# Ultra 3eTI

# WiFiProtect 3e-525/523 Series Wireless Access Points (NDcPP22e/WLANASEP10) Security Target

Version 0.6
12/15/20

**Ultra 3eTI**

12410 Milestone Center Drive, Suite 650
Germantown, MD 20876

www.ultra-3eTI.com

## LIST OF TABLES

# 1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Ultra 3eTI WiFiProtect 3e-525/523 Wireless Access Points provided by Ultra 3eTI. The TOE is being evaluated as a Network Device and Wireless Access Point.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Objectives (Section 3)
- Extended Components Definition (Section 4)
- Security Requirements (Section 5)
- TOE Summary Specification (Section 6)

***Conventions***

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a parenthetical number placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

## 1.1 Security Target Reference

**ST Title –**Ultra 3eTI WiFiProtect 3e-525/523 Series Wireless Access Points (NDcPP22e/WLANASEP10) Security Target

**ST Version** – Version 0.6

**ST Date** – 12/15/20

## 1.2 TOE Reference

**TOE Identification** – Ultra 3eTI WiFiProtect 3e-525/523 Series Access Points

**TOE Developer** – Ultra 3eTI

**Evaluation Sponsor** – Ultra 3eTI

## 1.3 TOE Overview

The Target of Evaluation (TOE) is Ultra 3eTI WiFiProtect 3e-525/523 Series Wireless Access Points running firmware version 5.1.0.

The Target of Evaluation (TOE) includes the following hardware models: 3e-525N, 3e-525N MP and 3e-523N. The models share identical hardware and run the same firmware image. Differences between models are limited to enclosure, power options and the number of Wi-Fi radio interfaces.

The table below shows the differences among the 3eTI Wireless Access Points (APs)

**Table 1-1 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-523N | 1 | Access Point | Indoor Enclosure | Operate in Industrial temperature range -40C to 75C |

### 1.3.1 TOE Operational Environment

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

Also note that SNMP management and AP to AP secured communication service are outside the evaluated configuration.

## 1.4 TOE Description

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 (802.11s is not validated).

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 an Access Point that mediates authenticated wireless client's data through encryption/decryption and integrity protection between the wireless link and the wired LAN.

### 1.4.1 TOE Architecture

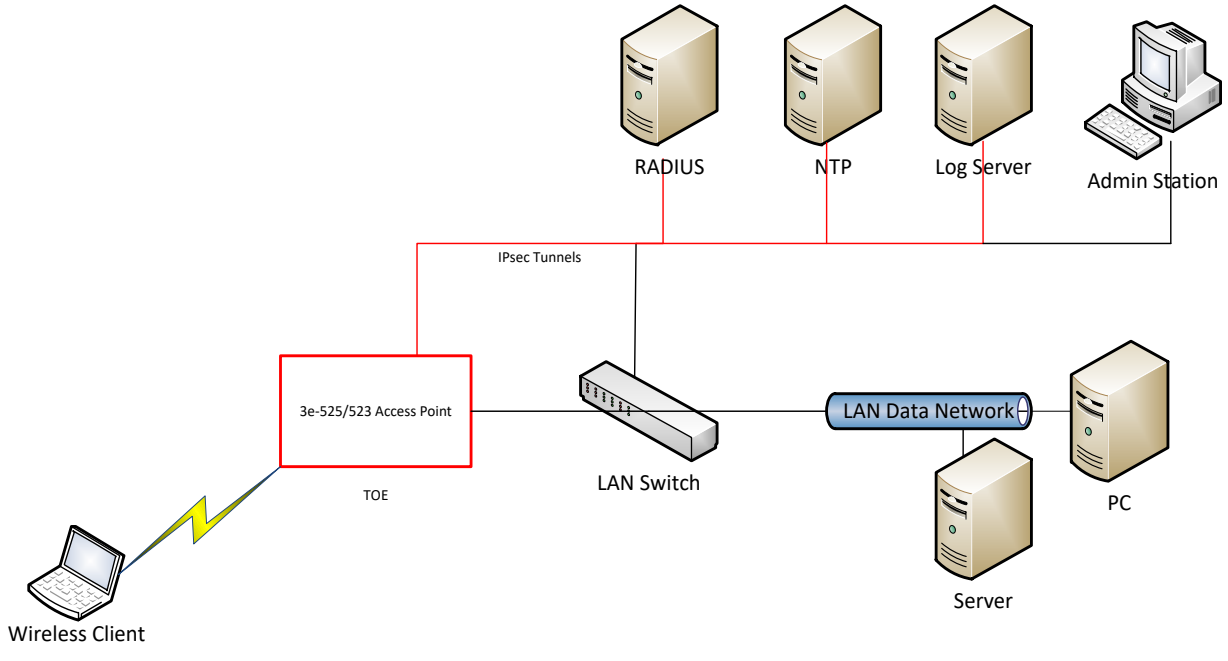
The 3eTI 3e-525N, 3e-525N MP and 3e-523N Access Points (hereafter referred to as Access Points or APs) provide the connection point between wireless client hosts and the wired network. Once installed as trusted nodes on the wired infrastructure, the APs provide the encryption service on the wireless 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 consisting 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, 802.11g 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 firmware 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 firmware 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 the TOE and Administration Station is TLS/HTTPS and the trusted path between the TOE and NTP, Log Server and RADIUS server is IPsec.

