed.

9.1.1.11 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 management of TSF data to the administrator. O.RESIDUAL_INFORMATION contributes to the mitigation of this threat by ensuring that any residual data is removed from network packet objects and ensuing that cryptographic material is not accessible once it is no longer needed. O.SELF_PROTECTION requires that the TOE environment be able to protect itself from tampering and that the security mechanisms in the TOE cannot be bypassed. Without this objective, there could be no assurance that users could not view or modify TSF data or TSF executables.

9.1.1.12 T.UNATTENDED_ SESSION

A user may gain unauthorized access to an unattended session. Since the only sessions that are established with the TOE are anticipated to be administrative sessions, this threat is restricted to administrative sessions. The termination of general user sessions is expected to be handled by the IT environment. O.TOE_ACCESS helps to mitigate this threat by including mechanisms that place controls on administrator sessions. Administrator sessions are dropped after a 10 minute time period of user inactivity. Dropping the connection of a session (after the specified time period) reduces the risk of someone accessing the machine where the session was established, thus gaining unauthorized access to the session.

9.1.1.13 T.UNAUTHORIZED_ ACCESS

A user may gain access to services (either on the TOE or by sending data through the TOE) for which they are not authorized according to the TOE security policy. O.MEDIATE works to mitigate this threat by ensuring that all network packets that flow through the TOE are subject to the information flow policies. One of the rules ensures that the network identifier in a packet is in the set of network identifiers associated with a TOE's network interface. Therefore, if a user supplied a network identifier in a packet that purported to originate from a network associated with a TOE network interface other than the one the user supplied the packet on, the packet would not be allowed to flow through the TOE, or access TOE services. Another rule provides further granularity of access control by enabling the administrator to control the source and destination address, destination port, protocol, and application level commands. By implementing this level of access control an attacker would not be allowed access to other hosts and applications residing on the protected network. Additionally, the TOE maintains "state" information of all approved connections. This function ensures that each packet arriving at a TOE interface purporting to be part of an approved connection through or to the TOE, is checked against a current and valid list of connection parameters (e.g. for a TCP/IP connection; source and destination address, ports, SYN and ACK numbers, flags, etc.) prior to allowing the packet through or to the TOE. The TOE requires successful authentication (strong authentication via single-use password, encrypted authentication and/or both, with account lock-out capability) to the TOE prior to gaining access to certain services on or mediated by the TOE. By implementing strong authentication to gain access to these services, an attacker's opportunity to successfully conduct a man-in-the-middle and/or password guessing attack is greatly reduced. Lastly, the TSF must ensure that all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services. The TOE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc to the Administrator/Crypto-Officer. This feature ensures that no other user can modify the information flow policy to bypass the intended TOE security policy.

9.1.1.14 T.UNAUTH_ADMIN_ACCESS

An ***unauthorized user or process may gain access to an administrative account.*** 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 mistakes that an administrator might make that could cause the TOE to be configured in a non-secure manner. O.MANAGE mitigates this threat by restricting access to administrative functions and management of TSF data to administrators. O.TOE_ACCESS helps to mitigate this threat by including mechanisms that place controls on administrator sessions. OE.NO_EVIL helps to mitigate this threat by ensuring that TOE administrators have guidance that instructs them how to administer the TOE in a secure manner.

9.1.1.15 T.UNIDENTIFIED_ ACTIONS

The administrator may fail to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach. O.AUDIT_REVIEW helps to mitigate this threat by providing the Crypto-Officer with a required minimum set of configurable audit events that could indicate a potential security violation. By configuring these auditable events, the TOE monitors the occurrences of these events (e.g. set number of authentication failures, set number of information policy flow failures, self-test failures, etc.) and immediately notifies all TOE administrators once an event has occurred or a set threshold has been met. If a potential security violation has been detected, the TOE displays a message that identifies the potential security violation to all administrative consoles. The consoles include the local TOE console and any active remote administrative sessions. If an administrator is not currently logged into the TOE, the message is stored and immediately displayed the next time an administrator logs into the TOE. This message is displayed to all administrative roles and will remain on the screen for each administrative role until each administrative role acknowledges the message. In addition to displaying the potential security violation, the message must contain all audit records that generated the potential security violation. By enforcing the message content and display, this objective provides assurance that a TOE administrator will be notified of a potential security violation.

