
# 3eTI Technologies International

# 3e-525/523 Series Wireless Network Access Points

## Security Target

**Version 1.0**

**Revision I**

**October 8th, 2015**

3e Technologies International Wireless Network Access Point Security Target, Revision I.

*Document ID Number: 22000225-701 Revision I*

Contact:

3e Technologies International, Inc.
9715 Key West Avenue
5th Floor
Rockville, MD 20850 USA

Telephone: +1 (301) 670-6779
Fax: +1 (301) 670-6989

Website: http://www.3eti.com/
Email: mailto:info@3eti.com

## Table of Contents

## List of Tables and Figures

# 1 Security Target Introduction

This section presents security target (ST) identification information and an overview of the ST. The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A.

## *1.1 Security Target References*

**ST Title:** 3eTI 3e-525/523 Series Wireless Network Access System Security Target

**ST Version:** Version 1.0, Rev I

**Vendor:** 3e Technology International, Inc.

**ST Publication Date:** October 08, 2015

**Keywords:** Access system, radio, wireless, network, wireless local area network, wireless LAN, WLAN, 802.1X, 802.11

### 1.1.1 Document References

The following documents were used to develop the Security Target.

**Table 1-1: US Government and Standards Document References**

| Reference | Document |
|---|---|
| [CC_PART1] | Common Criteria for Information Technology Security Evaluation-Part 1: Introduction and general model, September 2012, version 3.1 R4, CCMB-2012-09-001 |
| [CC_PART2] | Common Criteria for Information Technology Security Evaluation-Part 2: Security functional components, September 2012, version 3.1 R4, CCMB-2012-09-002 |
| [CC_PART3] | Common Criteria for Information Technology Security Evaluation-Part 2: Security assurance components, September 2012, version 3.1 R4, CCMB-2012-09-003 |
| [CEM] | Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2012, version 3.1 R4, CCMB-2012-09-004 |
| [WLANPP] | US Government, Protection Profile for Wireless Local Area Network (WLAN) Access Systems, Dec 01, 2011, Version 1.0 |
| [FIPS PUB 140-2] | National Institute of Standards and Technology, FIPS PUB 140-2 Security Requirements for Cryptographic Modules, December 2002. |
| [FIPS PUB 186-3] | Digital Signature Standard (DSS), June 2009 |
| [NIST SP 800-56A] | NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” |
| [NIST SP 800-57] | NIST Special Publication 800-57, “Recommendation for Key Management” |
| [NIST SP 800-120] | NIST Special Publication 800-120, Recommendation for EAP Methods Used in Wireless Network Access Authentication, September 2009. |
| [IEEE 802.1X] | IEEE 802.1X-2004, “Standard for Local and metropolitan area networks, Port-Based Network Access Control, 2004 |
| [IEEE 802.11] | IEEE 802.11-2007; Standard for Information Technology: Telecommunications and information exchange between systems: Local and metropolitan area networks: Specific requirements: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 802.11, March 2007 |
| RFC 2865 | Remote Authentication Dial In User Service (RADIUS), June 2000 |
| RFC 3394 | Advanced Encryption Standard (AES) Key Wrap Algorithm |
| RFC 5216 | The EAP-TLS Authentication Protocol, March 2008 |
| RFC 4301 | Security Architecture for the Internet Protocol |

| Reference | Document |
|---|---|
| RFC 4303 | IP Encapsulating Security Payload (ESP) |
| RFC 4106 | The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP) |

### *1.2 TOE References*

**TOE Identification:** 3eTI AirGuard™ Wireless Network Access System.

The TOE consists of the following products:

- 3e-525N Access Point; Hardware version 1.0,firmware version 5.1, build number 221
- 3e-525N MP Access Point; Hardware version 1.0,firmware version 5.1, build number 221
- 3e-525NV Access Point; Hardware version 1.0,firmware version 5.1, build number 221
- 3e-523N Access Point; Hardware version 1.0,firmware version 5.1, build number 221
- 3e-523NR Access Point; Hardware version 1.0,firmware version 5.1, build number 221

### *1.3 TOE Overview*

The Target of Evaluation (TOE) includes the following 3eTI AirGuard™ wireless LAN Access Points models: 3e-525N, 3e-525N MP, 3e-525NV, 3e-523N and 3e-523NR. The modules share the identical hardware platform and firmware. Differences between models are limited to enclosure, power options, the number of Wi-Fi radio interfaces and extra video component.

The table below shows the differences among the 3eTI Access Points

**Table 1-2 3eTI Access Point Products Comparison**

| Model | Number of Radio | Radio Mode | Mechanical | Comments |
|---|---|---|---|---|
| 3e-525N | 2 | Access Point | Ruggedized for industrial and outdoor | |
| 3e-525N MP | 2 | Access Point | Ruggedized for industrial and outdoor | Same as 3e-525N except mobile power input |
| 3e-525NV | 2 | Access Point | Ruggedized for industrial and outdoor | Same as 3e-525N with extra video capture card |
| 3e-523N | 1 | Access Point | Indoor | |
| 3e-523NR | 1 | Access Point | Ruggedized for industrial and | Same as 3e-523N expect |

| | | | | |
|---|---|---|---|---|
| | | | outdoor | enclosure for outdoor deployment |

### 1.3.1 TOE Type

The TOE is classified as a Wireless Local Area Network (WLAN) Access Device. The TOE employs Mesh networking, which allows multiple TOEs to network within the operational environment.

This ST claims conformance to the US Government Protection Profile for Wireless Local Area Network (WLAN) Access Systems, December 01, 2011.

### 1.3.2 TOE Usage

The TOE sits between wired and wireless portions of an enterprise network and provides integrity and confidentiality of wireless traffic and restricts access of wireless endpoints to wired network systems. The TOE provides a secure, yet flexible, WLAN environment as Access Points that mediate authenticated wireless client's data through encryption/decryption and integrity protection between the wireless link and the wired LAN.

### 1.3.3 Hardware, Firmware, and Software Required by the TOE

The TOE consists of hardware and firmware residing on the Access Point appliances as listed in Section 1.2 above.

The evaluated configuration of the TOE requires the following Operational Environment support which is not included in the TOE's physical boundary.

- **RADIUS Server:** The TOE requires a RADIUS Server in the Operational Environment for wireless client authentication.
  - **Wireless Clients:** All wireless client hosts connecting to the wired network from the wireless network.
  - **Administrator Workstations:** Trusted administrators access the TOE through the HTTPS protocol.
  - **Audit Servers:** The TOE relies upon the audit server for storage of audit records.
  - **NTP Servers:** The TOE relies upon an NTP server to provide reliable time**.**

## *1.4 TOE Description*

### 1.4.1 Acronyms

The following acronyms and abbreviations are used in this Security Target:

**Table 1-3: Acronyms**

| Acronym | Definition |
|---|---|
| AES | Advanced Encryption Standard |
| AP | Access Point |

| Acronym | Definition |
|---|---|
| AS | Authentication Server |
| CA | Certificate Authority |
| CAVP | Cryptographic Algorithm Validation Program |
| CBC | Cipher Block Chaining (AES mode) |
| CC | Common Criteria for Information Technology Security Evaluation |
| CCM | Counter with Cipher Block Chaining-Message Authentication Code (AES mode) |
| CCMP | CCM Protocol (used to meet IEEE 800.11i) |
| CCTL | Common Criteria Testing Laboratory |
| CEM | Common Evaluation Methodology for Information Technology Security |
| CM | Configuration Management |
| CMVP | Cryptographic Module Validation Program |
| COTS | Commercial Off-The-Shelf |
| CSP | Critical Security Parameter |
| DFS | Dynamic Frequency Selection |
| DN | Distinguished Name |
| DSA | Digital Signature Algorithm |
| DSS | Digital Signature Standard |
| EAL | Evaluation Assurance Level |
| EAP | Extensible Authentication Protocol |
| EAPOL | EAP over LAN |
| EAP-TLS | Extensible Authentication Protocol-Transport Layer Security |
| ECB | Electronic Codebook (AES Mode) |
| EE PROM | Electrically Erasable Programmable Read-Only Memory |
| ESSID | Extended Session Set ID |
| FIPS | Federal Information Processing Standard |
| GTK | Group-wise transient key |
| GUI | Graphic User Interface |
| HLD | High Level Design |
| HMAC | Hashed Message Authentication Code |
| HTTPS | Secure Hypertext Transfer Protocol |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IP | Internet Protocol |
| IT | Information Technology |
| KCK | Key Confirmation Key |
| KEK | Key Encryption Key |
| LAN | Local Area Network |
| LDAP | Lightweight Directory Access Protocol |
| MAC | Media Access Control |
| Mbps | Megabits per second |
| MSK | Master Session Key |
| NIAP | National Information Assurance Partnership |
| NIC | Network Interface Card |
| NIST | National Institute of Standards and Technology |
| OCSP | Online Certificate Status Protocol |
| OS | Operating System |
| PKI | Public Key Infrastructure |
| PMK | Pairwise Master Keys |
| PP | Protection Profile |
| PSK | Pre-shared key |
| PSP | Public Security Parameter |
| PTK | Pair-wise Transient Key |

| Acronym | Definition |
|---|---|
| QoS | Quality of Service |
| RADIUS | Remote Authentication Dial-In User Service |
| RF | Radio Frequency |
| RFC | Request for Comments |
| RSA | Rivest, Shamir, and Adleman |
| RSTP | Rapid Spanning Tree Protocol |
| SAR | Security Assurance Requirement |
| SDRAM | Synchronous Dynamic Random Access Memory |
| SFP | Security Function Policy |
| SFR | Security Functional Requirement |
| SHA-1 | US Secure Hash Algorithm 1 |
| SNMP | Simple Network Management Protocol |
| SOF | Strength of Function |
| SP | Security Parameter |
| SSID | Session Set ID |
| ST | Security Target |
| TCP | Transmission Control Protocol |
| TK | Temporal Key |
| TLS | Transport Layer Security |
| TOE | Target of Evaluation |
| TSF | TOE Security Function |
| TSP | TOE Security Policy |
| TTLS | Tunneled Transport Layer Security |
| UDP | User Datagram Protocol |
| WAN | Wide Area Network |
| WAP | Wireless Access Point |
| Wi-Fi | Wireless fidelity |
| WLAN | Wireless Local Area Network |
| WMM | Wi-Fi Multimedia |
| WPA2 | Wi-Fi Protected Access Version 2 |

### 1.4.2 Terminology

The following terminology is used in the Security Target:

**Table 1-4: Terms**

| Term | Definition |
|---|---|
| 802.1X | The IEEE 802.1X standard provides a framework for many authentication types at the link layer. |
| EAP | Extensible Authentication Protocol (EAP). It is a protocol that supports the communication of other authentication protocols. EAP uses its own start and end message to carry third-party messages between supplicants and an authentication server. |
| EAP-TLS | EAP-TLS (RFC 5216) stands for Extensible Authentication Protocol-Transport Layers Security. Transport Layer Security (TLS) provides a mechanism to use certificates for mutual authentication, integrity-protected cipher-suite negotiation, and key exchange between two endpoints. |
| Wireless Client | A device consisting of hardware and software used to provide a wirelessly interface to communicate with other wireless devices as defined by IEEE 802.11 STA behavior. |

| Term | Definition |
|---|---|
| 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. |

### 1.4.3 TOE Description

The Target of Evaluation (TOE) is a system of wireless LAN Access Point products that includes 3e-525N, 3e-525N MP, 3e-525NV, 3e-523N and 3e-523NR Access Points (APs).

### 1.4.4 Wireless Access Point (AP) TOE Component

The 3eTI 3e-525N, 3e-525N MP, 3e-525NV, 3e-523N and 3e-523NR Access Points (hereafter referred to as Access Points or APs) provide the connection point between wireless client hosts and the wired network. Once installed as trusted nodes on the wired infrastructure, the APs provide the encryption service on the wireless network between themselves and the wireless clients. The APs can also communicate among themselves through the secured channel via 3eTI mesh forming or 802.11s mesh network. However this AP to AP secured communication service is not evaluated here.

The Access Points are appliances and this component of the TOE consists of hardware and firmware.

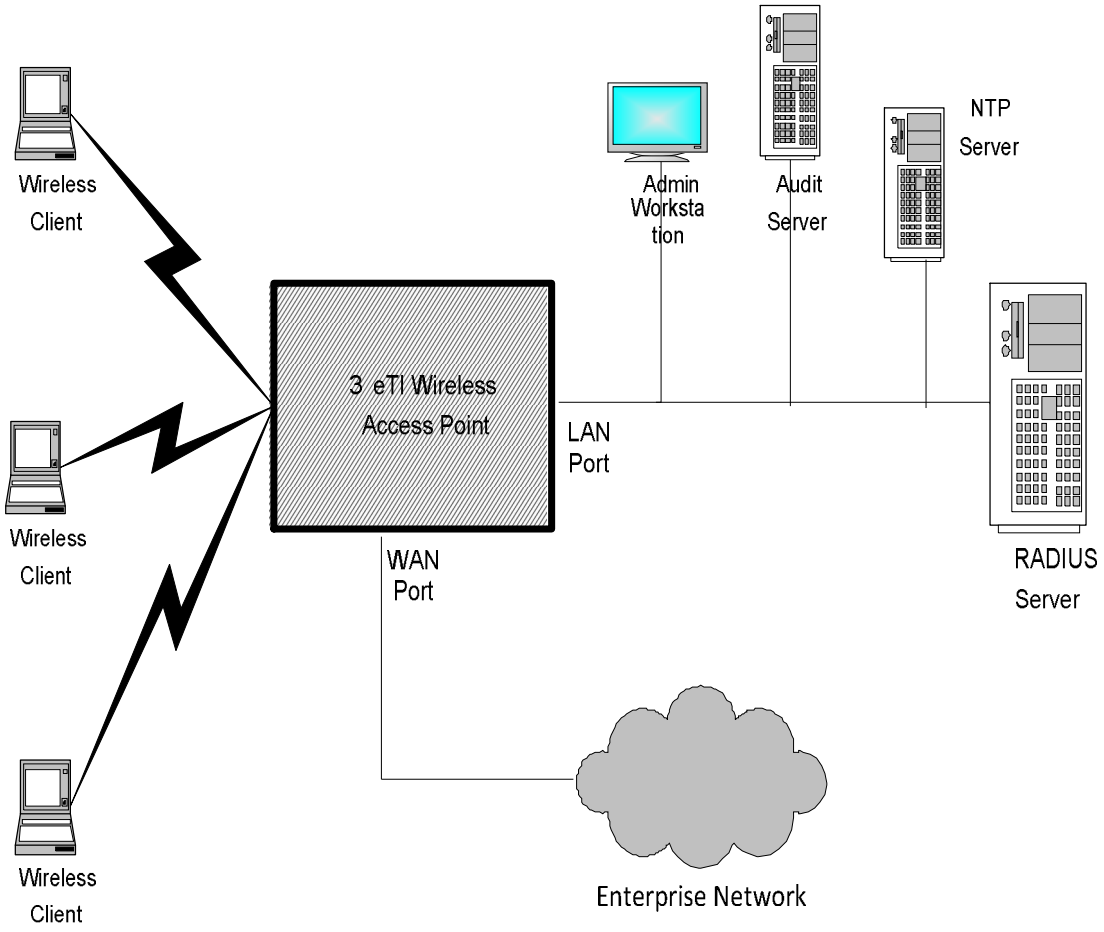
Wireless communications between clients and APs are carried out using the IEEE 802.11 protocol standard. The 802.11 standard governs communication transmission for wireless devices. For this evaluation, the APs use 802.11a, 802.11b, 802.11g and 802.11n for wireless communication. The wireless security protocol that is to be used with the APs is WPA2, which is the Wi-Fi Alliance interoperable specification based on IEEE 802.11i security standard.