The figure below illustrates the typical deployment use case and operational environment setup for TOE devices.




>>

#### 1.4.1.1 Physical Boundaries

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 an 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.

#### 1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by WiFiProtect 3e-525/523 Access Point:

- Security audit
- Cryptographic support
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

##### 1.4.1.2.1 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 Web User Interface (UI) 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.

##### 1.4.1.2.2 Cryptographic support

The TOE uses NIST SP 800-90 DRBG random bits generator and the following cryptographic algorithms: AES, RSA, ECDSA, SHA, HMAC to secure the wireless client data to the LAN, trusted channel and trusted path communication. The TOE zeroizes Critical Security Parameters (CSPs) to mitigate the possibility of disclosure or modification.

##### 1.4.1.2.3 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 a 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 an IPsec tunnel with a RADIUS server and supports IKEv2 with x.509 certificates for IPsec endpoints mutual authentication with its IPsec peer.

#### 1.4.1.2.4 Security management

The Web User Interface (UI) of the TOE provides the capabilities for configuration and administration. The Web UI can be accessed via the dedicated local Ethernet port configured for "out-of-band" management. 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 UI also offers an authorized administrator the capability to manage how security functions behave. For example, an administrator can enable/disable certain audit functions query and set encryption/decryption algorithms used for network packets.

#### 1.4.1.2.5 Protection of the TSF

Internal testing of the TOE hardware, firmware, and firmware updates against tampering ensures that all security functions are running and available before the TOE accepts 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 updates are installed.

#### 1.4.1.2.6 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

#### 1.4.1.2.7 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 clients using WPA2 with 802.1x EAP-TLS. IPsec tunnels are used by the TOE to setup trusted channels with an NTP, RADIUS and Audit Log server.

### 1.4.2 TOE Documentation

- Ultra Electronics 3eTI WiFiProtect User's Guide (3e-523N, 3e-525N, 3e-525N-MP), 15 December 2020, 29010012-001, Revision M (**Admin Guide**)

# 2. Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.
    - Part 3 Conformant
- Package Claims:
    - Network Device Collaborative Protection Profile (NDcPP) Extended Package Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 29 May 2015 (NDcPP22e/WLANASEP10) with technical decisions: TD0282, TD0271, TD0277 TD0315, and TD0456.
    - collaborative Protection Profile for Network Devices Version 2.2e, 23 March 2020 (NDcPP22E) with technical decisions: TD0527, TD0528, TD0536, TD0537, TD0538, TD0546 (not applicable SFR not claimed), and TD0547.

## 2.1 Conformance Rationale

The ST conforms to the NDcPP22e/WLANASEP10. As explained previously, the security problem definition, security objectives, and security requirements have been drawn from the PP.

# 3. Security Objectives

The Security Problem Definition may be found in the NDcPP22e/WLANASEP10 and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The NDcPP22e/WLANASEP10 offers additional information about the identified security objectives, but that has not been reproduced here and the NDcPP22e/WLANASEP10 should be consulted if there is interest in that material.

In general, the NDcPP22e/WLANASEP10 has defined Security Objectives appropriate for Network Device and Wireless Access Point and as such are applicable to the WiFiProtect 3e-525/523 TOE.

## 3.1 Security Objectives for the Operational Environment

**OE.ADMIN_CREDENTIALS_SECURE** The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

**OE.CONNECTIONS** TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic flowing among attached networks.

**OE.NO_GENERAL_PURPOSE** There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.

**OE.NO_THRU_TRAFFIC_PROTECTION** The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

**OE.PHYSICAL** Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

**OE.RESIDUAL_INFORMATION** The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.

**OE.TRUSTED_ADMIN** TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality.
For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.

**OE.UPDATES** The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

# 4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the NDcPP22e/WLANASEP10. The NDcPP22e/WLANASEP10 defines the following extended requirements and since they are not redefined in this ST the NDcPP22e/WLANASEP10 should be consulted for more information in regard to those CC extensions.

**Extended SFRs:**

- NDcPP22e:FAU_STG_EXT.1: Protected Audit Event Storage
- NDcPP22e:FCS_HTTPS_EXT.1: HTTPS Protocol
- NDcPP22e:FCS_IPSEC_EXT.1: IPsec Protocol
- WLANASEP10:FCS_IPSEC_EXT.1: Extended: Internet Protocol Security (IPsec) Communications
- NDcPP22e:FCS_NTP_EXT.1: NTP Protocol
- NDcPP22e:FCS_RBG_EXT.1: Random Bit Generation
- NDcPP22e: FCS_TLSS_EXT.1: TLS Server Protocol Without Mutual Authentication

- WLANASEP10:FIA_8021X_EXT.1: Extended: 802.1X Port Access Entity (Authenticator) Authentication
- NDcPP22e:FIA_PMG_EXT.1: Password Management
- WLANASEP10:FIA_PSK_EXT.1: Extended: Pre-Shared Key Composition
- NDcPP22e:FIA_UAU_EXT.2: Password-based Authentication Mechanism
- NDcPP22e:FIA_UIA_EXT.1: User Identification and Authentication
- NDcPP22e:FIA_X509_EXT.1/ITT: X.509 Certificate Validation
- NDcPP22e:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
- NDcPP22e:FIA_X509_EXT.2: X.509 Certificate Authentication
- NDcPP22e:FIA_X509_EXT.3: X.509 Certificate Requests
- NDcPP22e:FPT_APW_EXT.1: Protection of Administrator Passwords
- NDcPP22e:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
- NDcPP22e:FPT_STM_EXT.1: Reliable Time Stamps
- NDcPP22e:FPT_TST_EXT.1: TSF testing
- WLANASEP10:FPT_TST_EXT.1: Extended: TSF Testing
- NDcPP22e:FPT_TUD_EXT.1: Trusted update
- NDcPP22e:FTA_SSL_EXT.1: TSF-initiated Session Locking