9.1.1.16 P.ACCESS_BANNER

The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system. O.DISPLAY_BANNER satisfies this policy by ensuring that the TOE displays an Administrator configurable banner that provides all users with a warning about the unauthorized use of the TOE. A banner will be presented for all TOE services that require authentication. In other words, it will be required for all administrative actions. The presentation of banners prior to actions that take place in the environment as a result of the passing of traffic through the TOE is assumed to be provided by the IT environment.

9.1.1.17 P.ACCOUNTABILITY

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

O.AUDIT_GENERATION addresses this policy by providing the Crypto-Officer with the capability of configuring the audit mechanism to record the actions of a specific user, or review the audit trail based on the identity of the user. Additionally, the Crypto-Officer's ID is recorded when any security relevant change is made to the TOE (e.g. access rule modification, start-stop of the audit mechanism, establishment of a trusted channel, etc.).

O.MANAGE ensures that access to administrative functions and management of TSF data is restricted to the administrator.

OIE.TIME_STAMPS plays a role in supporting this policy by requiring the TOE IT Environment to provide a reliable time stamp (configured locally by the Administrator/Crypto-Officer or via an external NTP server). The audit mechanism is required to include the current date and time in each audit record. All audit records that include the user ID, will also include the date and time that the event occurred.

O.TOE_ACCESS supports this policy by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanism this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE.

9.1.1.18 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 to 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.

9.1.1.19 P.ENCRYPTED_CHANNEL

The TOE shall provide the capability to encrypt/decrypt wireless network traffic between the TOE and those wireless clients that are authorized to join the network. O.CRYPTOGRAPHY satisfies this policy by requiring the TOE to implement NIST FIPS-validated cryptographic services to provide confidentiality and integrity protection of TSF data while in transit to remote parts of the TOE.

9.1.1.20 P.NO_AD_HOC_NETWORKS

In concordance with the DOD Wireless Policy, there shall be no ad hoc 802.11 or 802.15 networks allowed. O.MEDIATE works to mitigate this threat by ensuring that all network packets that flow through the TOE are subject to the information flow policies. One of the rules ensures that the network identifier in a packet is in the set of network identifiers associated with a TOE's network interface. Therefore, if a user supplied a network identifier in a packet that purported to originate from a network associated with a TOE network interface other than the one the user supplied the packet on, the packet would not be allowed to flow through the TOE, or access TOE services. Another rule provides further granularity of access control by enabling the administrator to control the source and destination address, destination port, protocol, and application level commands. By implementing this level of access control an attacker would not be allowed access to other hosts and applications residing on the protected network. Additionally, the TOE maintains "state" information of all approved connections. This function ensures that each packet arriving at a TOE interface purporting to be part of an approved connection through or to the TOE, is checked against a current and valid list of connection parameters (e.g. for a TCP/IP connection; source and destination address, ports, SYN and ACK numbers, flags, etc.) prior to allowing the packet through or to the TOE. The TOE requires successful authentication (strong authentication via single-use password, encrypted authentication and/or both, with account lock-out capability) to the TOE prior to gaining access to certain services on or mediated by the TOE. By implementing strong authentication to gain access to these services, an attacker's opportunity to successfully conduct a man-in-the-middle and/or password guessing attack is greatly reduced. Lastly, the TSF must ensure that all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services. The TOE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc to the Administrator/Crypto-Officer. This feature ensures that no other user can modify the information flow policy to bypass the intended TOE security policy.

9.1.2 Non-IT Environment Security Objectives Rationale

9.1.2.1 A.HARDWARE

The software portion of TOE (3e-SS) will be installed in a hardware system that is running Windows 2000 Server or Windows 2003 Server, with a network interface card installed. OE.HARDWARE ensures that the TOE is operating on the hardware, operating system, and associated software that would ensure the software portion of the TOE operates correctly and has sufficient space to execute the security functions correctly.

9.1.2.2 A.NO_EVIL

Authorized Administrators, including Crypto-Officers, are non-hostile, appropriately trained and will follow and abide by the instructions provided by the TOE guidance documentation. OE.NO_EVIL ensures that administrators are responsible and will not intentionally create threats to the TOE.