The APs have one or more RF interfaces and one or more Ethernet interfaces. All these interfaces are controlled by the software executing on the APs. The Access Points included in the TOE vary by the number of RF and Ethernet interfaces and antenna support; however the differences do not affect the security functionality claimed by the TOE.

The APs maintain a security domain containing all hardware and software of the appliance for its own execution. The APs maintain this security domain by controlling the actions that can occur at the interfaces described above and providing the hardware resources that carry out the execution of tasks on the APs. The APs provide for isolation of different wireless clients that have sessions with the WLAN, which includes maintaining the keys necessary to support encrypted sessions with wireless devices.

The APs control the actions and the manner in which external users may interact with its external interfaces. Thus the APs ensure that the TOE's enforcement functions are invoked and succeed before allowing the external user to carry out any other security function with or through the APs. The figure below shows the TOE and its operational environment. The trusted path between TOE and Administration Station is TLS/HTTPS and the trusted path between TOE and NTP, Log Server and RADIUS server is IPsec.

**Figure 1-1: TOE Operational Environment**




Wireless Access Point Operational Enviroment

### 1.4.5 Product Guidance

**Table 1-5: Product Guidance**

| |
|---|
| 3e Technologies International, Inc., AirGuard™ Wireless Access Point 3e-520 Series User's Guide |
| |

### 1.4.6 Physical Scope of the TOE

The TOE physical boundary defines all hardware and software that is required to support the TOE's logical boundary and the TOE's security functions.

The TOE includes the following Access Points appliance models:

- 3e-525N Access Point; Hardware Version 1.0, firmware Version 5.1, build number 221

- 3e-525N MP Access Point; Hardware Version 1.0, firmware Version 5.1, build number 221
- 3e-525NV Access Point; Hardware Version 1.0, firmware Version 5.1, build number 221
- 3e-523N Access Point; Hardware version 1.0, firmware version 5.1, build number 221
- 3e-523NR Access Point; Hardware version 1.0, firmware version 5.1, build number 221

The TOE physical boundary defines all hardware and firmware that is required to support the TOE's logical boundary and the TOE's security functions. The TOE hardware platform uses FreeScale MPC8378E CPU and the TOE's firmware contains embedded Linux Kernel customized by 3eTI based on kernel version 3.6. In short, the TOE's physical boundary is the physical device/appliance for all models. The APs have the following physical interfaces.

- **AP antenna ports** – The AP antenna ports are connected to one 802.11a/b/g/n radio for wireless connectivity to secure WLAN clients.
- **LAN local port** – The LAN local port is used exclusively for management of the access point. It supports Ethernet 10/100/1000 Mbps wired traffic, full duplex for fast configuration and management. The LAN port is locally terminated – no data entering here goes out to the WLAN, only management data is accepted.
- **WAN uplink port** – The WAN uplink port is intended to connect the 3eTI access points to the wired LAN. It also supports Ethernet 10/100/1000 Mbps wired traffic in a full duplex configuration. The WAN port bridges all data between the wireless domain and the wired network.

### 1.4.7 Logical Scope of the TOE

The Logical Scope of the TOE includes Audit, Cryptographic Services, User Data Protection, Identification and Authentication, Management, Protection of the TSF, and TOE Access security functionality.

#### *1.4.7.1 Security Audit*

The TOE generates auditable events for actions on the TOE with the capability of selective audit record generation. The records of these events can be viewed within the TOE Management Interface or they can be exported to audit log servers in the Operational Environment. The TOE generates records for its own actions, containing information about the user/process associated with the event, the success or failure of the event, and the time that the event occurred. Additionally, all administrator actions relating to the management of TSF data and configuration data are logged by the TOE's audit generation functionality.

#### *1.4.7.2 Cryptographic Support*

The TOE uses a random number generator and secures communication channels with the following cryptographic algorithms: AES, RSA, ECDSA, SHA, and HMAC. The TOE also uses its designed mechanism to zeroize Critical Security Parameters (CSPs) to mitigate the possibility of disclosure or modification.

#### *1.4.7.3 User Data Protection*

The TOE protects user data, (i.e., only that data exchanged with wireless client devices), using the IEEE 801.11i standard wireless security protocol. The TOE mediates the flow of information passing to and from the WAN port and ensures that resources used to pass network packets through the TOE do not contain any residual information. The data between the TOE and management station is protected by HTTPS/TLS while data between TOE and RADIUS, NTP Server and Audit Log server is protected by IPsec.

#### *1.4.7.4 Identification and Authentication*

The TOE provides Identification and Authentication security functionality to ensure that all users are properly identified and authenticated before accessing TOE functionality. The TOE displays configurable access banner and enforces a local password-based authentication mechanism to perform administrative user authentication. Passwords are obscured when being displayed during any attempted login.

The wireless users are authenticated by the RADIUS server in the Operational Environment. EAP-TLS is used for WPA2 wireless authentication via x.509 certificates. The TOE sets up IPsec tunnel with RADIUS server and supports IKEv2 with x.509 certificates for IPsec endpoints mutual authentication.

#### *1.4.7.5 Security Management*

The Web Management Application of the TOE provides the capabilities for configuration and administration. The Web Management Application can be accessed via the dedicated LAN local Ethernet port configured for “out-of-band” management or through the WAN uplink Ethernet port. There is no local access such as a serial console port. Therefore, the local and remote management is considered the same for this evaluation.

An authorized administrator has the ability to modify, edit, and delete security parameters such as audit data, configuration data, and user authentication data. The Web Management Application also offers an authorized security administrator the capability to manage how security functions behave. For example a security administrator can enable/disable certain audit functions configurations and set encryption/decryption algorithms used for network packets.

#### *1.4.7.6 Protection of the TSF*

Internal testing of the TOE hardware, software, and software updates against tampering ensures that all security functions are running and available before the TOE accepting any communications. The TSF prevents reading of pre-shared keys, symmetric keys, private keys, and passwords. The TOE uses electronic signature verification before any firmware/software updates are installed.

The TOE runs a set of self-test on power-on to verify the correct operation of the TOE’s underlying hardware, TOE software and cryptographic modules. Additional cryptographic tests are performed during normal operation. The security of network data is maintained by ensuring no residual information is included in network packets.

The TOE has the capability to obtain reliable time from a remote Network Time Protocol (NTP) Server to provide reliable time stamps for audit services. Additionally, the administrator can manually set the time using the Web UI management interfaces.

#### *1.4.7.7 TOE Access*

The TOE provides the following TOE Access functionality:

- Configurable MAC address and/or IP address filtering with remote management session establishment
- TSF-initiated session termination when a connection is idle for a configurable time period
- Administrative termination of own session
- Configurable MAC address filtering for wireless client session establishment (either allow or deny the client access)
- TOE Access Banners

#### *1.4.7.8 Trusted Path/Channels*

The TOE protects interactive communication with administrators using TLS/HTTPS, both integrity and disclosure protection is ensured.

The TOE protects communication with wireless client via 802.11i-2007. IPsec tunnels are used by the TOE to setup trusted channel between TOE and NTP, RADIUS and Audit Log server.

#### *1.4.7.9 Resource Utilization*

The TOE can limit network connections in order to ensure that administrators will be able to connect when they need to perform security management operations on the TOE.

# 2 Conformance Claims

## *2.1 Common Criteria Conformance*

This ST claims conformance to Common Criteria for Information Technology Security Evaluation, Version 3.1 R4, September 2012. International Standard – ISO/IEC 15408:2000.

The requirements in this Security Target are Part 2 extended, and Part 3 conformant.

## *2.2 Protection Profile Claim*

This Security Target claims exact conformance to ***Protection Profile for Wireless Local Area Network (WLAN) Access Systems***, ***version 1.0, dated December 1, 2011***.

## *2.3 Conformance Rationale*

The TOE conforms to the Wireless Local Area Network (WLAN) Access System Protection Profile, Version 1.0, dated December 1, 2011. This Protection Profile is called WLANAS PP for convenience through this Security Target.

This security target claims strict conformance to only one Protection Profile [PP] – WLANAS PP.

The security problem definition of this ST is consistent with the statement of the security problem definition in the PP, as the ST claims *exact* conformance to the PP and no other threats, organizational security policies, or assumptions are added.

The security objectives of this ST are consistent with the statement of the security objectives in the PP as the ST claims *exact* conformance to the PP and no other security objectives are added.

The security requirements of this ST are consistent with the statement of the security requirements in the PP as the ST claims *exact* conformance to the PP.

The ST document incorporates the following Technical Decision (TD) concerning WLAN PP as listed in the table below

**Table 2-1: Technical Decisions ST Used**

| # | TD Name | TD Details |
|---|---|---|
| 1 | TD0002 | Use NDPPv1.1 FIA_PMG_EXT.1 requirement within the WLAS AS PP v1.0 |
| 2 | TD0010 | The administrator identity attribute is excluded from the list of attributes. |
| 3 | TD0020 | Update of Requirements for IKE Authentication |
| 4 | TD0021 | Update to Limits on SA Lifetimes for IKE v1 and IKE v2 |
| 5 | TD0027 | Removal of FPT_RPL.1 in WLAN AS PP |
| 6 | TD0036 | Removal of Low-level Crypto Failure Audit in WLAN AS PP |
| 7 | TD0042 | Removal of Low-level Crypto Failure Audit from PPs |

# 3 Security Problem Definition

This document identifies threats are identified as T.threat with “threat” specifying a unique name. Policies are identified as P.policy with “policy” specifying a unique name. Assumptions are identified as A.assumption with “assumption” specifying a unique name.

## *3.1 Threats to Security*

The following subsections define the security threats for the TOE, characterized by a threat agent, an asset, and an adverse action of that threat agent on that asset. These threats are taken directly from the PP unchanged.

**Table 3-1: Threats to Security**

| # | Threat Name | Threat Definition |
|---|---|---|
| 1 | T.ADMIN_ERROR | An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms. |
| 2 | T.RESOURCE_EXHAUSTION | A process or user may deny access to TOE services by exhausting critical resources on the TOE. |
| 3 | T.TSF_FAILURE | Security mechanisms of the TOE may fail, leading to a compromise of the TSF. |
| 4 | T.UNAUTHORIZED_ACCESS | A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data. |
| 5 | T.UNAUTHORIZED_UPDATE | A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE. |
| 6 | T.UNDETECTED_ACTIONS | Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated. |
| 7 | T.USER_DATA_REUSE | User data may be inadvertently sent to a destination not intended by the original sender. |

## *3.2 Organization Security Policies*

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. Table 3-2 below lists the Organizational Security Policies enforced by the TOE.

**Table 3-2: Organizational Security Policies**

| # | Policy Name | Policy Definition |
|---|---|---|
| 1 | P.ACCESS_BANNER | The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE. |

| # | Policy Name | Policy Definition |
|---|---|---|
| 2 | P.ACCOUNTABILITY | The authorized users of the TOE shall be held accountable for their actions within the TOE. |
| 3 | P.ADMIN_ACCESS | Administrators shall be able to administer the TOE both locally and remotely through protected communications channels. |
| 4 | P.COMPATIBILITY | The TOE must meet Request for Comments (RFC) requirements for implemented protocols to facilitate inter-operation with other network equipment (e.g., certificate authority, NTP server) using the same protocols. |
| 5 | P.EXTERNAL_SERVERS | The TOE must support standardized (RFCs) protocols for communication with a centralized audit server and a RADIUS authentication server. |

### *3.3 Secure Usage Assumptions*

Table 3-3 below lists the secure usage assumptions.

**Table 3-3: Secure Usage Assumptions**

| # | Assumption Name | Assumption Definition |
|---|---|---|
| 1 | A.NO_GENERAL_PURPOSE | It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available to the TOE, other than those services necessary for the operation, administration and support of the TOE. |
| 2 | A.NO_TOE_BYPASS | Information cannot flow between the wireless client and the internal wired network without passing through the TOE. |
| 3 | A.PHYSICAL | Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment. |
| 4 | A.TRUSTED_ADMIN | TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner. |

# 4 Security Objectives

This section defines TOE security objectives and objectives for the Operational Environment.

## *4.1 Security Objectives for the TOE*

Table 4-1 below lists the Security Objectives for the TOE.

**Table 4-1: Security Objectives**

| | TOE Security Objective | TOE Security Objective Definition |
|---|---|---|
| 1 | O.AUTH_COMM | The TOE will provide a means to ensure users are not communicating with some other entity pretending to be the TOE, and that the TOE is communicating with an authorized IT entity and not some other entity pretending to be an authorized IT entity. |
| 2 | O.CRYPTOGRAPHIC_FUNCTIONS | The TOE shall provide cryptographic functions (i.e., encryption/decryption and digital signature operations) to maintain the confidentiality and allow for detection of modification of TSF data that is transmitted between physically separated portions of the TOE, or stored outside the TOE. |
| 3 | O.DISPLAY_BANNER | The TOE will display an advisory warning regarding use of the TOE. |
| 4 | O.FAIL_SECURE | The TOE shall fail in a secure manner following failure of the power-on self -tests. |
| 5 | O.PROTECTED_COMMUNICATIONS | The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities. |
| 6 | O.PROTOCOLS | The TOE will ensure that standardized protocols are implemented in the TOE to RFC and/or Industry specifications to ensure interoperability, that also support communication with a centralized audit server and a RADIUS authentication server. |
| 8 | O.RESIDUAL_INFORMATION_CLEARING | The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated. |
| 9 | O.RESOURCE_AVAILABILITY | The TOE shall provide mechanisms that mitigate user attempts to exhaust TOE resources (e.g., persistent storage). |
| 10 | O.ROBUST_TOE_ACCESS | The TOE will provide mechanisms that control an administrator's logical access to the TOE and to control administrative access from a wireless client. |
| 11 | O.SESSION_LOCK | The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked. |
| 12 | O.SYSTEM_MONITORING | The TOE will provide the capability to generate audit data and send those data to an external IT entity. |

| | | |
|---|---|---|
| 13 | O.TIME_STAMPS | The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these timestamps. |
| 14 | O.TOE_ADMINISTRATION | The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators. |
| 15 | O.TSF_SELF_TEST | The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly. |
| 16 | O.VERIFIABLE_UPDATES | The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source. |
| 17 | O.WIRELESS_CLIENT_ACCESS | The TOE will provide the capability to restrict a wireless client in connecting to the TOE. |

### *4.2 Security Objectives for the Operational Environment*

Table 4-2 below lists the Security Objectives for the Operational Environment.