# 5. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the NDcPP22e/WLANASEP10. The refinements and operations already performed in the NDcPP22e/WLANASEP10 are not identified (e.g., highlighted) here, rather the requirements have been copied from the NDcPP22e/WLANASEP10 and any residual operations have been completed herein. Of particular note, the NDcPP22e/WLANASEP10 made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are also drawn from the NDcPP22e/WLANASEP10 which includes all the SARs for EAL 1. However, the SARs are effectively refined since requirement-specific 'Assurance Activities' are defined in the NDcPP22e/WLANASEP10 that serve to ensure corresponding evaluations will yield more practical and consistent assurance than the EAL 1 assurance requirements alone. The NDcPP22e/WLANASEP10 should be consulted for the assurance activity definitions.

## 5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by WiFiProtect 3e-525/523 Access Points TOE.

| Requirement Class | Requirement Component |
|---|---|
| **FAU: Security audit** | NDcPP22e:FAU_GEN.1: Audit Data Generation |
| | WLANASEP10:FAU_GEN.1: Audit Data Generation |
| | NDcPP22e:FAU_GEN.2: User identity association |
| | NDcPP22e:FAU_STG.3/LocSpace: Action in case of possible audit data loss |
| | NDcPP22e:FAU_STG.1: Protected audit trail storage |
| | NDcPP22e:FAU_STG_EXT.1: Protected Audit Event Storage |
| **FCS: Cryptographic support** | NDcPP22e:FCS_CKM.1: Cryptographic Key Generation |
| | WLANASEP10:FCS_CKM.1(2): Cryptographic Key Generation (Symmetric Keys for WPA2 Connections) |
| | NDcPP22e:FCS_CKM.2: Cryptographic Key Establishment |
| | WLANASEP10:FCS_CKM.2(2): Cryptographic Key Distribution (PMK) |
| | WLANASEP10:FCS_CKM.2(3): Cryptographic Key Distribution (GTK) |
| | NDcPP22e:FCS_CKM.4: Cryptographic Key Destruction |
| | WLANASEP10:FCS_COP.1(1): Cryptographic Operation (AES Data Encryption/Decryption) |
| | NDcPP22e:FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption) |
| | NDcPP22e:FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm) |
| | NDcPP22e:FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm) |
| | NDcPP22e:FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification) |
| | NDcPP22e:FCS_HTTPS_EXT.1: HTTPS Protocol |
| | NDcPP22e:FCS_IPSEC_EXT.1: IPsec Protocol |
| | WLANASEP10:FCS_IPSEC_EXT.1: Extended: Internet Protocol Security (IPsec) Communications |
| | NDcPP22e:FCS_NTP_EXT.1: NTP Protocol |

| | |
|---|---|
| | NDcPP22e:FCS_RBG_EXT.1: Random Bit Generation |
| | NDcPP22e:FCS_TLSS_EXT.1: TLS Server Protocol Without Mutual Authentication |
| **FIA: Identification and authentication** | WLANASEP10:FIA_8021X_EXT.1: Extended: 802.1X Port Access Entity (Authenticator) Authentication |
| | NDcPP22e:FIA_AFL.1: Authentication Failure Management |
| | WLANASEP10:FIA_AFL.1: Authentication Failure Handling |
| | NDcPP22e:FIA_PMG_EXT.1: Password Management |
| | WLANASEP10:FIA_PSK_EXT.1: Extended: Pre-Shared Key Composition |
| | WLANASEP10:FIA_UAU.6: Re-authenticating |
| | NDcPP22e:FIA_UAU.7: Protected Authentication Feedback |
| | NDcPP22e:FIA_UAU_EXT.2: Password-based Authentication Mechanism |
| | NDcPP22e:FIA_UIA_EXT.1: User Identification and Authentication |
| | NDcPP22e:FIA_X509_EXT.1/Rev: X.509 Certificate Validation |
| | NDcPP22e:FIA_X509_EXT.2: X.509 Certificate Authentication |
| | NDcPP22e:FIA_X509_EXT.3: X.509 Certificate Requests |
| **FMT: Security management** | NDcPP22e:FMT_MOF.1/Functions: Management of Security Functions Behaviour |
| | NDcPP22e:FMT_MOF.1/ManualUpdate: Management of security functions behaviour |
| | NDcPP22e:FMT_MOF.1/Services: Management of Security Functions Behaviour |
| | NDcPP22e:FMT_MTD.1/CoreData: Management of TSF Data |
| | NDcPP22e:FMT_MTD.1/CryptoKeys: Management of TSF Data |
| | NDcPP22e:FMT_SMF.1: Specification of Management Functions |
| | WLANASEP10:FMT_SMR.1: Security Management Roles |
| | NDcPP22e:FMT_SMR.2: Restrictions on Security Roles |
| **FPT: Protection of the TSF** | NDcPP22e:FPT_APW_EXT.1: Protection of Administrator Passwords |
| | WLANASEP10:FPT_FLS.1: Failure with preservation of secure state |
| | NDcPP22e:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys) |
| | NDcPP22e:FPT_STM_EXT.1: Reliable Time Stamps |
| | NDcPP22e:FPT_TST_EXT.1: TSF testing |
| | WLANASEP10:FPT_TST_EXT.1: Extended: TSF Testing |
| | NDcPP22e:FPT_TUD_EXT.1: Trusted update |
| **FTA: TOE access** | NDcPP22e:FTA_SSL.3: TSF-initiated Termination |
| | NDcPP22e:FTA_SSL.4: User-initiated Termination |
| | NDcPP22e:FTA_SSL_EXT.1: TSF-initiated Session Locking |
| | NDcPP22e:FTA_TAB.1: Default TOE Access Banners |
| | WLANASEP10:FTA_TSE.1: TOE Session Establishment |
| **FTP: Trusted path/channels** | NDcPP22e:FTP_ITC.1: Inter-TSF trusted channel |
| | WLANASEP10:FTP_ITC.1: Inter-TSF Trusted Channel |
| | NDcPP22e:FTP_TRP.1/Admin: Trusted Path |