9.1.2.3 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, in addition to the physical security provided by the enclosure of the TOE itself. The physical environment provides reliable power and air conditioning controls to insure reliable operation of the hardware. OE.PHYSICAL assures that the TOE will be protected from physical threats by restricting access to the location where the TOE resides.

9.2 Security Requirements Rationale

9.2.1 TOE Security Requirements Rationale

Table 16 - Rationale for TOE Security Requirements

	O.ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.AUDIT_REVIEW	O.CONFIGURATION_ IDENTIFICATION	O.CORRECT_ TSF_OPERATION	O.CRYPTOGRAPHY	O.DISPLAY_BANNER	O.DOCUMENTED_DESIGN	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_ TESTING	O.RESIDUAL_ INFORMATION	O.SELF_PROTECTION	O.TOE_ACCESS	O.VULNERABILITY_ANALYSIS
FAU_GEN.1-NIAP-0410		X													
FAU_GEN.2-NIAP-0410		X													
FAU_SAR.1			X												
FAU_SAR.2			X												
FAU_SAR.3			X												
FAU_SEL.1-NIAP-0407		X													
FCS_BCM_EXP.1						X									
FCS_CKM.1						X									
FCS_CKM_EXP.2						X						X			
FCS_CKM.4						X						X			
FCS_COP_EXP.1						X									
FCS_COP_EXP.2						X									
FDP_IFC.1 (1)										X					
FDP_IFC.1 (2)										X					
FDP_IFF.1-NIAP-0407 (1)										X					
FDP_IFF.1-NIAP-0407 (2)										X					
FDP_ITT.1												X			
FDP_RIP.1 (1)												X			
FIA_AFL.1-NIAP-0425														X	
FIA_ATD.1														X	
FIA_UAU.1														X	
FIA_UID.1														X	
FIA_USB.1-NIAP-0415		X													
FMT_MOF.1 (1)									X						
FMT_MOF.1 (2)									X						
FMT_MSA.1									X						
FMT_MSA.2									X						
FMT_MSA.3-NIAP-0409									X	X					
FMT_MTD.1 (1)									X						
FMT_MTD.1 (2)									X						
FMT_MTD.1 (3)									X						
FMT_REV.1										X					
FMT_SMF.1 (1)									X						
FMT_SMF.1 (2)									X						
FMT_SMF.1 (3)										X					
FMT_SMF.1 (4)										X					

	O.ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.AUDIT_REVIEW	O.CONFIGURATION_ IDENTIFICATION	O.CORRECT_ TSF_OPERATION	O.CRYPTOGRAPHY	O.DISPLAY_BANNER	O.DOCUMENTED_DESIGN	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_ TESTING	O.RESIDUAL_ INFORMATION	O.SELF_PROTECTION	O.TOE_ACCESS	O.VULNERABILITY_ANALYSIS
FMT_SMR.1 (1)									X						
FPT_RVM.1													X		
FPT_SEP.1													X		
FPT_TST_EXP.1					X										
FPT_TST_EXP.2					X										
FTA_SSL.3														X	
FTA_TAB.1							X								
ACM_CAP.3				X											
ACM_SCP.1				X											
ADO_DEL.1	X														
ADO_IGS.1															
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	X
AVA_VLA.1															X

9.2.1.1 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 that the administrator has the information necessary to install the TOE in the evaluated configuration. Often a vendor 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 mandates the developer provide the administrator with guidance on how to operate the TOE in a secure manner. This includes describing the interfaces the administrator uses in managing the TOE and any security parameters that are configurable by the administrator. The documentation also provides a description of how to 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. This could include guidance on the setup of wireless clients for use with the TOE. If it is the case that the wireless clients may be configured by administrators that are not administrators of this TOE, then that guidance may be user guidance from the perspective of this TOE.

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.

9.2.1.2 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 Crypto-Officer 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.

FAU_GEN.2-NIAP-0410 ensures that the audit records associate a user identity with the auditable event. In the case of authorized users, the association is accomplished with the user ID. In all other cases, the association is based on the source network identifier, which is presumed to be the correct identity, but cannot be confirmed since these subjects are not authenticated.