**Table 4-2: Security Objectives for the Operational Environment**

| # | TOE Security Objective | TOE Security Objective Definition |
|---|---|---|
| 1 | OE.NO_GENERAL_PURPOSE | There are no general-purpose computing capabilities (e.g., compilers or user applications) available to the TOE, other than those services necessary for the operation, administration and support of the TOE. |
| 2 | OE.NO_TOE_BYPASS | Information cannot flow between external and internal networks located in different enclaves without passing through the TOE. |
| 3 | OE.PHYSICAL | Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment. |
| 4 | OE.TRUSTED_ADMIN | TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner. |

# 5 Extended Components Definition

This section provides definition of the extended security functional and assurance requirements; the components that are CC Part 2 extended (if present), and CC Part 3 extended (if present), i.e., NIAP interpreted requirements, and extended requirements.

## *5.1 Extended Security Function Requirements Definitions*

All SFRs listed as extended in this ST are taken directly from the claimed protection profile. There are no additional extended Security Functional Requirements defined in this Security Target.

## *5.2 Extended Security Assurance Requirement Definitions*

There are no extended Security Assurance Requirements defined in this Security Target.

# 6 Security Requirements

The following conventions have been applied in this document:

- **Security Functional Requirements:** Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
- **Extended Security Functional Requirements**: Extended requirements were written by the PP author when Part 2 of the CC did not offer suitable requirements to meet the authors' needs. Extended requirements will be indicated with the "_EXT" inserted within the component name (e.g., FAU_STG_EXT.1)
- **Iteration**: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a reference in parenthesis placed at the end of the component. For example FCS_COP.1 (1) and FCS_COP.1 (2) indicate that the ST includes two iterations of the FCS_COP.1 requirement, (1) and (2).
- **ST Author Assignment**: allows the specification of an identified parameter. Assignments made by the ST author are indicated using bold text and are surrounded by brackets (e.g., [**assignment**]).
- **ST Author Selection**: allows the specification of one or more elements from a list. Selections made by the ST author are indicated using bold text and are surrounded by brackets (e.g., [**selection**]).
- **ST Author Refinement**: The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements made by the ST author is denoted by the italicized and bold text. (e.g. ***refinement*** )
- **PP Author Selections, Assignments, & Refinements:** PP author selections and assignments are shown in normal text. Refinements made by the PP authors will not be identified as refinements in this ST. The "Refinement" identifier is reserved for identifying any refinements made by the ST author.

## *6.1 TOE Security Functional Requirements*

The following table describes the SFRs that are satisfied by 3eTI's WLAN APs.

**Table 6-1: 3e-525N & 3e-523N Security Functional Requirements**

| Functional Class | Functional Components | | # |
|---|---|---|---|
| Security Audit (FAU) | FAU_GEN.1 | Audit Data Generation | 1 |
| | FAU_GEN.2 | User Audit Association | 2 |
| | FAU_SEL.1 | Selective Audit | 3 |
| | FAU_STG.1 | Protected Audit Trail Storage (Local Storage) | 4 |
| | FAU_STG_EXT.1 | Extended: External Audit Trail Storage | 5 |
| | FAU_STG_EXT.3 | Extended: Action in Case of Loss of Audit Server Connectivity | 6 |

| Functional Class | Functional Components | | # |
|---|---|---|---|
| | FAU_STG_EXT.4 | Extended: Prevention of Audit Data Loss | 7 |
| | FAU_SAR.1 | Audit Review | 8 |
| | FAU_SAR.2 | Restricted Audit Review | 9 |
| Cryptographic Support (FCS) | FCS_CKM.1 (1) | Cryptographic Key Generation (Symmetric Keys for WPA2 Connections) | 10 |
| | FCS_CKM.1 (2) | Cryptographic Key Generation (Asymmetric Keys) | 11 |
| | FCS_CKM.2 (1) | Cryptographic Key Distribution (PMK) | 12 |
| | FCS_CKM.2 (2) | Cryptographic Key Distribution (GTK) | 13 |
| | FCS_CKM_EXT.4 | Extended: Cryptographic Key Zeroization | 14 |
| | FCS_COP.1 (1) | Cryptographic Operation (Data Encryption/Decryption) | 15 |
| | FCS_COP.1 (2) | Cryptographic Operation (Cryptographic Signature) | 16 |
| | FCS_COP.1 (3) | Cryptographic Operation (Cryptographic Hashing) | 17 |
| | FCS_COP.1 (4) | Cryptographic Operation (Keyed-Hash Message Authentication) | 18 |
| | FCS_COP.1 (5) | Cryptographic Operation (WPA2 Data Encryption/Decryption) | 19 |
| | FCS_IPSEC_EXT.1 | Extended: Internet Protocol Security (IPsec) Communications | 20 |
| | FCS_RBG_EXT.1 | Extended: Cryptographic Operation (Random Bit Generation) | 21 |
| | FCS_HTTPS_EXT.1 | Extended: HTTP Security (HTTPS) | 22 |
| | FCS_TLS_EXT.1 | Extended: Transport Layer Security (TLS) | 23 |
| User Data Protection (FDP) | FDP_RIP.2 | Full Residual Information Protection | 24 |
| Identification and Authentication (FIA) | FIA_AFL.1 | Authentication Failure Handling | 25 |
| | FIA_PMG_EXT.1 | Extended: Password Management | 26 |
| | FIA_UIA_EXT.1 | Extended: User Identification and Authentication | 27 |
| | FIA_UAU_EXT.5 | Extended: Password-based Authentication Mechanism | 28 |
| | FIA_UAU.6 | Re-authenticating | 29 |
| | FIA_UAU.7 | Protected Authentication Feedback | 30 |
| | FIA_8021X_EXT.1 | Extended: 802.1X Port Access Entity (Authenticator) Authentication | 31 |
| | FIA_PSK_EXT.1 | Extended: Pre-Shared Key Composition | 32 |

| Functional Class | Functional Components | | # |
|---|---|---|---|
| | FIA_X509_EXT.1 | Extended: X509 Certificates | 33 |
| Security Management (FMT) | FMT_MOF.1 | Management of Security Functions Behavior | 34 |
| | FMT_MTD.1 (1) | Management of TSF Data (General TSF Data) | 35 |
| | FMT_MTD.1 (2) | Management of TSF Data (Reading of Authentication Data) | 36 |
| | FMT_MTD.1 (3) | Management of TSF Data (for reading of all symmetric keys) | 37 |
| | FMT_SMF.1 | Specification of Management Functions | 38 |
| | FMT_SMR.1 | Security Management Roles | 39 |
| Protection of TSF (FPT) | FPT_FLS.1 | Fail Secure | 40 |
| | FPT_STM.1 | Reliable Time Stamp | 41 |
| | FPT_TST_EXT.1 | Extended: TSF Testing | 42 |
| | FPT_TUD_EXT.1 | Extended: Trusted Update | 43 |
| Resource Utilization (FRU) | FRU_RSA.1 | Maximum Quotas | 44 |
| TOE Access (FTA) | FTA_SSL_EXT.1 | Extended: TSF-initiated session locking | 45 |
| | FTA_SSL.3 | TSF-initiated termination | 46 |
| | FTA_SSL.4 | User-initiated termination | 47 |
| | FTA_TAB.1 | Default TOE Access Banners | 48 |
| | FTA_TSE.1 | TOE Session Establishment | 49 |
| Trusted Path/Channels (FTP) | FTP_ITC.1 | Inter-TSF trusted channel | 50 |
| | FTP_TRP.1 | Trusted Path | 51 |

### 6.1.1 Security Audit (FAU) Requirements

#### *6.1.1.1 FAU_GEN.1 Audit Data Generation*

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and

c) All administrative actions;

d) Specifically defined auditable events listed in ***Table 6-2***.

**Table 6-2: Auditable Events**

| # | Requirement | Auditable Events | Additional Audit Record Contents |
|---|---|---|---|
| 1 | FAU_GEN.1 | None | |
| 2 | FAU_GEN.2 | None | |

| # | Requirement | Auditable Events | Additional Audit Record Contents |
|---|---|---|---|
| 3 | FAU_SEL.1 | All modifications to the audit configuration that occur while the audit collection functions are operating. | **None** |
| 4 | FAU_STG.1 | None | |
| 5 | FAU_STG_EXT.1 | None | |
| 6 | FAU_STG_EXT.3 | Loss of connectivity. | **None** |
| 7 | FAU_STG_EXT.4 | None | |
| 8 | FAU_SAR.1 | None | |
| 9 | FAU_SAR.2 | None | |
| 10 | FCS_CKM.1 (1) | Failure of the key generation activity for authentication keys. | **No additional information** |
| 11 | FCS_CKM.1 (2,3) | Failure of the key generation activity for authentication keys. | **No additional information** |
| 12 | FCS_CKM.2 (1) | Failure of the key distribution activity. | **None** |
| 13 | FCS_CKM.2 (2) | Failure of the key distribution activity, including failures related to wrapping the GTK. | **Identifier(s) for intended recipients of wrapped key.** |
| 14 | FCS_CKM_EXT.4 | None | **None** |
| 15 | FCS_COP.1 (1) | None | **None** |
| 16 | FCS_COP.1 (2) | None | **None** |
| 17 | FCS_COP.1 (3) | None | **None** |
| 18 | FCS_COP.1 (4) | None | **None** |
| 19 | FCS_COP.1 (5) | None | **None** |
| 20 | FCS_IPSEC_EXT.1 | Protocol failures.<br>Establishment/Termination of an IPsec SA.<br>Negotiation “down” from an IKEv2 to IKEv1 exchange. | **Reason for failure.**<br>**Non-TOE endpoint of connection (IP address) for both successes and failures.** |
| 21 | FCS_RBG_EXT.1 | Failure of the randomization process | **No additional information** |
| 22 | FCS_HTTPS_EXT.1 | Protocol failures<br>Establishment/Termination of a HTTPS session. | **Reason for failure.**<br>**Non-TOE endpoint of connection (IP address) for both successes and failures.** |
| 23 | FCS_TLS_EXT.1 | Protocol failures.<br>Establishment/Termination of a TLS session. | **Reason for failure.**<br>**Non-TOE endpoint of connection (IP address) for both successes and failures.** |
| 24 | FDP_RIP.2 | None | |
| 25 | FIA_AFL.1 | The reaching of the threshold for the unsuccessful authentication attempts and the actions taken (e.g., disabling of an account) and the subsequent, if appropriate, restoration to the normal state (e.g., re-enabling of a terminal). | |
| 26 | FIA_PMG_EXT.1 | None | |

| # | Requirement | Auditable Events | Additional Audit Record Contents |
|---|---|---|---|
| 27 | FIA_UIA_EXT.1 | All use of the identification and authentication mechanism | **Provided user identity, origin of the attempt (e.g., IP address)** |
| 28 | FIA_UAU_EXT.5 | All use of the authentication mechanism. | **Origin of the attempt (e.g., IP address)** |
| 29 | FIA_UAU.6 | Attempts to re-authenticate. | **Origin of the attempt (e.g., IP address).** |
| 30 | FIA_UAU.7 | None | |
| 31 | FIA_8021X_EXT.1 | Attempts to access to the 802.1X controlled port. | **Provided client identity (IP address).** |
| 32 | FIA_PSK_EXT.1 | None | |
| 33 | FIA_X509_EXT.1 | Attempts to load certificates.<br>Attempts to revoke certificates. | **None** |
| 34 | FMT_MOF.1 | None | |
| 35 | FMT_MTD.1 (1) | None | |
| 36 | FMT_MTD.1 (2) | None | |
| 37 | FMT_MTD.1 (3) | None | |
| 38 | FMT_SMF.1 | None | |
| 39 | FMT_SMR.1 | None | |
| 40 | FPT_FLS.1 | Failure of the TSF. | **Indication that the TSF has failed with the type of failure that occurred.** |
| 41 | FPT_STM.1 | Changes to the time | **The old and new values for the time. Origin of the attempt (e.g., IP address).** |
| 42 | FPT_TST_EXT.1 | Execution of this set of TSF self-tests.<br>Detected integrity violations. | **For integrity violations, the TSF code file that caused the integrity violation.** |
| 43 | FPT_TUD_EXT.1 | Initiation of the update.<br>Any failure to verify the integrity of the update. | **No additional information** |
| 44 | FRU_RSA.1 | Maximum quota being exceeded. | **Resource identifier.** |
| 45 | FTA_SSL_EXT.1 | Locking of an interactive session by the session locking mechanism.<br>Any attempts at unlocking of an interactive session. | **None** |
| 46 | FTA_SSL.3 | The termination of a remote session by the session locking mechanism. | **None** |
| 47 | FTA_SSL.4 | Terminating a session by quitting or logging off. | **None** |
| 48 | FTA_TAB.1 | None | |

| # | Requirement | Auditable Events | Additional Audit Record Contents |
|---|---|---|---|
| 49 | FTA_TSE.1 | Denial of a session establishment due to the session establishment mechanism. | **Reason for denial, origin of establishment attempt.** |
| 50 | FTP_TRP.1 | All Attempts to establish a remote administrative session. Detection of modification of session data. | **Identification of the initiating IT entity (e.g., IP address).** |
| 51 | FTP_ITC.1 | All attempts to establish a trusted channel.<br>Detection of modification of channel data. | **Identification of the initiator and target of channel.** |

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, information specified in column three of the ***Table 6-2***.

#### *6.1.1.2 FAU_GEN.2 User Audit Association*

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

#### *6.1.1.3 FAU_SEL.1 Selective Audit*

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

a) event type;
b) success of auditable security events;
c) failure of auditable security events; and
d) [**None**].