**Table 1 TOE Security Functional Components**

### 5.1.1 Security audit (FAU)

#### 5.1.1.1 Audit Data Generation (NDcPP22e:FAU_GEN.1)

**NDcPP22e:FAU_GEN.1.1**

The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrative actions comprising:
- Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).
- Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).
- Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).
- Resetting passwords (name of related user account shall be logged).
- [***no other actions***];
d) Specifically defined auditable events listed in Table 2.

| Requirement | Auditable Events | Additional Content |
|---|---|---|
| **NDcPP22e:FAU_GEN.1** | None | None |
| **WLANASEP10:FAU_GEN.1** | None | None |
| **NDcPP22e:FAU_GEN.2** | None | None |
| **NDcPP22e:FAU_STG.3/LocSpace** | Low storage space for audit events. | None |
| **NDcPP22e:FAU_STG.1** | None | None |
| **NDcPP22e:FAU_STG_EXT.1** | None | None |
| **NDcPP22e:FAU_STG_EXT.4** | None | None |
| **NDcPP22e:FAU_STG_EXT.5** | None | None |
| **NDcPP22e:FCS_CKM.1** | None | None |
| **WLANASEP10:FCS_CKM.1(2)** | None. (TD0456 applied) | None. (TD0456 applied) |
| **NDcPP22e:FCS_CKM.2** | None | None |
| **WLANASEP10:FCS_CKM.2(2)** | None. (TD0456 applied) | None. (TD0456 applied) |
| **WLANASEP10:FCS_CKM.2(3)** | None. (TD0456 applied) | None. (TD0456 applied) |
| **NDcPP22e:FCS_CKM.4** | None | None |
| **WLANASEP10:FCS_COP.1(1)** | None. (TD0456 applied) | None. (TD0456 applied) |
| **NDcPP22e:FCS_COP.1/DataEncryption** | None | None |
| **NDcPP22e:FCS_COP.1/Hash** | None | None |
| **NDcPP22e:FCS_COP.1/KeyedHash** | None | None |
| **NDcPP22e:FCS_COP.1/SigGen** | None | None |
| **NDcPP22e:FCS_HTTPS_EXT.1** | Failure to establish a HTTPS Session. | Reason for failure. |
| **NDcPP22e:FCS_IPSEC_EXT.1** | Failure to establish an IPsec SA. | Reason for failure. |
| **WLANASEP10:FCS_IPSEC_EXT.1** | Protocol failures. Establishment/Termination of an IPsec SA. Negotiation “down” from an IKEv2 to IKEv1 exchange. | Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures. |
| **NDcPP22e:FCS_NTP_EXT.1** | Configuration of a new time server Removal of configured time server | Identity if new/removed time server |
| **NDcPP22e:FCS_RBG_EXT.1** | None | None |

| | | |
|---|---|---|
| **NDcPP22e:FCS_TLSS_EXT.1** | Failure to establish a TLS Session. | Reason for failure. |
| **WLANASEP10:FIA_8021X_EXT.1** | Attempts to access the 802.1X controlled port prior to successful completion of the authentication exchange. | Provided client identity (MAC address). |
| **NDcPP22e:FIA_AFL.1** | Unsuccessful login attempt limit is met or exceeded. | Origin of the attempt (e.g., IP address). |
| **WLANASEP10: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). | None |
| **NDcPP22e:FIA_PMG_EXT.1** | None | None |
| **WLANASEP10:FIA_PSK_EXT.1** | None | None |
| **WLANASEP10:FIA_UAU.6** | Attempts to re-authenticate. | Origin of the attempt (e.g., IP address). |
| **NDcPP22e:FIA_UAU.7** | None | None |
| **NDcPP22e:FIA_UAU_EXT.2** | All use of identification and authentication mechanism. | Origin of the attempt (e.g., IP address). |
| **NDcPP22e:FIA_UIA_EXT.1** | All use of identification and authentication mechanism. | Origin of the attempt (e.g., IP address). |
| **NDcPP22e:FIA_X509_EXT.1/Rev** | Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the TOE's trust store | Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store |
| **NDcPP22e:FIA_X509_EXT.2** | None | None |
| **NDcPP22e:FIA_X509_EXT.3** | None | None |
| **NDcPP22e:FMT_MOF.1/Functions** | None | None |
| **NDcPP22e:FMT_MOF.1/ManualUpdate** | Any attempt to initiate a manual update. | None |
| **NDcPP22e:FMT_MOF.1/Services** | None | None |
| **NDcPP22e:FMT_MTD.1/CoreData** | None | None |
| **NDcPP22e:FMT_MTD.1/CryptoKeys** | Management of cryptographic keys. | None |
| **NDcPP22e:FMT_SMF.1** | All management activities of TSF data. | None |
| **WLANASEP10:FMT_SMR.1** | None | None |
| **NDcPP22e:FMT_SMR.2** | None | None |
| **NDcPP22e:FPT_APW_EXT.1** | None | None |
| **WLANASEP10:FPT_FLS.1** | Failure of the TSF. | Indication that the TSF has failed with the type of failure that occurred. |
| **NDcPP22e:FPT_SKP_EXT.1** | None | None |
| **NDcPP22e:FPT_STM_EXT.1** | Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be | For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address). |