FAU_SEL.1-NIAP-0407allows for the selection of events to be audited. This requires that the criteria used for the selection of auditable events to be defined. For example, the user identity can be used as selection criteria for the events to be audited.

FIA_USB.1-NIAP-0415 plays a role is satisfying this objective by requiring a binding of security attributes associated with users that are authenticated with the subjects that represent them in the TOE. This only applies to authorized users, since the identity of unauthenticated users cannot be confirmed. Therefore, the audit trail may not always have the proper identity of the subject that causes an audit record to be generated (e.g., presumed network address of an unauthenticated user may be a spoofed address).

9.2.1.3 OE.AUDIT_REVIEW

The TOE will provide the capability to selectively view audit information.

FAU_SAR.1 ensures that the TSF provides those responsible for the TOE with facilities to review the TOE audit records (e.g., the Crypto-Officer can construct a sequence of events provided the necessary events were audited).

FAU_SAR.2 ensures that the audit records can only be reviewed by users specifically granted that right, which is the defined Crypto-Officer account.

FAU_SAR.3 provides the Crypto-Officer with the ability to selectively review the contents of the audit trail based on established criteria. This capability allows the Crypto-Officer to focus their audit review to what is pertinent at that time.

9.2.1.4 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.

9.2.1.5 O.CORRECT_ TSF_OPERATION

The TOE shall provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site. This is accomplished through the Audit Log & System Log, which records security relevant operational events, as well as internal operational errors, if any. FPT_TST_EXP.1 is necessary to ensure the correct operation TSF hardware. 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 addresses 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.

9.2.1.6 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.1 and FCS_COP_EXP.2 mandates the use of FIPS validated 3DES (FIPS 46-3) and AES (FIPS 197) algorithms for all encryption/decryption operations.

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 data decryption and encryption that a NIST approved algorithm is used, and that the algorithm meets the FIPS PUB 140-2 standard.

9.2.1.7 O.DISPLAY_BANNER

The TOE shall display an advisory warning regarding use of the TOE prior to permitting the use of any TOE services that require authentication. FTA_TAB.1 meets this objective by requiring the TOE display a Administrator/Crypto-Officer defined banner before a user can establish an authenticated session. This banner is under complete control of the Administrator/Crypto-Officer in which he specifies any warnings regarding unauthorized use of the TOE and removes any product or version information if desired. The only time that it is envisioned that an authenticated session would need to be established is for the performance of TOE administration. Bannering is not necessary prior to use of services that pass network traffic through the TOE.

9.2.1.8 *O.DOCUMENTED_DESIGN*

The design of the TOE is adequately and accurately documented. ADV_FSP.1, ADV_HLD.1, and ADV_RCR.1 support this objective by requiring that the TOE be developed using sound engineering principles. The use of a high level design document and functional specification ensure that developers responsible for TOE development understand the overall design of the TOE. This in turn decreases the likelihood of design flaws and increases the chance that accidental design errors will be discovered.

9.2.1.9 *O.MANAGE*

The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. The FMT requirements are used to satisfy this 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 management functions in order to control the behavior of security functions.

FMT_MSA.1, FMT_MSA.2 provides the Administrator/Crypto-Officer the ability to accept only secure values and modify security attributes.

FMT_MSA.3-NIAP-0409(1) requires that, by default, the TOE does not allow an information flow, rather than allowing information flows until a rule in the rule set disallows it.

FMT_MOF.1(1)(2) and FMT_MSA.3-NIAP-0409(2) are related to the services provided by FIA_UAU.1(1) and provide the Administrator/Crypto-Officer control as to the availability of these services. FMT_MOF.1(1)(2) provides the ability to enable or disable the TOE services to the Administrator/Crypto-Officer. FMT_MSA.3-NIAP-0409(2) requires that these services by default are disabled. Since the Administrator/Crypto-Officer must explicitly enable these services it ensures the Administrator/Crypto-Officer is aware that they are running. This requirement does afford the Administrator/Crypto-Officer the capability to override this restrictive default and allow the services to be started whenever the TOE reboots or is restarted.