#### *6.1.1.4 FAU_STG.1 Protected Audit Trail Storage (Local Storage)*

FAU_STG.1.1 The TSF shall protect [**256KB**] locally stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorized modifications to the stored audit records in the audit trail.

#### *6.1.1.5 FAU_STG_EXT.1 Extended: External Audit Trail Storage*

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel implementing the [**IPsec**] protocol.

#### *6.1.1.6 FAU_STG_EXT.3 Extended: Action in Case of Loss of Audit Server Connectivity*

FAU_STG_EXT.3.1 The TSF shall [**log audit server communication error and attempts to reestablish the secure channel**] if the link to the external IT entity collecting the audit data generated by the TOE is not available.

#### *6.1.1.7 FAU_STG_EXT.4 Extended: Prevention of Audit Data Loss*

FAU_STG_EXT.4.1 The TSF shall provide the Authorized Administrator the capability to select one or more of the following actions:

a) prevent auditable events, except those taken by the Authorized Administrator, and
b) overwrite the oldest stored audit records to be taken if the audit trail is full.

#### *6.1.1.8 FAU_SAR.1 Audit Review*

FAU_SAR.1.1 The TSF shall provide Authorized Administrators with the capability to read all audit data from the audit records.

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

#### *6.1.1.9 FAU_SAR.2 Restricted Audit Review*

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records in the audit trail, except Authorized Administrators.

### 6.1.2 Cryptographic Support (FCS) Requirements

#### *6.1.2.1 FCS_CKM.1 (1) Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)*

FCS_CKM.1.1 (1) The TSF shall derive symmetric cryptographic keys in accordance with a specified cryptographic key derivation algorithm PRF-384 with specified cryptographic key size 128 bits using a Random Bit Generator as specified in FCS_RBG_EXT.1 and that meet the following: 802.11-2007.

#### *6.1.2.2 FCS_CKM.1(2) Cryptographic Key Generation (Asymmetric Keys)*

FCS_CKM.1.1(2) The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with [

- **NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and** [**P-521**] **(as defined in FIPS PUB 186-3, "Digital Signature Standard")**

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

#### *6.1.2.3 FCS_CKM.1(3) Cryptographic Key Generation (Asymmetric Keys)*

FCS_CKM.1.1(3) The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with [

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

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

#### *6.1.2.4 FCS_CKM.2 (1) Cryptographic Key Distribution (PMK)*

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

#### *6.1.2.5 FCS_CKM.2 (2) Cryptographic Key Distribution (GTK)*

FCS_CKM.2.1 (2) The TSF shall distribute Group Temporal Key in accordance with a specified cryptographic key distribution method: AES Key Wrap in an EAPOL-Key frame that meets the following: RFC 3394 for AES Key Wrap, 802.11-2007 for the packet format and timing considerations and does not expose the cryptographic keys.

#### *6.1.2.6 FCS_CKM_EXT.4 Extended: Cryptographic Key Zeroization*

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

#### *6.1.2.7 FCS_COP.1 (1) Cryptographic Operation (Data Encryption/Decryption)*

FCS_COP.1.1 (1) The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm AES operating in [**CCM, CBC, ECB and GCM**] and cryptographic key sizes 128-bits, 256-bits, and [**192 bits**] that meets the following:

- FIPS PUB 197, "Advanced Encryption Standard (AES)"
- **[NIST SP 800-38A, NIST SP 800-38C, NIST SP 800-38D].**

#### *6.1.2.8 FCS_COP.1 (2) Cryptographic Operation (Cryptographic Signature)*

FCS_COP.1.1 (1) (2) The TSF shall perform cryptographic signature services in accordance with a

[

- **RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater**

]

that meets the following:

**Case**: **RSA Digital Signature Algorithm**

- **FIPS PUB 186-3, "Digital Signature Standard"**

FCS_COP.1.1(2) (2) The TSF shall perform cryptographic signature services in accordance with a

[

- **Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater**

]

that meets the following:

**Case: Elliptic Curve Digital Signature Algorithm**

- **FIPS PUB 186-3, "Digital Signature Standard"**
- **The TSF shall implement "NIST curves" P-256, P-384 and [P-521] (as defined in FIPS PUB 186-3, "Digital Signature Standard").**

#### *6.1.2.9 FCS_COP.1 (3) Cryptographic Operation (Cryptographic Hashing)*

FCS_COP.1.1 (3) The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [**SHA-1, SHA-256, SHA-384**] and message digest sizes [**160, 256, 384**] bits that meet the following: FIPS PUB 180-4, "Secure Hash Standard".

#### *6.1.2.10 FCS_COP.1 (4) Cryptographic Operation (Keyed-Hash Message Authentication)*

FCS_COP.1.1 (4) The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC- [**SHA-1, SHA-256, SHA-384**], key size [**160, 256, 384 bits**], and message digest size of [**160, 256, 384**] bits that meet the following: FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code", and FIPS PUB 180-4, "Secure Hash Standard".

***Application Note:*** *The PP calls out for FIPS PUB 180-3. Since the time of the approved PP FIPS PUB 180-4 has been approved and supersedes 180-3. Therefore, the vendor is claiming the latest standard.*

### *6.1.2.11 FCS_COP.1 (5) Cryptographic Operation (WPA2 Data Encryption/Decryption)*

FCS_COP.1.1 (5) The TSF shall perform encryption and decryption in accordance with the specified cryptographic algorithm AES CCMP and cryptographic key size of 128 bits that meet the following: FIPS PUB 197, NIST SP 800-38C and IEEE 802.11-2007.

### *6.1.2.12 FCS_IPSEC_EXT.1 Extended: Internet Protocol Security (IPsec) Communications*

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602), [**AES-GCM-128, AES-GCM-256 as specified in RFC 4106**], and using [**IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23), 4307, and [RFC 4868 for hash functions**]] for connections to the Authentication Server and [**NTP Server, Audit Log Server**].

FCS_IPSEC_EXT.1.2 The TSF shall ensure that only ESP confidentiality and integrity security service is used.

FCS_IPSEC_EXT.1.3 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.4 The TSF shall ensure that [**IKEv2 SA lifetimes can be configured by an administrator based on number of packets or length of time**].

FCS_IPSEC_EXT.1.5 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in gx mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least **[224, 256, 384, 512]** bits.

FCS_IPSEC_EXT.1.6 The TSF shall generate nonces used in IKE exchanges in a manner such that the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^[**112, 128, 192, 256**].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP) and [**19 (256-bit Random ECP), 20 (384-bit Random ECP)**, [**21 (512-bit Random ECP**)]].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that all IKE protocols implement peer authentication using [**RSA, ECDSA**] that use X.509v3 certificates that conform to RFC 4945 and [**Pre-shared Keys**].

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

### *6.1.2.13 FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)*

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [**NIST Special Publication 800-90 using [CTR_DRBG (AES)]** ]seeded by an entropy source that accumulates entropy from at least one independent TSF-hardware-based noise sources.

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [**256 bits**] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

#### *6.1.2.14 FCS_HTTPS_EXT.1 Extended: HTTP Security (HTTPS)*

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

#### *6.1.2.15 FCS_TLS_EXT.1 Extended: Transport Layer Security (TLS)*

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [**TLS 1.0 (RFC 2346), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)**] supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Optional Ciphersuites:

[

**TLS_RSA_WITH_AES_128_CBC_SHA256**
**TLS_RSA_WITH_AES_256_CBC_SHA256**
**TLS_DHE_RSA_WITH_AES_128_CBC_SHA256**
**TLS_DHE_RSA_WITH_AES_256_CBC_SHA256**
].

### 6.1.3 User Data Protection (FDP) Requirements

#### *6.1.3.1 FDP_RIP.2 Full Residual Information Protection*

FDP_RIP.2.1 The TSF shall enforce that any previous information content of a resource is made unavailable upon the [**allocation of the resource to**] all objects.

### 6.1.4 Identification and Authentication (FIA) Requirements

#### *6.1.4.1 FIA_AFL.1 Authentication Failure Handling*

FIA_AFL.1.1 The TSF shall detect when an Authorized Administrator configurable positive integer of successive unsuccessful authentication attempts occur related to administrators attempting to authenticate remotely.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [**prevent the offending remote administrator from successfully authenticating until an Authorized Administrator defined time period has elapsed**].

#### *6.1.4.2 FIA_PMG_EXT.1 Extended: Password Management*

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

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: **[“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [ “+”, “-“]**];
2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater;

*Note: This SFR is from NDPPv1.1. per Technical Decision TD0002, “Until a time that the WLAS AS PP v1.0 is updated to align with the NDPP v1.1, the FIA_PMG_EXT.1 requirement and assurance activities from NDPP v1.1 can be used to satisfy the FIA_PMG_EXT.1 requirement within the WLAS AS PP v1.0.”*

#### *6.1.4.3 FIA_UIA_EXT.1 Extended: User Identification and Authentication*

FIA_UIA_EXT.1.1 The TSF shall allow responses to the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [**ICMP Echo**]

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

#### *6.1.4.4 FIA_UAU_EXT.5 Extended: Password-based Authentication Mechanism*

FIA_UAU_EXT.5.1 The TSF shall provide a local password-based authentication mechanism, [**none**] to perform administrative user authentication.

FIA_UAU_EXT.5.2 The TSF shall ensure that administrative users with expired passwords are **[forced to change password at next login**].

#### *6.1.4.5 FIA_UAU.6 Re-authenticating*

FIA_UAU.6.1 The TSF shall re-authenticate the administrative user under the conditions: when the user changes their password, [**following TSF-initiated locking (FTA_SSL)**].

#### *6.1.4.6 FIA_UAU.7 Protected Authentication Feedback*

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

#### *6.1.4.7 FIA_8021X_EXT.1 Extended: 802.1X Port Access Entity (Authenticator) Authentication*

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

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

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

#### *6.1.4.8 FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition*

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec and [**no other protocols**].

FIA_PSK_EXT.1.2.(1) The TSF shall be able to accept text-based pre-shared keys for IPsec that:

- are 22 characters and [**16 to 32 characters**];
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using [**SHA-1, SHA-256, [SHA-384]**].

FIA_PSK_EXT.1.4 The TSF shall be able to [**accept**] bit-based pre-shared keys.

#### *6.1.4.9 FIA_X509_EXT.1 Extended: X509 Certificates*

FIA_X509_EXT.1.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec and [**TLS**] connections.

FIA_X509_EXT.1.2 The TSF shall store and protect certificate(s) from unauthorized deletion and modification.

FIA_X509_EXT.1.3 The TSF shall provide the capability for Authorized Administrators to load X.509v3 certificates into the TOE for use by the security functions specified in this ST.

## 6.1.5 Security Management (FMT) Requirements

### *6.1.5.1 FMT_MOF.1 Management of Security Functions Behavior*

FMT_MOF.1.1 The TSF shall restrict the ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE identified in this ST to the Authorized Administrator.

### *6.1.5.2 FMT_MTD.1 (1) Management of TSF Data (General TSF Data)*

FMT_MTD.1.1 (1) The TSF shall restrict the ability to manage the TSF data to the Authorized Administrators.

### *6.1.5.3 FMT_MTD.1 (2) Management of TSF Data (Reading of Authentication Data)*

FMT_MTD.1.1 (2) The TSF shall prevent reading of the password-based authentication data.

### *6.1.5.4 FMT_MTD.1 (3) Management of TSF Data (for reading of all symmetric keys)*

FMT_MTD.1.1 (3) The TSF shall prevent reading of all pre-shared keys, symmetric key, and private keys.

### *6.1.5.5 FMT_SMF.1 Specification of Management Functions*

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

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

### *6.1.5.6 FMT_SMR.1 Security Management Roles*

FMT_SMR.1.1 The TSF shall maintain the roles:

- Authorized Administrator;
- No other roles

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

FMT_SMR.1.3 The TSF shall ensure that the conditions:

- Authorized Administrator role shall be able to administer the TOE locally;
- Authorized Administrator role shall be able to administer the TOE remotely;
- The ability to remotely administer the TOE remotely from a wireless client shall be disabled by default;

are satisfied.

### 6.1.6 Protection of TSF (FPT) Requirements

#### *6.1.6.1 FPT_FLS.1 Fail Secure*

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

#### *6.1.6.2 FPT_STM.1 Reliable Time Stamp*

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

#### *6.1.6.3 FPT_TST_EXT.1 Extended: TSF Testing*

FPT_TST_EXT.1.1 The TSF shall run a suite of self tests during the initial start-up (on power on) to demonstrate the correct operation of the TSF.

#### *6.1.6.4 FPT_TUD_EXT.1 Extended: Trusted Update*

FPT_TUD_EXT.1.1 The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [**no other functions**] prior to installing those updates.

### 6.1.7 Resource Utilization (FRU)

#### *6.1.7.1 FRU_RSA.1 Maximum Quotas*

FRU_RSA.1.1 (1) The TSF shall enforce maximum quotas of the following resources: [**connections to the TOE by wireless clients limited to 64**], [**no other resources**] that [**defined group of users**] can use [**simultaneously**].

FRU_RSA.1.1 (2)1 The TSF shall enforce maximum quotas of the following resources: [**administrative sessions limited to 1**], [**no other resources**] that [**defined group of users**] can use [**simultaneously**].

### 6.1.8 TOE Access (FTA) Requirements

#### *6.1.8.1 FTA_SSL_EXT.1 Extended: TSF-initiated session locking*

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [**terminate the session**] after an Authorized Administrator specified time period of inactivity.

#### *6.1.8.2 FTA_SSL.3 TSF-initiated termination*

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

#### *6.1.8.3 FTA_SSL.4 User-initiated termination*

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

#### *6.1.8.4 FTA_TAB.1 Default TOE Access Banners*

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

#### *6.1.8.5 FTA_TSE.1 TOE Session Establishment*

FTA_TSE.1.1 The TSF shall be able to deny establishment of a wireless client session based on location, time, day, [***none***].

### 6.1.9 Trusted Path/Channels (FTP) Requirements

#### *6.1.9.1 FTP_ITC.1 Inter-TSF trusted channel*

FTP_ITC.1.1 The TSF shall use 802.11-2007, IPsec, and [**no other protocols**] to provide a trusted communication channel between itself and all authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit the TSF, or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**IPsec tunnel to RADIUS server, NTP server and Audit Log Server**].

#### *6.1.9.2 FTP_TRP.1 Trusted Path*

FTP_TRP.1.1 The TSF shall use [**TLS/HTTPS**] provide a trusted communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and detection of modification of the communicated data.