| | | |
|---|---|---|
| | logged. See also application note on FPT_STM_EXT.1) | |
| **NDcPP22e:FPT_TST_EXT.1** | None | None |
| **WLANASEP10:FPT_TST_EXT.1** | Execution of this set of TSF self-tests. Detected integrity violations. | For integrity violations, the TSF code file that caused the integrity violation. |
| **NDcPP22e:FPT_TUD_EXT.1** | Initiation of update; result of the update attempt (success or failure). | None |
| **NDcPP22e:FTA_SSL.3** | The termination of a remote session by the session locking mechanism. | None |
| **NDcPP22e:FTA_SSL.4** | The termination of an interactive session. | None |
| **NDcPP22e:FTA_SSL_EXT.1** | (if 'lock the session' is selected) Any attempts at unlocking of an interactive session. (if 'terminate the session' is selected) The termination of a local session by the session locking mechanism. | None |
| **NDcPP22e:FTA_TAB.1** | None | None |
| **WLANASEP10:FTA_TSE.1** | Denial of a session establishment due to the session establishment mechanism. | Reason for denial, origin of establishment attempt. |
| **NDcPP22e:FTP_ITC.1** | Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions. | Identification of the initiator and target of failed trusted channels establishment attempt. |
| **WLANASEP10:FTP_ITC.1** | Failed attempts to establish a trusted channel (including IEEE 802.11). Detection of modification of channel data. | Identification of the initiator and target of channel. |
| **NDcPP22e:FTP_TRP.1/Admin** | Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions. | None |

Table 2: Security Functional Requirements and Auditable Events

**NDcPP22e: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 cPP/ST, information specified in column three of Table 2.

#### 5.1.1.2 User identity association (NDcPP22e:FAU_GEN.2)

**NDcPP22e:FAU_GEN.2.1**

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

.

#### 5.1.1.3 Action in case of possible audit data loss (NDcPP22e:FAU_STG.3/LocSpace)

**NDcPP22e:FAU_STG.3.1/LocSpace**

The TSF shall generate a warning to inform the Administrator if the audit trail exceeds the local audit trail storage capacity.

#### 5.1.1.4 Protected audit trail storage (NDcPP22e:FAU_STG.1)

**NDcPP22e:FAU_STG.1.1**

The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

**NDcPP22e:FAU_STG.1.2**

The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.

#### 5.1.1.5 Protected Audit Event Storage (NDcPP22e:FAU_STG_EXT.1)

**NDcPP22e: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 according to FTP_ITC.1.

**NDcPP22e:FAU_STG_EXT.1.2**

The TSF shall be able to store generated audit data on the TOE itself. In addition, [***TOE shall consist of a single standalone component that stores audit data locally***]

**NDcPP22e:FAU_STG_EXT.1.3**

The TSF shall [***overwrite previous audit records according to the following rule: [when allotted space has reached its threshold]***] when the local storage space for audit data is full.

### 5.1.2 Cryptographic support (FCS)

#### 5.1.2.1 Cryptographic Key Generation (NDcPP22e:FCS_CKM.1)

**NDcPP22e:FCS_CKM.1.1**

The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

***- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS) ', Appendix B.3,***

***- ECC schemes using 'NIST curves' [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4,***

***-FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.1,***

***- FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526].***

#### 5.1.2.2 Cryptographic Key Generation (Symmetric Keys for WPA2 Connections) (WLANASEP10:FCS_CKM.1(2))

**WLANASEP10:FCS_CKM.1.1(2)**

Refinement: The TSF shall generate symmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm PRF-384 and [***no other***] and specified cryptographic key sizes 128 bits and [***no other key sizes***] using a Random Bit Generator as specified in FCS_RBG_EXT.1 that meet the following: IEEE 802.11-2012 and [***no other standards***].

#### 5.1.2.3 Cryptographic Key Establishment (NDcPP22e:FCS_CKM.2)

**NDcPP22e:FCS_CKM.2.1**

The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [

***- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1,***

***- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography',***

***- Finite field-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography'***

***- FFC Schemes using "safe-prime" groups that meet the following: "NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526]***].