FMT_MOF.1(1) is used to ensure the administrators have the ability to invoke the TOE self-tests at any time. The ability to invoke self-tests is provided to all administrators. The Administrator/Crypto-Officer is able to modify the behavior of the tests (e.g., select when they run, select a subset of the tests). FMT_MOF.1(2) specifies the ability of the administrators to control the security functions associated with audit and alarm generation. The ability to control these functions has been assigned to the appropriate administrative roles.

FMT_MTD.1(1)(2)(3) relate to the ability of the administrators to review, establish and modify security settings for the TOE, including the initialization of authentication credentials and cryptographic keys.

FMT_SMF.1(1) specifies the ability of the Crypto-Officer to establish the encryption settings for the network using approved encryption algorithms. FMT_SMF.1(2) specifies the ability of authorized administrators to modify the audit functions of the TOE, tailoring the recording of events to the environment.

FMT_SMR.1 specifies that the TOE shall maintain the roles of Crypto-Officer, Administrator and User. The Crypto-Officer access is the first default account, while User accounts are all clients of the TOE without administrative-level access.

9.2.1.10 *O.MEDIATE*

The TOE must mediate the flow of information to and from wireless clients communicating via the TOE RF Transmitter/Receiver interface in accordance with its security policy. FDP_IFC.1(1) and FDP_IFF.1-NIAP-0407(1) ensure that the TOE has the ability to mediate packet flow based upon the authentication credentials of the sender. FDP_IFC.1(2) and FDP_IFF.1-NIAP-0407(2) ensure that the TOE enforces cryptographic policies on the packet flow based on the administrator settings. FDP_IFC.1 provides the capability to set policy, while FDP_IFF.1-NIAP-0407 identifies the attributes that will be used to make policy decisions FMT_SMF.1(3), FMT_SMF.1(4) and FMT_MSA.3 ensure that the TOE provides an interface through which the information flow control policy can be set. FMT_REV.1 ensures that the credentials can be revoked preventing previously authorized users from continuing to access TOE resources.

9.2.1.11 *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.PARTIAL_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.

9.2.1.12 *O.RESIDUAL_ INFORMATION*

The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.

FDP_RIP.1 is used to ensure the contents of resources are not available once the resource is reallocated. For this TOE it is critical that the memory used to build network packets is either cleared or that some buffer management scheme be employed to prevent the contents of a packet being disclosed in a subsequent packet (e.g., if padding is used in the construction of a packet, it must not contain another user's data or TSF data).

FDP_ITT.1 is used to ensure that internal communications between separate parts of the TOE are secured against unauthorized access which could result in the loss, disclosure or modification of such data. This is critical in protecting the client authentication credentials when they are stored on a separate authentication server.

FCS_CKM_EXP.2 places requirements on how cryptographic keys are managed within the TOE. This requirement places restrictions in addition to FDP_RIP.1, in that when a cryptographic key is moved from one location to another (e.g., calculated in some scratch memory and moved to a permanent location) that the memory area is immediately cleared as opposed to waiting until the memory is reallocated to another subject.

FCS_CKM.4 applies to the destruction of cryptographic keys used by the TSF. This requirement specifies how and when cryptographic keys must be destroyed. The proper destruction of these keys is critical in ensuring the content of these keys cannot possibly be disclosed when a resource is reallocated to a user.

9.2.1.13 O.SELF_PROTECTION

The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure. FPT_SEP.1 was chosen to ensure the TSF provides a domain that protects itself from untrusted users. If the TSF cannot protect itself it cannot be relied upon to enforce its security policies. FPT_RVM.1 ensures that the TSF makes policy decisions on all interfaces that perform operations on subjects and objects that are scoped by the policies. Without this non-bypassability requirement, the TSF 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 TOE resources (including TSF data and executable code) regardless of the defined policies. This includes controlling the accessibility to interfaces, as well as what access control is provided within the interfaces.

9.2.1.14 O.TOE_ACCESS

The TOE shall provide mechanisms that control a user's logical access to the TOE.

FIA_AFL.1-NIAP-0425 assures that unsuccessful authentication attempts to the management interface will result in the account being locked, requiring that another administrator unlock the account. This assures access to the management interface is not subject to brute force attacks.

FIA_ATD.1 ensures that all users will have some form of credentials to authenticate to the system. User accounts are not allowed to have null passwords.