FTP_TRP.1.2 The TSF shall permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial administrator authentication and all remote administration actions.

### *6.2 TOE Security Assurance Requirements*

The security assurance requirements for the TOE are specified in Part 3 of the Common Criteria (with the exception of some name changes in accordance with the NDPP). Table 6-3 lists the assurance components.

**Table 6-3: TOE Security Assurance Requirements**

| Assurance Class | Assurance Components |
|---|---|
| Development (ADV) | ADV_FSP.1 Basic Functional Specification |
| Guidance Documents (AGD) | AGD_OPE.1 Operational User Guidance |
| | AGD_PRE.1 Preparative Procedures |
| Life-cycle Support (ALC) | ALC_CMS.1 TOE CM coverage |
| | ALC_CMC.1 Labeling of the TOE |
| Tests (ATE) | ATE_IND.1 Independent testing – conformance |
| Vulnerability Assessment (AVA) | AVA_VAN.1 Vulnerability Survey |

## 6.2.1 Development (ADV)

#### *6.2.1.1 Basic Functional Specification (ADV_FSP.1)*

**ADV_FSP.1.1d** The developer shall provide a functional specification.

**ADV_FSP.1.2d** The developer shall provide a tracing from the functional specification to the SFRs.

**ADV_FSP.1.1c** The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

**ADV_FSP.1.2c** The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

**ADV_FSP.1.3c** The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

**ADV_FSP.1.4c** The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

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

**ADV_FSP.1.2e** The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

## 6.2.2 Guidance documents (AGD)

### *6.2.2.1 Operational User Guidance (AGD_OPE.1)*

**AGD_OPE.1.1d** The developer shall provide operational user guidance.

**AGD_OPE.1.1c** The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

**AGD_OPE.1.2c** The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

**AGD_OPE.1.3c** The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

**AGD_OPE.1.4c** The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

**AGD_OPE.1.5c** The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

**AGD_OPE.1.6c** The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

**AGD_OPE.1.7c** The operational user guidance shall be clear and reasonable.

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

### *6.2.2.2 Preparative Procedures (AGD_PRE.1)*

**AGD_PRE.1.1d** The developer shall provide the TOE including its preparative procedures.

**AGD_PRE.1.1c** The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

**AGD_PRE.1.2c** The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

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

**AGD_PRE.1.2e** The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

### 6.2.3 Life-cycle Support (ALC)

#### *6.2.3.1 Labeling of the TOE (ALC_CMC.1)*

**ALC_CMC.1.1d** The developer shall provide the TOE and a reference for the TOE.

**ALC_CMC.1.1c** The TOE shall be labeled with its unique reference.

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

#### *6.2.3.2 TOE CM coverage (ALC_CMS.1)*

**ALC_CMS.1.1d** The developer shall provide a configuration list for the TOE.

**ALC_CMS.1.1c** The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

**ALC_CMS.1.2c** The configuration list shall uniquely identify the configuration items.

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

### 6.2.4 Tests (ATE)

#### *6.2.4.1 Independent testing - conformance (ATE_IND.1)*

**ATE_IND.1.1d** The developer shall provide the TOE for testing.

**ATE_IND.1.1c** The TOE shall be suitable for testing

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

**ATE_IND.1.2e** The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

## 6.2.5 Vulnerability Assessment (AVA)

### *6.2.5.1 Vulnerability Survey (AVA_VAN.1)*

**AVA_VAN.1.1d** The developer shall provide the TOE for testing.

**AVA_VAN.1.1c** The TOE shall be suitable for testing.

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

**AVA_VAN.1.2e** The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

**AVA_VAN.1.3e** The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

***NOTE**: There were inconsistencies in the assurance naming convention used in the PP. The Table 6-3 has been and section titles have been corrected to be consistent within this ST.*

# 7 TOE Summary Specification

This chapter identifies and describes the security functions implemented by the TOE. The Security Functions are summarized in Table 6-1.

## *7.1 Audit Functions*

### 7.1.1 Audit Generation

FAU_GEN.1

The TOE collects audit data for the events listed in Table 6-2. The TOE generates records for several separate classes of events: authentication/access to the system, actions taken directly on the system by network clients, and management of security functions by authorized administrators.

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).

### 7.1.2 Audit Identity Association

FAU_GEN.2

All actions performed by the TOE are associated with users or with the unique MAC/IP address of a client. User associated events are those performed through the Management UI, such as an administrator changing the TOE configuration settings. MAC address associated events are those that deal with traffic sent by wireless 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.

### 7.1.3 Audit Review

FAU_SAR.1, FAU_SAR.2

The Management GUI provides an interface for Authorized Security Administrators to review audit records.

Audit records can be selected on the basis of start time, end time, MAC address, and record ID.

### 7.1.4 Audit Selection

FAU_SEL.1

The TSF is able to select auditable events based on the following: user identity, event type, success of auditable security events and failure of auditable security events. The administrator selects auditable events using the Web Management UI.

### 7.1.5 Local and External Audit Trail Storage

FAU_STG.1, FAU_STG_EXT.1, FAU_STG_EXT.3, FAU_STG_EXT.4

The TOE stores audit logs locally with up to a fixed size of 256K bytes. The Security Administrator can configure the TOE to send email alert upon the audit logs reaching a configurable percentage of the fixed size.

Local password based authentication and authorization limits the access to the local audit log records thus preventing unauthorized access. Only the Security Administrator can gain access to the local audit log records and those records are delivered confidentially over IPsec encryption.

When the TOE is configured to transmit audit logs to an external SYSLOG server, it simultaneously sends the message to the server and local store. The TOE requires the external audit server and itself to be connected via a IPsec session. The User Guide provides details about the “Auditing Logs” configuration.

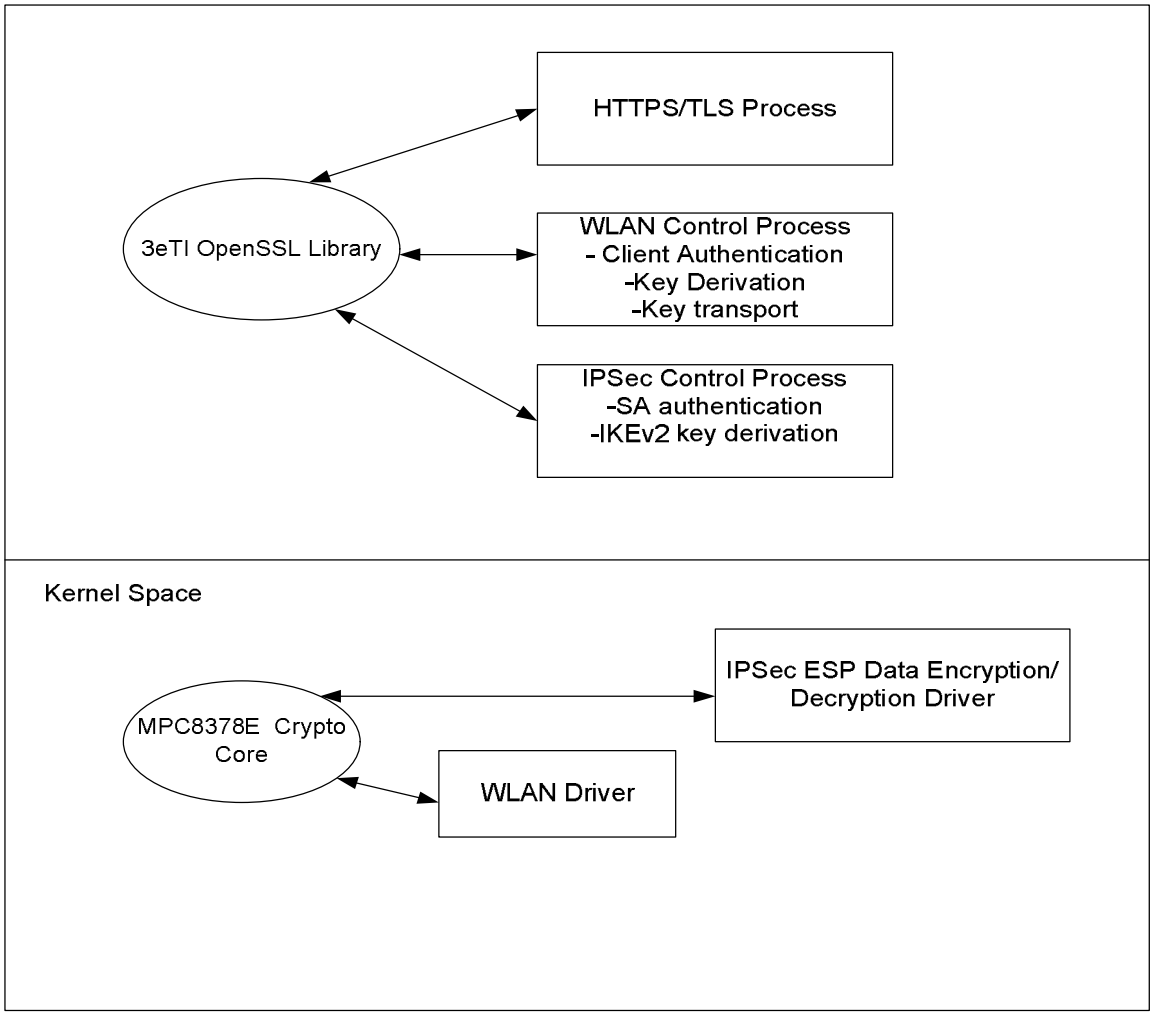
The TOE exports audit data over IPsec using AES128/192/256 bit encryption. Disconnection to external entities such as syslog, NTP and RADIUS server will result in log of communication error and attempt to re-establish secure channel. Data will be transmitted in encrypted format..

When the audit log storage space is full, the TOE provides the Authorized Security Administrator the option of avoiding audit data loss by preventing auditable events from occurring. The Authorized Administrator actions under these circumstances are not logged. The TOE also provides the Authorized Administrator the option of overwriting “old” audit records rather than preventing auditable events.

## *7.2 Cryptographic Support Functions*

There are two cryptographic engines within the device, thus within the TOE as shown in the figure below.

**Figure 7-1: TOE Cryptographic Cores**




First is the 3eTI's own OpenSSL library. 3eTI's OpenSSL Library serves as the sole user application level cryptographic library. It provides the FCS_COP functions listed below. All user level applications, such as HTTPS/TLS Web UI, Wireless LAN Control Application and IPsec SA Authentication Process use this library.

3eTI's OpenSSL provides the following cryptographic algorithms in FIPS mode:

- AES
- RSA
- HMAC
- SHS
- ECDSA
- DRBG

There is a FreeScale MPC8378E cryptographic core within the TOE as well. It provides cryptographic function for the Linux kernel drivers. Wireless client data encryption/decryption functions are provided by this engine. IPsec ESP data encryption/decryption using AES-CBC with SHS or AES-GCM is provided by this engine as well.

The Kernel Crypto Library provides the following cryptographic algorithms in FIPS mode:

- AES (CCM, CMAC & GCM)
- HMAC
- SHS

**Table 7-1: TOE FIPS-140 Tested Algorithms**

| Algorithm | Cert No. | SFR Mapping |
|---|---|---|
| **3eTI OpenSSL** | | |
| AES (ECB, CBC, 128, 256 bits key) | 2060 | FCS_COP.1(1)<br>FCS_CKM.2(2) |
| ECDSA, sign/verify with P256, P384 and P521 | 303,415 | FCS_COP.1(2)<br>FCS_CKM.1(2) |
| SHS | 1801 | FCS_COP.1(3) |
| HMAC | 1253 | FCS_COP.1(4) |
| RSA | 1072,1278,1491 | FCS_COP.1(2)<br>FCS_CKM.1(1) |
| DRBG NIST SP800-90 with one independent hardware based noise source of 256 bits of non-deterministic | 822 | FCS_RBG_EXT.1 |
| **MPC8378E Cryptographic Core** | | |
| AES (ECB, CBC,CCM) | 2078 | FCS_COP.1(1)<br>FCS_COP.1(5) |
| AES_GCM | 2105 | FCS_COP.1(1) |
| HMAC | 1259 | FCS_COP.1(4) |
| SHS | 1807 | FCS_COP.1(3) |

Secondly, the TOE also contains NIST CMVP validate cryptographic module with validation number 1791. Compliance to the CC WLANPP evaluated configuration for cryptography is provided out of the box. There is no means to modify/disable/enable the cryptography used.

### 7.2.1 Cryptographic Symmetric Key Generation

FCS_CKM.1 (1), FCS_CKM.1 (2)

Symmetric keys are generated using the Random Number Generator during the key agreement operations.

The symmetric key for communications between the TOE and the wireless client is generated during the 802.11i defined 4-way handshake process using random numbers generated by a FIPS-Approved Random Number Generator. 802.11-2007 specified cryptographic key derivation algorithm [PRF-384] is strictly followed by the TOE. The TOE is Wi-Fi Alliance

certificated to prove the correctness of key derivation and interoperability between the TOE and other commercial Wi-Fi products. The following 3rd party wireless clients are used to validate the correctness of PRF-384 implementation of the TOE:

1. Atheros AR5BXB-0092DA version: 9.2.0.499 Windows XP
2. Broadcom BCM943224HMS version: 5.10.112.3 XP
3. Intel 6300/633AN.HMWG/633AN.HMWWB version: 13.5.0.6 Windows 7
4. Ralink RT3800PD2 version: 1.4.13.16.17 Windows XP

The tests are derived out of "**WiFi Certified n System Interoperaility Test Plan**" version 2.0.34 table 260, published b Wi-Fi Alliance.