#### 5.1.2.4 Cryptographic Key Distribution (PMK) (WLANASEP10:FCS_CKM.2(2))

**WLANASEP10:FCS_CKM.2.1(2)**

Refinement: The TSF shall receive the 802.11 Pairwise Master Key (PMK) in accordance with a specified cryptographic key distribution method: from 802.1X Authorization Server that meets the following: IEEE 802.11-2012 and does not expose the cryptographic keys.

#### 5.1.2.5 Cryptographic Key Distribution (GTK) (WLANASEP10:FCS_CKM.2(3))

**WLANASEP10:FCS_CKM.2.1(3)**

Refinement: The TSF shall distribute Group Temporal Key (GTK) in accordance with a specified cryptographic key distribution method: [***AES Key Wrap in an EAPOL-Key frame***] that meets the following: NIST SP 800-38F, IEEE 802.11-2012 for the packet format and timing considerations and does not expose the cryptographic keys. (TD0282 applied)

#### 5.1.2.6 Cryptographic Key Destruction (NDcPP22e:FCS_CKM.4)

**NDcPP22e:FCS_CKM.4.1**

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

- For plaintext keys in volatile storage, the destruction shall be executed by a [***single overwrite consisting of [zeros]***];
- For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [
  ***o logically addresses the storage location of the key and performs a [ single-pass] overwrite consisting of [a new value of the key]***]

that meets the following: No Standard.

#### 5.1.2.7 Cryptographic Operation (AES Data Encryption/Decryption) (WLANASEP10:FCS_COP.1(1))

**WLANASEP10:FCS_COP.1.1(1)**

Refinement: The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in CBC, CCMP [***GCM***] mode and cryptographic key sizes 128 bits [***256 bits***] that meet the following: AES as specified in ISO 18033-3, CCMP as defined in NIST SP 800-38C and IEEE 802.11-2012, [***CBC as specified in ISO 10116, GCM as specified in ISO 19772, CCMP as specified in NIST SP800-38D***].

#### 5.1.2.8 Cryptographic Operation (AES Data Encryption/Decryption) (NDcPP22e:FCS_COP.1/DataEncryption)

**NDcPP22e:FCS_COP.1.1/DataEncryption**

The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [***CBC, GCM***] mode and cryptographic key sizes [***128 bits, 256 bits***] that meet the following: AES as specified in ISO 18033-3, [***selection: CBC as specified in ISO 10116, GCM as specified in ISO 19772***].

#### 5.1.2.9 Cryptographic Operation (Hash Algorithm) (NDcPP22e:FCS_COP.1/Hash)

**NDcPP22e:FCS_COP.1.1/Hash**

The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [***SHA-1, SHA-256, SHA-384, SHA-512***] and message digest sizes [***160, 256, 384, 512***] that meet the following: ISO/IEC 10118-3:2004.

#### 5.1.2.10 Cryptographic Operation (Keyed Hash Algorithm) (NDcPP22e:FCS_COP.1/KeyedHash)

**NDcPP22e:FCS_COP.1.1/KeyedHash**

The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [***HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512***] and cryptographic key sizes [***160, 256, 384, 512 bits***] and message digest sizes [***160, 256, 384, 512***] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 'MAC Algorithm 2'.

#### 5.1.2.11 Cryptographic Operation (Signature Generation and Verification) (NDcPP22e:FCS_COP.1/SigGen)

**NDcPP22e:FCS_COP.1.1/SigGen**

The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [

***- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048 bits],***

***- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256, 384, 512 bits]***

]

that meet the following:

[

***- For RSA schemes: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,***

***- For ECDSA schemes: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 6 and Appendix D, Implementing 'NIST curves' [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4***

].

#### 5.1.2.12 HTTPS Protocol (NDcPP22e:FCS_HTTPS_EXT.1)

**NDcPP22e:FCS_HTTPS_EXT.1.1**

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

**NDcPP22e:FCS_HTTPS_EXT.1.2**

The TSF shall implement HTTPS using TLS.

**NDcPP22e:FCS_HTTPS_EXT.1.3**

If a peer certificate is presented, the TSF shall [***not establish the connection***] if the peer certificate is deemed invalid.

#### 5.1.2.13 IPsec Protocol (NDcPP22e/ WLANAScEP10:FCS_IPSEC_EXT.1)

**NDcPP22e/ WLANAScEP10:FCS_IPSEC_EXT.1.1**

The TSF shall implement the IPsec architecture as specified in RFC 4301.

**NDcPP22e/ WLANAScEP10:FCS_IPSEC_EXT.1.2**

The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

**NDcPP22e/ WLANAScEP10:FCS_IPSEC_EXT.1.3**

The TSF shall implement [***transport mode, tunnel mode***].

**NDcPP22e/ WLANAScEP10:FCS_IPSEC_EXT.1.4**

The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [***AES-CBC-128 (RFC 3602), AES-CBC-256 (RFC 3602), AES-GCM-128 (RFC 4106), AES-GCM-256 (RFC 4106)***] together with a Secure Hash Algorithm (SHA)-based HMAC [***HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512***].

**NDcPP22e/ WLANAScEP10:FCS_IPSEC_EXT.1.5**

The TSF shall implement the protocol: [***IKEv2 as defined in RFC 5996 and [with mandatory support for NAT traversal as specified in RFC 5996, section 2.23], and [no other RFCs for hash functions]***].

**NDcPP22e/ WLANAScEP10:FCS_IPSEC_EXT.1.6**

The TSF shall ensure the encrypted payload in the [***IKEv2***] protocol uses the cryptographic algorithms [***AES-CBC-128, AES-CBC-256 (specified in RFC 3602)***].