FIA_UID.1 plays a small role in satisfying this objective by ensuring that every user is identified before the TOE performs any mediated functions. In most cases, the identification cannot be authenticated (e.g., a user attempting to send a data packet through the TOE that does not require authentication. It is impractical to require authentication of all users that attempt to send data through the TOE, therefore, the requirements specified in the TOE require authentication where it is deemed necessary. This does impose some risk that a data packet was sent from an identity other than specified in the data packet.

AVA_SOF.1 requires that any permutational or probabilistic mechanism in the TOE be analyzed 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.

FIA_UAU.1 contributes to this objective by limiting the services that are provided by the TOE to unauthenticated users. Management requirements and the unauthenticated information flow policy requirement provide additional control on these services.

FTA_SSL.3 contributes to the security of the management interface by assuring that inactive sessions are automatically closed after a specified amount of time.

In order to control logical access to the TOE an authentication mechanism is required. The local administrator authentication mechanism is necessary to ensure an administrator has the ability to login to the TOE regardless of network connectivity (e.g., it would be unacceptable if an administrator could not login to the TOE because the authentication server was down, or that the network path to the authentication server was unavailable).

9.2.1.15 O.VULNERABILITY_ ANALYSIS

The TOE shall undergo some vulnerability analysis demonstrate 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 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.

9.2.2 IT Environment Security Requirements Rationale

Table 17 - Rationale for Requirements on the TOE IT Environment

	OIE.TIME_STAMPS
FPT_STM.1	**X**

9.2.2.1 OIE.TIME_STAMPS

The IT Environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps. FPT_STM.1 requires that the IT Environment be able to provide reliable time stamps for its own use as well as the TOE. Time stamps include date and time and are reliable in that they are always available to the TOE.

9.3 Rationale for Assurance Requirements

EAL2 augmentation 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), ACM_CAP.3 (Authorization Controls), and AVA_MSU.1 (Misuse – Examination of Guidance).) was believed to best achieve this goal. It was 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.

9.4 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 18 - TOE Security Functional Requirement Dependencies

Requirement Number	Functional Requirements	Dependencies	Dependency	Dependency Met
1	FAU_GEN.1	FPT_STM.1	33	X
2	FAU_GEN.2	FAU_GEN.1	1	X
		FIA_UID.1	21	X
4	FAU_SAR.1	FAU_GEN.1	1	X
5	FAU_SAR.2	FAU_SAR.1	4	X
6	FAU_SAR.3	FAU_SAR.1	4	X
7	FAU_SEL.1	FAU_GEN.1	1	X
		FMT_MTD.1	27	X
8	FCS_BCM_EXP.1	No dependencies	-	X
9	FCS_CKM.1	FCS_CKM_EXP.2 or FCS_COP_EXP.1	10 (FCS_CKM_EXP.2)	X
		FCS_CKM.4	11	X
		FMT_MSA.2	25	X
10	FCS_CKM_EXP.2	FDP_ITC.1 or FCS_CKM.1	9 (FCS_CKM.1)	X
		FMT_MSA.2	25	X
11	FCS_CKM.4	FCS_CKM.1	9 (FCS_CKM.1)	X
		FMT_MSA.2	25	X
12	FCS_COP_EXP.1	FCS_CKM.1	9 (FCS_CKM.1)	X
		FCS_CKM.4	11	X
		FMT_MSA.2	25	X
13	FCS_COP_EXP.2	FCS_CKM.1	9 (FCS_CKM.1)	X
		FCS_CKM.4	11	X
		FMT_MSA.2	25	X
14	FDP_IFC.1	FDP_IFF.1-NIAP-0407 *	15	X
15	FDP_IFF.1-NIAP-0407 *	FDP_IFC.1	14	X
		FMT_MSA.3	26	X
16	FDP_ITT.1	FDP_IFC.1	15 (FDP_IFC.1)	X
17	FDP_RIP.1	No dependencies	-	X
18	FIA_AFL.1	FIA_UAU.1	20	X
19	FIA_ATD.1	No dependencies	-	X
20	FIA_UAU.1	FIA_UID.1	21	X
21	FIA_UID.1	No dependencies	-	X
22	FIA_USB.1	FIA_ATD.1	19	X
23	FMT_MOF.1	FMT_SMF.1	29	X
		FMT_SMR.1	30	X
24	FMT_MSA.1	FDP_IFC.1	14 (FDP_IFC.1)	X
		FMT_SMF.1	29	X
		FMT_SMR.1	30	X
25	FMT_MSA.2	ADV_SPM.1		Rationale
		FDP_IFC.1	14 (FDP_IFC.1)	X
		FMT_MSA.1	24	X
		FMT_SMR.1	30	X
26	FMT_MSA.3	FMT_MSA.1	24	X
		FMT_SMR.1	30	X
27	FMT_MTD.1	FMT_SMF.1	29	X
		FMT_SMR.1	30	X
28	FMT_REV.1	FMT_SMR.1	30	X
29	FMT_SMF.1	No dependencies	-	X
30	FMT_SMR.1	FIA_UID.1	21	X
31	FPT_RVM.1	No dependencies	-	X
32	FPT_SEP.1	No dependencies	-	X