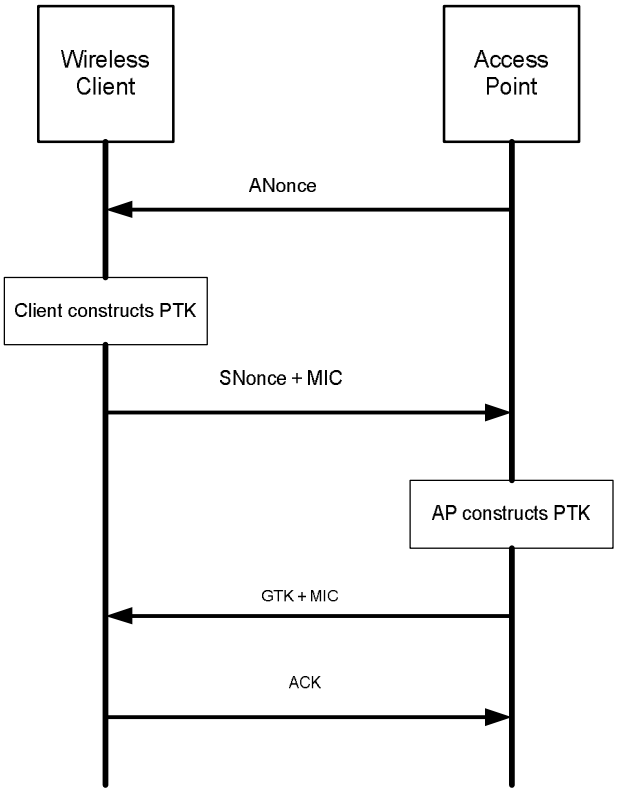
End-to-end wireless encryption between the TOE and the wireless client is implemented using WPA2. The PMK is generated by the RADIUS Server in coordination with the wireless client, encrypted by the IPsec tunnel, and passed to the AP in the RADIUS ACCESS_ACCEPT message. The AP uses the PMK and the 802.11i four-way handshake to generate the Pairwise Transient Key (PTK) and the GTK (Group Temporal Key).

The PTK is generated by concatenating the following attributes: PMK, AP nonce (ANonce), the client (station) nonce (SNonce), AP MAC address, and client MAC address. The product is then put through a cryptographic hash function. The four steps are as follows:

1. The AP sends a nonce-value to the client (ANonce). The client now has all the attributes to construct the PTK.
2. The client sends its own nonce-value (SNonce) to the AP together with a MIC, including authentication, which is really a Message Authentication and Integrity Code: (MAIC).
3. The AP sends the GTK and a sequence number together with another MIC. This sequence number will be used in the next multicast or broadcast frame, so that the receiving STA can perform basic replay detection.
4. The client sends an acknowledgement to the AP.

The messages exchanged during the handshake are depicted in Figure 7-2 below.

**Figure 7-2: 802.11i Four Way Handshake**




The PTK is divided into the individual session keys including the Key Encryption Key (KEK), the Key Confirmation Key (KCK) and the temporal key (TK)) for encrypting the wireless traffic with each wireless client that has been authenticated. The KEK is used by the EAPOL-Key frames to provide confidentiality. The KCK is used by IEEE 802.11i to provide data origin authenticity. The TK, also known as the CCMP key, is the 802.11i session key for unicast communications.

The TSF distribute Group Temporal Key (GTK) by using AES Key Wrap in an EAPOL-Key frame that meets RFC 3394 for AES Key Wrap and 802.11-2007 standard for the packet format and timing considerations.

The TOE allows for the detection of modification of user data while carrying out network communications on the wireless network through the use of AES operating in CCM (CCMP). This is done through the integrity protection capabilities of the algorithm. The Cipher Block Chaining Message Authentication Code (CBC-MAC) component of CCMP provides data integrity. The CBC-MAC allows for the detection of a modified packet. If a CBC-MAC indicates a packet has been modified the packet is dropped.

### 7.2.2 Cryptographic Asymmetric Key Generation

FCS_CKM.1 (2)

The TOE support both RSA and ECDSA for authentication. TOE enforces the RSA key size to be 2048 bits or greater. All keys are generated with the Approved RBG then internally verified with 3eTI OpenSSL public key verification function (PKV)

The TOE generally fulfills all of the NIST SP 800-56A requirements without extensions; the following table specifically identifies the “should”, “should not”, and “shall not” conditions from the publication along with an indication of whether the TOE conforms to those conditions with deviations rationalized.

**Table 7-2: NIST SP500-56A Conformance**

| NIST SP500-56A Section Reference | “should”, “should not”, or “shall not” | Implemented accordingly? | Rationale for deviation |
|---|---|---|---|
| 5.4 | Should | yes | |
| 5.5 | Should(first occurrence) | yes | |
| 5.5 | Should (second occurrence) | yes | |
| 5.6.2 | Should | yes | |
| 5.6.2.1 | Should | yes | |
| 5.6.2.2 | Should | yes | |
| 5.6.2.3 | Should | yes | |
| 5.6.3.1 | Should(first occurrence) | yes | |
| 5.6.3.1 | Should (second occurrence) | yes | |
| 5.6.3.2 | Should | yes | |
| 5.6.4.2 | Should | yes | |
| 5.6.4.3 | Should (first occurrence) | yes | |
| 5.6.4.3 | Should(second occurrence) | yes | |
| 5.6 | Shall not (first occurrence) | yes | |
| 5.6 | Shall not (second occurrence) | yes | |
| 5.8 | Shall not (first occurrence) | no | Not needed for TOE operation, therefore not implemented. |
| 5.8 | Shall not (second occurrence) | no | Not needed for TOE operation, therefore not implemented. |
| 6 | Should (first occurrence) | yes | |
| 6 | Should (second occurrence) | yes | |
| 7 | Shall not (first occurrence) | no | Not needed for TOE operation, therefore not implemented. |
| 7 | Shall not (second occurrence) | no | Not needed for TOE operation, therefore not implemented. |
| 9 | Shall not | no | Not needed for TOE operation, therefore not implemented. |

The TOE generally fulfills all of the NIST SP 800-56B requirements without extensions; the following table specifically identifies the “should”, “should not”, and “shall not” conditions from the publication along with an indication of whether the TOE conforms to those conditions with deviations rationalized.

**Table 7-3: NIST SP800-56B Implementation**

| NIST SP800-56B Section Reference | “should”, “should not”, or “shall not” | Implemented accordingly? | Rationale for deviation |
|---|---|---|---|
| 5.6 | Should | Yes | |
| 5.8 | Shall Not | No | RSA OAEP is not supported. The TOE supports RSA PKCS1 Padding |
| 5.9 | Shall Not (1st instance) | Yes | |
| 5.9 | Shall Not (2nd instance) | Yes | |
| 6.1 | Should Not | Yes | |
| 6.1 | Should (1st instance) | Yes | |
| 6.1 | Should (2nd instance) | Yes | |
| 6.1 | Should (3rd instance) | Yes | |
| 6.1 | Should (4th instance) | Yes | |
| 6.1 | Shall Not (1st instance) | Yes | |
| 6.1 | Shall Not (2nd instance) | Yes | |
| 6.2.3 | Should | Yes | |
| 6.5.1 | Should | Yes | |
| 6.5.2 | Should | Yes | |
| 6.5.2.1 | Should | Yes | |
| 6.6 | Shall Not | Yes | |
| 7.1.2 | Should | Yes | |
| 7.2.1.3 | Should | Yes | |
| 7.2.1.3 | Should Not | Yes | |
| 7.2.2.3 | Shall Not | No | RSA OAEP is not supported. The TOE supports RSA PKCS1 Padding |
| 7.2.2.3 | Should (1st instance) | No | RSA OAEP is not supported. The TOE supports RSA PKCS1 Padding |
| 7.2.2.3 | Should (2nd instance) | No | RSA OAEP is not supported. The TOE supports RSA PKCS1 Padding |

| NIST SP800-56B Section Reference | "should", "should not", or "shall not" | Implemented accordingly? | Rationale for deviation |
|---|---|---|---|
| 7.2.2.3 | Should (3rd instance) | No | RSA OAEP is not supported. The TOE supports RSA PKCS1 Padding |
| 7.2.2.3 | Should (4th instance) | No | RSA OAEP is not supported. The TOE supports RSA PKCS1 Padding |
| 7.2.2.3 | Should Not | No | RSA OAEP is not supported. The TOE supports RSA PKCS1 Padding |
| 7.2.3.3 | Should (1st instance) | No | RSA-KEM-KSW is not supported |
| 7.2.3.3 | Should (2nd instance) | No | RSA-KEM-KSW is not supported |
| 7.2.3.3 | Should (3rd instance) | No | RSA-KEM-KSW is not supported |
| 7.2.3.3 | Should (4th instance) | No | RSA-KEM-KSW is not supported |
| 7.2.3.3 | Should (5th instance) | No | RSA-KEM-KSW is not supported |
| 7.2.3.3 | Should Not | No | RSA-KEM-KSW is not supported |
| 8 | Should | Yes | |
| 8.3.2 | Should Not | Yes | |

When the TOE is operated in FIPS-mode, all cryptographic operations performed by the TOE are FIPS-compliant, using only FIPS-approved algorithms. The corresponding FIPS 140-2 approved algorithms are all CAVP validated by 3eTI as listed in Table 7-2.

### 7.2.3 Cryptographic Key Distribution

FCS_CKM.2 (1), FCS_CKM.2 (2)

The TSF's key material, such as the Pair-wise Master Key (PMK) for Wireless Protected Access (WPA2) in is distributed by RADIUS server to the TOE's 802.1X authenticator components via the ACCESS_ACCEPT message after the wireless client's successful authentication with the RADIUS server. The MSK/PMK is included in the message with attribute: MS_MPPE_SEND_KEY (16) Vendor Specific Attribute (VSA) as defined by RFC 2548. The IPsec tunnel between the TOE and RADIUS server protect the PMK from exposure.

The TSF distribute Group Temporal Key (GTK) by using AES Key Wrap in an EAPOL-Key frame that meets RFC 3394 for AES Key Wrap and 802.11-2007 standard for the packet format

and timing considerations. The GTK is first distributed to the client after the client's successful authentication with the RADIUS server, followed by the process of 802.11i 4-way handshakes which is detailed in section 7.2.1. Figure 7-2 illustrates the GTK distribution.

The TOE has a configurable GTK timeout value. At the configured time expiration, the TOE will update each client the GTK using the AES key wrap mechanism just described.

### 7.2.4 Cryptographic Key Destruction

FCS_CKM_EXT.4

Table 7-4 below lists all the keys and CSPs used and managed by the TOE.

**Table 7-4: TOE CSPs Use and Management**

| Non-Protocol Keys/CSPs | | | | | | |
|---|---|---|---|---|---|---|
| **Key/CSP** | **Type** | **Generation/ Input** | **Output** | **Storage** | **Zeroization** | **Use** |
| Operator passwords | ASCII string | Input encrypted (using TLS session key) | Not output | PKCS5 hash in flash | Zeroized when reset to factory settings. | Used to authenticate CO and Admin role operators |
| Firmware verification key | ECDSA public key | Embedded in firmware at compile time. Firmware upgrade is through encrypted (using TLS session key) | Not output | Plaintext in flash | Zeroized when firmware is upgraded. | Used for firmware digital signature verification |
| 802.1X RADIUS Server Password | ASCII string | Input encrypted (using TLS session key) | Not output | Plaintext in flash | Zeroized when password is upgraded. | Used to create authentication hash value with RADIUS server |
| **DRBG Keys/CSPs** | | | | | | |
| **Key/CSP** | **Type** | **Generation/ Input** | **Output** | **Storage** | **Zeroization** | **Use** |
| NIST SP800-90 DRBG Seed Key | 32-byte value | 512 bytes from hardware noise, then hashed by HMAC-SHA256 | Not output | Plaintext in RAM | Zeroized every time a new random number is generated using the FIPS PRNG after it is | Used to initialize DRBG |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | used. | |
| DRBG Seed | 32-byte value | 512 bytes from hardware noise, then hashed by HMAC-SHA256 | Not output | Plaintext in RAM | Zeroized every time a new random number is generated using the FIPS PRNG after it is used. | Used as seed for DRBG. |
| **RFC 2818 HTTPS Keys/CSPs** | | | | | | |
| **Key/CSP** | **Type** | **Generation/ Input** | **Output** | **Storage** | **Zeroization** | **Use** |
| RSA private key | RSA (2048) (key wrapping; key establishment methodology provides 112-bits of encryption strength) | Not input (installed at factory) | Not output | Plaintext in flash | Zeroized when new private key is uploaded | Used to support CO and Admin TLS/HTTPS interfaces. |
| TLS session key for encryption | Triple-DES (192)<br>AES (128/192/256) | Not input, derived using TLS protocol | Not output | Plaintext in RAM | Zeroized when a page of the web GUI is served after it is used. | Used to protect TLS/HTTPS session. |
| IPsec Keys | | | | | | |
| DH Private Key | 1024, 1536, 2048 bits private key | Generated | Not output | Plaintext in RAM | Zeroized when no longer used | IKE v2 SA setup |
| ECCDH Private Key | 256,384,521 bits | Generated | Not output | Plaintext in RAM and encrypted in FLASH | RAM copy zeroized when no longer used | IKE v2 SA setup |
| IPSec SA Authentication certificate private key | RSA (2048, 4096), ECDSA (256,384,512) | Input encrypted using TLS session key | Not output | Plaintext in RAM and encrypted in FLASH | RAM copy zeroized when no longer used | IKE v2 SA authentication |
| IPSec SA private key password | Text string | Input encrypted using TLS session key | Not output | Plaintext in RAM and encrypted in FLASH | Zeroized when no longer used | Encrypt the IPSec SA certificate private key |

| | | | | | | |
|---|---|---|---|---|---|---|
| IPSec SA session key | Derived from DH/ECCDH key exchange | Not input | Not output | Plaintext in RAM | Zeroized when no longer used | Encrypt and authenticate SA_Auth messages of IKE v2 |
| IPSec ESP symmetric Data encryption key | AES, AES_CCM, AES_GCM (128,192,256) | Not input (derived from SA setup) | Not output | Plaintext in RAM | Zeroized when child SA lifetime expired | Encrypt IPSec ESP data |
| Wireless Access Point Keys | | | | | | |
| PMK | 802.11i pairwise master key | If 802.11i PSK, it's input directly as a Hex string. Input encrypted using the TLS session key.<br><br>If 802.11i EAP-TLS, then not input, instead derived (TLS master secret resulting from successful User EAP-TLS authentication) | Not output | If 802.11i PSK, then plaintext in flash<br><br>For both 802.11i PSK and EAP-TLS, plaintext in RAM | Zeroized when wireless user disconnect or at PMK expiration<br><br>If 802.11i PSK, zeroized when reset to factory settings. | 802.11i PMK |
| KCK | HMAC key (128 bits from PTK) | Not input (derived from PTK) | Not output | Plaintext in RAM | When 802.11i session ends. | 802.11i KCK |
| KEK | AES ECB(e/d; 128) | Not input (derived from PTK) | Not output | Plaintext in RAM | When 802.11i session ends. | 802.11i KEK |
| PTK | AES CCM (e/d; 128) | Not input (derived from PTK) | Not output | Plaintext in RAM | When 802.11i session ends. | 802.11i TK |
| PTK (copy in driver) | AES CCM (e/d; 128) | Not input (derived from PTK) | Not output | Plaintext in RAM | When 802.11i session ends. | 802.11i TK |
| GTK | AES CCM (e/d; 128) | Not input (derived from | Output encrypted | Plaintext in RAM | Zeroized when local antennae | 802.11i GTK |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | GMK) | (using KEK) | | Approved encrypting mode either reconfigured or changed from IEEE 802.11i mode to any other local antennae Approved encrypting mode (including from 802.11i PSK to 802.11i EAP-TLS, and 802.11i EAP-TLS to 802.11i PSK).<br><br>When re-key period expires | |
| **Public Security Parameter** | | | | | | |
| HTTPS Public certificate | RSA (2048) | Input encrypted (using TLS session key) | During TLS session setup | | | Used to setup TLS session for TLS/HTTPS |
| | | | | | | |
| HTTPS root certificate | RSA (2048) | Input encrypted (using TLS session key) | Not output | | | Used to setup TLS session for TLS/HTTPS |

The zeroization technique is to write all 0xa5, then 0x5a, 0xff and finally all zeros to the memory location where the key is stored. The same zeroization technique is applied to flash and RAM with maximum time delay of approximately 100 ns. Therefore there is not sufficient time to read keys and CSPs before they are zeroized, ie from the zeroization determination time to the zeroization effective time.