**NDcPP22e/ WLANAScEP10:FCS_IPSEC_EXT.1.7**

The TSF shall ensure that [***IKEv2 SA lifetimes can be configured by a Security Administrator based on [o length of time, where the time values can be configured within [1-24] hours]***].

**NDcPP22e/ WLANAScEP10:FCS_IPSEC_EXT.1.8**

The TSF shall ensure that [***IKEv2 Child SA lifetimes can be configured by a Security Administrator based on [o number of bytes, o length of time, where the time values can be configured within [1-24] hours]***].

**NDcPP22e/ WLANAScEP10:FCS_IPSEC_EXT.1.9**

The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ('x' in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [***112 , 128 , 192***] bits.

**NDcPP22e/ WLANAScEP10:FCS_IPSEC_EXT.1.10**

The TSF shall generate nonces used in [***IKEv2***] exchanges of length [***according to the security strength associated with the negotiated Diffie-Hellman group***].

**NDcPP22e/ WLANAScEP10:FCS_IPSEC_EXT.1.11**

The TSF shall ensure that IKE protocols implement DH Group(s) [

- ***14 (2048-bit MODP) according to RFC 3526,***
- ***19 (256-bit Random ECP),***
- ***20 (384-bit Random ECP) according to RFC 5114***

].

**NDcPP22e/ WLANAScEP10:FCS_IPSEC_EXT.1.12**

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.

**NDcPP22e/ WLANAScEP10:FCS_IPSEC_EXT.1.13**

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

**NDcPP22e/ WLANAScEP10:FCS_IPSEC_EXT.1.14**

The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: [***SAN: Fully Qualified Domain Name (FQDN), Distinguished Name (DN)***] and [***no other reference identifier type***].

#### 5.1.2.14 NTP Protocol (NDcPP22e:FCS_NTP_EXT.1)

**NDcPP22e:FCS_NTP_EXT.1.1**
The TSF shall use only the following NTP version(s) [***NTP v4 (RFC 5905)***].

**NDcPP22e:FCS_NTP_EXT.1.2**
The TSF shall update its system time using [ ***[IPsec] to provide trusted communication between itself and an NTP time source.***].

**NDcPP22e:FCS_NTP_EXT.1.3**
The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

**NDcPP22e:FCS_NTP_EXT.1.4**
The TSF shall support configuration of at least three (3) NTP time sources.

#### 5.1.2.15 Random Bit Generation (NDcPP22e:FCS_RBG_EXT.1)

**NDcPP22e:FCS_RBG_EXT.1.1**
The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [***CTR_DRBG (AES)***].

**NDcPP22e:FCS_RBG_EXT.1.2**
The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [ ***[1] platform-based noise source***] with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011Table C.1 'Security Strength Table for Hash Functions', of the keys and hashes that it will generate.

#### 5.1.2.16 TLS Server Protocol Without Mutual Authentication (NDcPP22e:FCS_TLSS_EXT.1)

**NDcPP22e:FCS_TLSS_EXT.1.1**
The TSF shall implement [***TLS 1.2 (RFC 5246***] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:
[***TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268,***
***TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268,***
***TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268,***
***TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268,***
***TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,***
***TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246,***
***TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246,***
***TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246,***]
and no other ciphersuites.

**NDcPP22e:FCS_TLSS_EXT.1.2**
The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and [***TLS 1.1***].

**NDcPP22e:FCS_TLSS_EXT.1.3**
The TSF shall perform key establishment for TLS using [***RSA with key size [2048 bits], Diffie-Hellman parameters with size [2048 bits]***].

**NDcPP22e:FCS_TLSS_EXT.1.4**
The TSF shall support [***no session resumption or session tickets***].

### 5.1.3 Identification and authentication (FIA)

#### 5.1.3.1 Extended: 802.1X Port Access Entity (Authenticator) Authentication (WLANASEP10:FIA_8021X_EXT.1)

**WLANASEP10:FIA_8021X_EXT.1.1**
The TSF shall conform to IEEE Standard 802.1X for a Port Access Entity (PAE) in the 'Authenticator' role.

**WLANASEP10:FIA_8021X_EXT.1.2**

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

**WLANASEP10: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.

#### 5.1.3.2 Authentication Failure Management (NDcPP22e:FIA_AFL.1)

**NDcPP22e:FIA_AFL.1.1**

The TSF shall detect when an Administrator configurable positive integer within [**1-8**] unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely using a password.

**NDcPP22e:FIA_AFL.1.2**

When the defined number of unsuccessful authentication attempts has been met, the TSF shall [***prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until an Administrator defined time period has elapsed***].

#### 5.1.3.3 Authentication Failure Handling (WLANASEP10:FIA_AFL.1)

**WLANASEP10:FIA_AFL.1.1**

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

**WLANASEP10: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 Administrator defined time period has elapsed***].

#### 5.1.3.4 Password Management (NDcPP22e:FIA_PMG_EXT.1)

**NDcPP22e:FIA_PMG_EXT.1.1**

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

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [***'!', '@', '#', '$', '%', '^', '&', '*', '(', ')'***];

b) Minimum password length shall be configurable to between [**8**] and [**30**] characters.