Requirement Number	Functional Requirements	Dependencies	Dependency	Dependency Met
33	FPT_STM.1	No dependencies	-	X
34	FPT_TST_EXP.1	No dependencies	-	X
35	FPT_TST_EXP.2	No dependencies	-	X
36	FTA_SSL.3	No dependencies	-	X
37	FTA_TAB.1	No dependencies	-	X

9.5 *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. The following table identifies the functional requirement, its correspondent dependency and the analysis and rationale for not supporting the dependency in this ST.

Table 19 - Unsupported Dependency Rationale

Requirement	Unsatisfied Dependencies	Dependency Analysis and Rationale
FMT_MSA.2	ADV_SPM.1	Typically, this requirement is part of an EAL4 requirement set. At basic robustness, there is no requirement for the vendor to model the security policies within this ST. Informal models of the Specified Users SFP and the Wireless Encryption SFP are contained within the ST, and are therefore not required to be provided by the vendor.

9.6 *Explicitly Stated Requirements Rationale*

Table 20 - 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.
FCS_CKM_EXP.2	Cryptographic key handling & storage	This explicit requirement is necessary since the CC does not specifically provide components for key handling and storage.
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	This explicit requirement is necessary because it describes requirements for a cryptomodule rather that the entire TSF.
FPT_TST_EXP.1	TSF Testing	This explicit requirement is necessary because, as identified in the US Government PP 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.
FDP_IFF.1-NIAP-0407 *	Simple Security Attributes	This requirement was taken from the Common Criteria Basic Robustness Guide.
FAU_GEN.1-NIAP-0410	Audit data generation	This requirement was taken from the Common Criteria Basic Robustness Guide.
FAU_GEN.2-NIAP-0410	User identity association	This requirement was taken from the Common Criteria Basic Robustness Guide.
FAU_SEL.1-NIAP-0407	Selective audit	This requirement was taken from the Common Criteria Basic Robustness Guide.
FIA_AFL.1-NIAP-0425	Administrator Authentication failure handling	This requirement was taken from the Common Criteria Basic Robustness Guide.

Explicit Requirement	Identifier	Rationale
FIA_USB.1-NIAP-0415	User-subject binding	This requirement was taken from the Common Criteria Basic Robustness Guide.
FMT_MSA.3-NIAP-0409	Static attribute initialization	This requirement was taken from the Common Criteria Basic Robustness Guide.

9.7 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.

9.8 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.

The Strength of Function claim is SOF-basic based on the overall TOE. Strength of Function has been documented in the FIPS 140-2 Security Policy as follows:

Authentication Mechanism	Strength of Mechanism
Userid and password	Minimum 8 characters => 72^8 = 7.22E14
Static Key (TDES or AES)	TDES (192-bits) or AES (128, 192, or 256-bits)
HMAC SHA-1 shared secret	Minimum 10 characters => 72^10 = 3.74E18
CA signature	128-bit
AES CCM pre-shared key	Minimum 8 characters => 72^8 = 7.22E14
EAP-TLS	CA signature => 128-bit

9.9 Protection Profile Claims Rationale

There is no claimed PP conformance for this ST.