### 7.2.5 Cryptographic Operation (Data Encryption/Decryption)

FCS_COP.1 (1), FCS_COP.1 (5)

AES is implemented with key sizes of 128, 192, and 256 bits in Counter with Cipher Block Chaining-Message Authentication Code (CCM) mode, Electronic Codebook (ECB) mode, Cipher Block Chaining (CBC) mode and Galois Counter Mode (GCM).

The 3eTI's OpenSSL Library provides AES services for application level data encryption and decryption. The management interface uses this library to provide Transport Layer Security (TLS/HTTPS). For TOE's TLS interface, AES_CBC with 128, 192 or 256 bits key is used.

The TOE performs WPA2 encryption/decryption on wireless traffic by having the radio driver use FIPS approved algorithms and meets FIPS PUB 197, NIST SP 800-38C, and IEEE 802.11-2007. A block of data, a key, and a block mode are passed in, and an encrypted/decrypted block and size are returned. The encryption and decryption is performed by the AES CCMP algorithm with a key size of 128 bits. This service is performed by 3eTI's MPC8378E Cryptographic Core. This cryptographic core provided AES_GCM and AES_CBC services for IPsec data encryption as well. 128, 192 and 256 bits keys are supported.

Table 7-2 lists the AES mode and key sizes, all AES algorithm implementations are NIST CAVP validated.

### 7.2.6 Cryptographic Operation (Cryptographic Signature)

FCS_COP.1 (2)

The 3eTI OpenSSL Library provides the RSA Digital Signature Algorithm (rDSA) to the TLS/HTTPS Daemon for the TLS session. The TLS/HTTPS Daemon enforces a 2048 or larger bits RSA key length for use with the RSA. TOE Firmware's digital signature is using ECDSA with P256. The 3eTI OpenSSL library provides ECDSA sign/verify operation support. IPsec tunnels can be configured to use rDSA (2048, 4096) or ECDSA (256, 384,512) certificate for IPsec SA authentication. Table 7-2 lists RSA and ECDSA CAVP validation certificate numbers.

### 7.2.7 Cryptographic Operation (Cryptographic Hashing)

FCS_COP.1 (3)

The TSF supports SHA-1, SHA-256 and SHA-384 for secure hashing. See Table 7-2 for details.

### 7.2.8 Cryptographic Operation (Keyed-Hash Message Authentication)

FCS_COP.1 (4)

The TOE's OpenSSL Library and the MCP Cryptographic Core both implement HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-384, keyed-hash message authentication supporting digest sizes: 160, 256, and 384 bits and key size of 160 bits implemented to meet FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code", and FIPS PUB 180-3, "Secure Hash Standard.

### 7.2.9 Internet Protocol Security (IPsec) Communications

FCS_IPSEC_EXT.1.1

The TOE implements IPsec protocol in full compliance with IETF RFCs as specified by FCS_IPSEC_EXT.1.1. Within the TOE, 802.1X authenticator service setups IPsec trusted

channel with RADIUS server, NTP client uses IPsec tunnel with NTP server and audit log service will use IPsec tunnel to the remote log server.

FCS_IPSEC_EXT.1.2

The TOE supports ESP mode only. Authentication Header and ESP pass through modes are not supported.The ESP enforces cipher suite of either AES-GCM or AES-CBC with SHA-384, SHA-265 and SHA1. Thus the ESP packet integrity is enforced all times as well as confidentiality. The “confidentiality only” mode is disabled.

FCS_IPSEC_EXT.1.1, FCS_IPSEC_EXT.1.3, FCS_IPSEC_EXT.1.4, FCS_IPSEC_EXT.1.5, , FCS_IPSEC_EXT.1.6, FCS_IPSEC_EXT.1.7, , FCS_IPSEC_EXT.1.8, , FCS_IPSEC_EXT.1.9

The TOE supports IKEv2 only as defined by RFCs 5996 and 4307. During the Security Association (SA) setup phase, the TOE supports the following DH groups:

- ecp521
- ecp384
- ecp256
- modp2048

The group is chosen and enforced by the TOE to make sure that the SA confidentiality strength is equivalent or greater than the configured ESP confidentiality strength. The TOE enforces that the parent SA’s confidentiality strength is equal or greater than child SA’s strength by the following:

1. If the administrator select “Cipher Suite” through the Web GUI, the Web GUI offers a fixed set of ciphers already enforces the above (admin doesn’t have to freedom to choose ciphers violating the rule)
2. If the administrator select “auto negotiation”, then the TOE enforces the above automatically. During the IPsec SA association process, it negotiates cipher with IPsec peer, it will eliminates the weaker ciphers to make sure the parent SA’s strength is equal or greater than the child’s.

The TOE uses NIST SP800-90 DRBG to generate the “x” in each DH group and the nonce. After the Diffie Hellman exchanges that setup the session keys, the IKEv2 payload is protected by the following encryption algorithms:

- AES-CBC-256
- AES-CBC-192
- AES-CBC-128

SHA-384, SHA-256 and SHA1 are used at the mean time to provide payload data integrity. X.509 certificates with rDSA 2048 bits or larger key or ECDSA 256/384/512 bits key are used for IPsec tunnel authentication with its peer.

The TOE supports IPsec tunnel ESP mode encapsulation only. It uses the following ciphers to encrypt the IPsec ESP data:

1. GCM mode with Nonce length of 128, 96 and 64 bytes
    - AES-GCM-128
    - AES-GCM-192
    - AES-GCM-256
2. CBC mode with SHA-384, SHA-256, SHA1 as integrity
    - AES-CBC-128
    - AES-CBC-192
    - AES-CBC-256

The IPsec daemon module implements implicit policies such that only expected data packages are allowed. Any data packages that violate the policy will be discarded.

### 7.2.10 Random Number Generation

FCS_RBG_EXT.1

The TOE implement RBG as defined in NIST SP800-90 using AES. The entropy source is hardware based noise generator.

Entropy is obtained from a zener diode operated in avalanche mode. The noise from the diode is passed through a cascaded pair of operational amplifiers, then applied to the input of a Microchip MCP3221. MCP3221 is a successive approximation analog to digital converter (ADC) with a 12 bit resolution.

The TOE communicates with the MCP3221 hardware over the 2-wire I2C and read in the raw entropy. The raw entropy is further conditioned by the Linux kernel to produce 8 bits of entropy per byte. Then the random bytes are read by the DRBG implementation of 256 bits of DRBG key and DRBG seed.

## *7.3 User Data Protection Functions*

### 7.3.1 Full Residual Information Protection

FDP_RIP.2

Message buffers are zeroized before reallocation to ensure that the TOE does not allow data from a previously transmitted packet to be inserted into unused areas or passed in the current packet. Newly allocated memory buffers are also zeroized prior to its usage.

Message buffers are stored in a pool. Each message buffers is zeroized by writing a zero to each memory location in the buffer before the buffer is added to the pool. Buffers get used by removing them from the pool, used, then returned to the pool. The buffer is zeroized by writing a zero to each memory location before it is returned to the pool.

## *7.4 Identification and Authentication Functions*

### 7.4.1 Authentication failure handling

FIA_AFL.1

The only way to remotely administrate the TOE is through the Web Management UI. The Web Management UI Application will authenticate the administrator when the administrator logs in through the HTTPS connection. The user name and password will be check against the local hashed value. If the failure count reaches the configured threshold, the TOE's HTTPS server will refuse connection from this end point for an administrator configuration time period. The default timeout period is 10 minutes. The authentication failure threshold is configurable by authorized security administrator, the default value is 3. Once a connection is refused, the administrator would have to re-login after the configurable time period has elapsed.

### 7.4.2 Password Management

FIA_PMG_EXT.1, FIA_UAU_EXT.5

The TOE supports the password policy defined in FIA_PMG_EXT.1. Additionally, the TOE supports password lengths up to 32 characters long. NOTE: The TOE will truncate passwords that are longer than 32 characters when creating a user or changing passwords for an existing user.

### 7.4.3 User Identification and Authentication

**Administrative User Authentication**

FIA_UIA_EXT.1, FTA_TAB.1, FIA_UAU.6, FIA_UAU.7

The administrator logs on the TOE through either dedicated local Ethernet port or over WAN Ethernet port to access the Web Management UI. The Web Management UI is accessible over HTTPS only and the TOE support TLS 1.0/1.1/1.2. The Web Management Application can be accessed via the dedicated LAN local Ethernet port configured for "out-of-band" management or through the WAN uplink Ethernet port. There is no local access such as a serial console port. Therefore, the local and remote management is considered the same for this evaluation.

A successful authentication is determined by a successful username and password combination after the HTTPS connection. Incorrect password will result in a failed authentication attempt. When a user is entering their password information, the password is obscured such that no observer could read the password off the screen.

An administrative user is required to re-authenticate when that he/she changes password, and following a TSF-initiated locking as described in any of the FTA_SSL requirements in this ST. There are two TSF responses allowed prior to administrative authentication. The TSF displays the access banner warning and reply to ICMP echo messages packets.

**Wireless Client User Authentication**

FIA_8021X_EXT.1

When a wireless user attempts to associate to a given network, they must first associate with an AP. The TOE maintains the userID and MAC address for the user (and their client) throughout the user's session.

During the security policy discovery phase of 802.11i, the wireless client determines the security methods enforced by the TOE that are advertised by the AP. The Extensible Authentication Protocol (EAP) over LAN (EAPOL) protocol is used for communication between the wireless client and the AP.

Once the wireless client and the AP have negotiated the required security methods, the authentication phase of the process is initiated. The Access Point acts as 802.1X authenticator and provides remote EAP-TLS authentication pass through. During this 802.1x authentication state, the AP denies all packets sent by the client that are not 802.1x EAP packets.

After successful authentication of a wireless client, an IP address is also associated with the client. The IP address may be obtained from a DHCP server on the wired network, or if the client is not using DHCP, then the IP address already configured into the client will be used as an additional identifier for the client along with the MAC address. The TOE shares the identical firmware and hardware design and it is WiFi alliance certified.

The TOE conforms to the 802.1X-2010 standard as described in the following Protocol Implementation Conformance check list located in **Annex A** of **IEEE Std 802.1X-2010**. The sections of the 802.1X-2010 standard that have been implemented as well as applicable options to those sections are specified in the check list below.

Major Capabilities and options:

| Item | Feature | Status | References | Support |
|---|---|---|---|---|
| pae | Are the mandatory functions for a PAE for each real port implemented? | M | 5.3, 5.4, 12, A.6 | Yes [X] |
| supp | Is PAE functionality for an EAP/PACP Supplicant implemented? | O.1 | 5.3, 5.6, 12, 8, 11, A.7 | Yes [ ] No [X] |
| auth | Is the PAE functionality for an EAP/PACP Authenticator implemented? | O.1 | 5.3, 5.8, 12, 8, 11, A.8 | Yes [X] No [ ] |
| mka | Is the PAE functionality for MACsec Key Agreement implemented? | O.1 | 5.3, 5.10, 12, 9, A.9 | Yes [ ] No [X] |
| announce | Is the PAE capable of transmitting EAPOL announcements? | O | 5.14, 12, 10, A.10 | Yes [ ] No [X] |
| paeListen | Is the PAE capable of listening to EAPOL announcements? | O | 5.16, A.11 | Yes [ ] No [X] |
| mgt | Does the implementation support remote PAE management? | O | 5.18, 13, A.12 | Yes [ ] No [X] |
| vp | Is the PAE capable of implementing virtual ports? | O | 5.12, 12, A.13 | Yes [X] No [ ] |
| pac | Is a PAC implemented for each port that does not implement a SecY? | M | 5.3, 5.18, 6.4, A.14 | Yes [X] N/A [ ] |

PAE requirements and options

| Item | Feature | Status | References | Support |
|---|---|---|---|---|
| eapol | Are EAPOL PDUs encoded, decoded, addressed, and validated as specified? | M | 11 | Yes [X] |
| paeRb | Are group addressed EAPOL PDUs transmitted using one, and only one, of the specified addresses? | M | 5.4, Table 11-1 | Yes [X] |
| paeRc | Is the Logon Process functionality implemented as specified in 12.5? | M | 5.4, 12.5 | Yes [X] |
| paeRd | Is the CP state machine implemented as specified in 12.4.? | M | 12.4 | Yes [X] |
| paeRe | Are the EAPOL frame reception statistics maintained and can they be retrieved? | M | 5.4, 12.8.1 | Yes [X] |
| paeRf | Are the EAPOL frame reception diagnostics maintained and can they be retrieved? | M | 5.4, 12.8.2 | Yes [X] |
| paeRg | Are the EAPOL frame transmission statistics maintained and can they be retrieved? | M | 5.4, 12.8.3 | Yes [X] |
| paeRh | Are the system configuration functions specified in 12.9 supported? | M | 5.4, 12.8.3 | Yes [X] |
| paeRi | Are a CAK and CKN derived from using EAP information as specified? | (supp OR auth) AND mka:M | 5.4, 6.2.2 | Yes [ ] N/A [X] |
| paeRj | Specify the group address used: | M | 5.4 | 01:80:C2:00:00:03 |
| paeRk | Are EAPOL Packet Types other than Announcements transmitted using a MACsec protected Controlled Port? | X | 5.4, 10.2 | No[X] |

Authenticator requirements and options

| Item | Feature | Status | References | Support |
|---|---|---|---|---|
| authRa | Is EAP used as an authentication protocol, with PACP implemented as specified by the state machine, variables, and interfaces of Clause 8? | auth:M | 5.6, 8.7 | Yes [X] N/A [ ] |
| authRb | Are EAP methods that do not meet the requirements of 8.11 used? | X | 5.6, 8.11 | No [X] |
| authRc | Does the implementation support configuration of reAuthEnabled and reAuthPeriod? | auth:M | 5.8, 8.6, 8.9 | Yes [X] N/A [ ] |
| authOa | Are the Authenticator diagnostic counters maintained and can they be retrieved? | auth:O | 5.9, 8.10 | Yes [X] No [ ] |
| authO1 | Does the Authenticator support use of a Secure Device Identifier? | auth:O | 5.9, 5.9.1 | Yes [X] N/A [ ] |
| authO1a | Is the EAP method-EAP TLS implemented? | authO1:M | 5.7.1, 8.11.2 | Yes [X] N/A [ ] |

Virtual ports

| Item | Feature | Status | References | Support |
|---|---|---|---|---|
| vpRa | Specify the number of virtual ports that can be supported. | vp:M | 5.12 | 64 |
| vpRb | Is the PAE capable of operating 2 or more MKAinstances per port? | vp:M | 5.12 | Yes [X] |
| vpRc | Is each virtual port supported by a SecY? | vp:M | 5.12 | Yes [X] |
| vpRd | Are virtual ports created and managed as specified? | vp:M | 5.12, 6.3.6, 9.14, 12.7 | Yes [X] |
| vpRe | Are virtual ports created with Supplicant functionality? | X | 5.12 | Yes [X] |
| vpRf | Can the PAE support simultaneous EAP exchanges for each virtual port? | vp:M | 5.12 | Yes [X] |
| vpRg | Is each virtual port that is a Bridge Port supported as specified? | vp:M | 7.6 | Yes [X] |

PAC

| Item | Feature | Status | References | Support |
|---|---|---|---|---|
| pacRa | Does the PAC provide an Uncontrolled and Controlled Port over a real Common Port? | pac:M | 6.4 | Yes [X] |

### TLS and IPsec Authentication

FIA_PSK_EXT.1, FIA_X509_EXT.1

TLS and IPsec authentications peer use X.509 certificate. The TOE is configured with the certificates and their corresponding private key by security administrator. The security administrator can load and delete certificates for usage of TLS/IPsec authentication. During the IPsec authentication using X509 certificate, the TOE develop a certification path from a trust anchor configured by security administrator by fully compliant with RFC 5280. The security administrator can optionally configure the TOE to use CRL as well. The X.509 certificates are stored internally to the TOE. There is no general access interfaces to the certificate stores. The only interface to import the certificates is via the Web UI by authorized administrator via Web server application. There is no interface to export the certificates out of the TOE. The certificate store is protected by access control over the Web UI. Internally, the certificates integrity is always validated at TOE initialization time and at usage time when the certificate is accessed by internal applications. The certificates' private keys are stored in encrypted forms; only internal application with the correct private key password can access the private keys.

RFC 5280 is fully supported in the product. All of the MUSTs, SHALLs, and REQUIRED statements are supported; all of the MUST NOT and SHALL NOT statements are not implemented.

The TOE uses pre-shared keys for IPsec. IPsec PSK keys must be 22 character or between 16 and 32 characters. They must be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").The

TOE conditions the text-based pre-shared keys using the SHA1,SHA-256, and SHA384 hash algorithm and can accept and generate bit based pre-shared keys using the random bit generator.

All authentication successful and unsuccessful authentication attempts are audited by the Access Point including authentication of wireless clients, local authentication for the management user, TLS authentication for TLS connection with audit log server and IPsec

### *7.5 Security Management Functions*

The Web Management Application provides capabilities for the authorized security administrator to manage cryptographic, audit, and authentication functions and data. No administrative functions are accessible through a TOE interface prior to administrator's successful log-in. This management interface is restricted to physical Ethernet connections only.

FMT_MOF.1, FMT_SMR.1, FMT_SMF.1, FMT_MTD.1 (1-3)

The TOE provides the authorized security administrator with the ability to configure the cryptographic settings of the WLAN environment.

The security administrator can perform the following cryptographic operations:

- Load a key
- Delete/zeroize a key
- Set a key lifetime
- Set the cryptographic algorithm
- Set the TOE to encrypt or not to encrypt wireless transmissions
- Execute self tests of TOE hardware and the cryptographic functions

FMT_MTD.1(2)

The authentication data such as user password is stored in PKCS5 hashed format on the flash. Administrator of the TOE can't access the flash memory location through any internal interfaces. Keys are stored in encrypted format on the flash.

The TOE provides visual confirmation that it is running in FIPS-mode

The TOE provides the security administrator with the ability to manage the audit settings of the TOE. The security administrator can perform the following audit functions:.

- Pre-selection of the events that trigger an audit record,
- Select the behavior of audit log when the storage space is full.
- Configure the audit log export behavior to audit log server and configure the TLS setting.

The authorized administrator can perform the following identification and authentication operations:

- Set user password expiration time.
- Set the number of authentication failures that may occur before the TOE takes action to disallow future logins

The TOE also provides the following Remote Management GUI interfaces for administrators to manage the three security functions in the TOE Access (FTA) class:

- Set the length of time a session may remain inactive before it is terminated
- Set TOE Access Banner
- Enable or disable filtering by MAC address
- Configure filtering by MAC address

The TOE safeguards all Critical Security Parameters (CSPs) such as password and private keys. The password is stored in PKCS5 format and the persistent keys are encrypted and stored on flash. There are no interfaces to output the CSPs

***Security Roles***

The TOE provides two roles: Security Administrator and Administrator.

The Security Administrator and Administrator are both authorized administrators.

The Security Administrator and Administrator roles have many common management functions, however, Security Administrator role has extra privileges not available to the Administrator role. The following functions are unique to the Security Administrator:

- Initialization and management of security modules and cryptographic keys
- Audit configuration and viewing
- User management (creation, deletion, reset of users, timeout settings, lockout settings).

All other management functions in the TOE can be performed by the Administrator as well as the Security Administrator. The table below shows the user roles and services.

**Table 7-6: Security Roles**

| Service and Purpose | Details | Crypto Officer (Security Administrator) | Administrator |
|---|---|---|---|
| Input of Keys | IKE v2 digital certificate private key, 802.1X supplicant private key, device HTTPS private keys, authentication key with RADIUS Server. | X | |
| Create and manage users | Support up to 10 administrator users and 5 crypto officer users. | X | |
| Change password | Administrator changes his own password only. | X | X |
| Show system status | View traffic status and systems log excluding security audit log. | X | X |
| Manage audit logging | Select audit events to be logged. Configure remote audit logging. View audit event records. | X | |
| Key zeroization via reboot | All keys in RAM will be zeroized | X | X |

| | | | |
|---|---|---|---|
| Factory default | Delete all configurations and set device back to factory default state. | X | |
| Perform Self-Test | Run algorithm KAT through reboot. | X | X |
| Load New Firmware | Upload 3eTI digitally signed firmware. | X | |
| SNMP Management | Manage all SNMP settings including SNMPv3 encryption key. | X | X |
| HTTPS Management | Load HTTPS server certificate and private key. | X | |
| IPsec Management | Generate IPsec profiles and load certificate or Pre-shared keys | X | |
| WPA2 Security Management | Load WPA2 Pre-shared keys. Configure RADIUS Authentication Server IP address and shared secret. | X | |

## *7.6 Protection of the TSF Functions*

### 7.6.1 Time Stamps

FPT_STM.1

The Access Point has a running NTP daemon to synchronize the local time with an external NTP server. IPsec tunnel is setup between the TOE and NTP server to protect the integrity and privacy of the time source. In the absence of an NTP server in the Operational Environment, the authorized administrator has the capability to set the time locally.

The local time is used for the following security functions identified in this ST:

- Time stamping each audit record.
- Verifying the validity of the Web Server X509v3 Certificate.
- Verifying the validity of the IPsec tunnel peer's Certificate.
- Verifying the validity of the Firmware X509v3 Certificate during the firmware upload process.
- Enforcing user lockout periods for "Bad Password" login attempts.
- Timing out login sessions due to inactivity.

### 7.6.2 TSF Testing

FPT_TST_EXT.1

The TSF performs a firmware integrity check and a configuration file integrity check on system start up. Algorithm Known Answer Tests are run at startup time as shown below:

Power-on self-tests:

Software Integrity Test

- Bootloader Integrity Test
- Firmware Integrity Test

FreeScale PowerQUICC Crypto Engine Power-on self-tests:

- AES ECB encrypt/decrypt KAT
- AES_CCM encrypt/decrypt KAT
- AES_GCM encrypt/decrypt KAT
- SHA-1, SHA256, SHA384 KAT
- HMAC SHA-1, SHA256, SHA384 KAT

3eTI OpenSSL library Power-on self-tests:

- AES ECB – encrypt/decrypt KAT
- Triple-DES CBC – encrypt/decrypt KAT
- HMAC SHA-1, SHA256, SHA384 KAT
- SHA-1, SHA256, SHA384 KAT
- NIST SP800-90 DRBG KAT
- RSA sign/verify KAT
- ECDSA sign/verify KAT

Vectors for each known answer test (KAT) are compiled into the Firmware. The known inputs are provided to the cryptographic function and the output of that function is compared to the known output. The firmware is halted if any of the known answer tests fail.

After device is powered on, the first thing done by bootloader is to check its own integrity. If the integrity is broken, firmware won't boot. Firmware integrity is performed at firmware boot up. Both firmware and bootloader are digitally signed with ECDSA.

Conditional self-tests:

- Continuous DRBG reseed test
- DH pair-wise consistency test at key generation time
- Firmware load test

The Continuous DRBG reseed test is performed whenever the reseed function is invoked and before the reseed is performed on the operational DRBG instantiation.

### 7.6.3 Fail Secure

FPT_FLS.1

In case of any self tests failure or runtime continuous tests failure, the TOE will put itself into SYS_HALT state where all interfaces are disabled and all cryptographic services are disabled. The TOE will flash the "FIPS" LED to indicate such failure and state.This is the only failure mode of the TOE.

### 7.6.4 Trusted Update

FPT_TUD_EXT.1

The Security Administrator can update the TOE's firmware. The firmware is digitally signed with ECDSA. The TOE uses the public key to verify the digital signature. Upon successful verification, the TOE will load the new update upon reboot. The update will be rejected if the verification fails.

The TOE's firmware contains a self-signed X509v3 certificate compiled into the firmware. This certificate is used to verify future firmware updates. The certificate contains an ECDSA public key using prime256v1 curve. Firmware updates must be signed using the corresponding private key held in confidence by 3eTI. The certificate is built with validity dates between the years 1970 and 2038. The certificate is manually updated when a new firmware image is loaded into the device.

The customer of TOE can contact 3eTI to obtains the Common Criteria compliant firmware. The firmware is usually delivered to customer via CD/DVD or secured FTP download.

## *7.7 Resource Utilization*

FRU_RSA.1

The TSF enforces a maximum number of simultaneous wireless connections to 64. This limits memory usage and number of virtual interfaces and buffers. This is imposed per subject (wireless connection) for simultaneous usage. Once the quota is reached, the TSF does not allow any additional wireless connections. The TOE allows one security administrator to log in the system at any given time. A new security administrator's login will cause the other's session to be closed.

## *7.8 TOE Access (FTA)*

### 7.8.1 TSF-Initiated Termination

FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4

The Web Management Application terminates the remote or local session if it detects inactivity longer than the configured time period. The default time period is 10 minutes. The remote session will be closed by the Web Management Application together with the HTTPS session. The Security Administrator is required to re-authenticate with the TOE and setup a new session. The time intervals are configurable by the security administrator.

### 7.8.2 TOE Access Banners

FTA_TAB.1

The Management GUI displays a customizable TOE access banner to the security administrative user before the user can log into the system for local and remote access.The security administrator can access the Management GUI through either dedicated local LAN port or WAN port.

### 7.8.3 TOE Session Establishment (FTA_TSE)

The TOE implements wireless client MAC address filtering functions. The security administrator can specify while list (allow) or black list (deny) or both. The list's attributes are IP address, client WiFi MAC address, time (hour and minute) and day.

An authorized security administrator can configure the TSF to deny establishment of a wireless client based on that client's location, time or day. The location is based on client MAC address as the client will usually move within one wireless BSS.

## *7.9 Trusted Path/Channels Functions*

### 7.9.1 Inter-TSF Trusted Channel

FTP_ITC.1, FCS_TLS_EXT.1, FCS_IPSEC_EXT.1

The TOE provide a trusted communication channel between itself and all authorized IT entities that is logically distinct from other communication channels. IPsec is setup between the TOE and the audit log server, RADIUS and NTP server. The trusted channel can be initiated either by the TOE or by the remote IT entities.

### 7.9.2 Trust Path

FTP_TRP.1, FCS_TLS_EXT.1, FCS_HTTPS_EXT.1

The management interface with remote administration station is always TLS/HTTPS. The HTTPS implementation is fully compliant with RFC 2818. The TOE acts as HTTPS server and waits for client connection on TCP port 443. The TOE's HTTPS server permits an HTTP client to close the connection at any time, and the HTTPS server will recover gracefully. In particular, the HTTPS server is prepared to receive an incomplete close from the client, and is willing to resume TLS sessions closed in this fashion.

The TOE's HTTPS server supports TLS version 1.0/1.1/1.2. It support the following ciphers:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

The TOE's TLS/HTTPS server uses RSA 2048 bits certificate for TLS authentication. After the TLS session's successful setup, the security administrator logs into the TOE via user name and passwords. If the failure count reaches the configured threshold, the TLS/HTTPS session will be terminated by the TLS/HTTPS server.

The TOE supports TLS protocol version 1.0 which is defined in RFC 2246 (Note: the WLAN PP incorrectly calls out RFC 2346). The All of the MUSTs, SHALLs, and REQUIRED statements are supported; all of the MUST NOT and SHALL NOT statements are not implemented.

The TOE supports TLS protocol version 1.1 which is defined in RFC 4346 The All of the MUSTs, SHALLs, and REQUIRED statements are supported; all of the MUST NOT and SHALL NOT statements are not implemented.

The TOE supports TLS protocol version 1.2 which is defined in RFC 5246 The All of the MUSTs, SHALLs, and REQUIRED statements are supported; all of the MUST NOT and SHALL NOT statements are not implemented.

The TOE implements HTTP Over TLS as defined by RFC 2818, May 2000 Analysis: This RFC is fully supported in the product. All of the MUSTs, SHALLs, and REQUIRED statements are supported; all of the MUST NOT and SHALL NOT statements are not implemented.