#### 5.1.3.5 Extended: Pre-Shared Key Composition (WLANASEP10:FIA_PSK_EXT.1)

**WLANASEP10:FIA_PSK_EXT.1.1**

The TSF shall be able to use pre-shared keys for [***IPSEC***] and [***IEEE 802.11 WPA2-PSK***]. (TD0277 applied)

**WLANASEP10:FIA_PSK_EXT.1.2**

The TSF shall be able to accept text-based pre-shared keys that:

- are 22 characters and [ ***/*lengths from 8 to 63 characters for WPA2; and lengths from 16 to 32 characters for IPsec*/***];
- are composed of any combination of upper and lower case letters, numbers, and special characters (that include: '!', '@', '#', '$', '%', '^', '&', '*', '(', and ')').

**WLANASEP10:FIA_PSK_EXT.1.3**

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

#### 5.1.3.6 Re-authenticating (WLANASEP10:FIA_UAU.6)

**WLANASEP10: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)***].

#### 5.1.3.7 Protected Authentication Feedback (NDcPP22e:FIA_UAU.7)

**NDcPP22e: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.

#### 5.1.3.8 Password-based Authentication Mechanism (NDcPP22e:FIA_UAU_EXT.2)

**NDcPP22e:FIA_UAU_EXT.2.1**

The TSF shall provide a local [***password-based***] authentication mechanism to perform local administrative user authentication.

#### 5.1.3.9 User Identification and Authentication (NDcPP22e:FIA_UIA_EXT.1)

**NDcPP22e:FIA_UIA_EXT.1.1**

The TSF shall allow 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;
- [ **/network packets configured by an authorized administrator may flow through the TOE/**].

**NDcPP22e: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.

#### 5.1.3.10 X.509 Certificate Validation (NDcPP22e:FIA_X509_EXT.1/Rev)

**NDcPP22e:FIA_X509_EXT.1.1/Rev**

The TSF shall validate certificates in accordance with the following rules:
- RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [***a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3***]
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - o Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - o Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - o Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
  - o OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

**NDcPP22e:FIA_X509_EXT.1.2/Rev**

The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

#### 5.1.3.11 X.509 Certificate Authentication (NDcPP22e:FIA_X509_EXT.2)

**NDcPP22e:FIA_X509_EXT.2.1**
The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [***HTTPS, IPsec, TLS***], and [***no additional uses***].

**NDcPP22e:FIA_X509_EXT.2.2**
When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [***accept the certificate***].

#### 5.1.3.12 X.509 Certificate Requests (NDcPP22e:FIA_X509_EXT.3)

**NDcPP22e:FIA_X509_EXT.3.1**
The TSF shall generate a Certification Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [***Common Name, Organization, Organizational Unit, Country***].

**NDcPP22e:FIA_X509_EXT.3.2**
The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

### 5.1.4 Security management (FMT)

#### 5.1.4.1 Management of Security Functions Behaviour (NDcPP22e:FMT_MOF.1/Functions)

**NDcPP22e:FMT_MOF.1.1/Functions**
The TSF shall restrict the ability to [***determine the behaviour of, modify the behaviour of***] the functions ***transmission of audit data to an external IT entity, audit functionality when Local Audit Storage Space is full***] to Security Administrators.

#### 5.1.4.2 Management of security functions behaviour (NDcPP22e:FMT_MOF.1/ManualUpdate)

**NDcPP22e:FMT_MOF.1.1/ManualUpdate**
The TSF shall restrict the ability to enable the functions to perform manual update to Security Administrators.

#### 5.1.4.3 Management of Security Functions Behaviour (NDcPP22e:FMT_MOF.1/Services)

**NDcPP22e:FMT_MOF.1.1/Services**
The TSF shall restrict the ability to start and stop services to Security Administrators.

#### 5.1.4.4 Management of TSF Data (NDcPP22e:FMT_MTD.1/CoreData)

**NDcPP22e:FMT_MTD.1.1/CoreData**
The TSF shall restrict the ability to manage the TSF data to Security Administrators.

#### 5.1.4.5 Management of TSF Data (NDcPP22e:FMT_MTD.1/CryptoKeys)

**NDcPP22e:FMT_MTD.1.1/CryptoKeys**
The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

#### 5.1.4.6 Specification of Management Functions (NDcPP22e:FMT_SMF.1)

**NDcPP22e:FMT_SMF.1.1**
The TSF shall be capable of performing the following management functions:
- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;

- Ability to update the TOE, and to verify the updates using [***digital signature***] capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- [ ***o Ability to configure audit behavior (e.g. changes to storage locations for audit; changes to behavior when local audit storage space is full),***
***o Ability to modify the behavior of the transmission of audit data to an external IT entity,***
***o Ability to manage the cryptographic keys,***
***o Ability to configure the cryptographic functionality,***
***o Ability to configure the lifetime for IPsec SAs,***
***o Ability to re-enable an Administrator account,***
***o Ability to set the time which is used for time-stamps;,***
***o Ability to configure NTP,***
***o Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors,***
***o Ability to import X509v3 certificates to the TOE's trust store***].

#### 5.1.4.7 Security Management Roles (WLANASEP10:FMT_SMR.1)

**WLANASEP10:FMT_SMR.1.3**
The TSF shall ensure that the ability to remotely administer the TOE from a wireless client shall be disabled by default.

#### 5.1.4.8 Restrictions on Security Roles (NDcPP22e:FMT_SMR.2)

**NDcPP22e:FMT_SMR.2.1**
The TSF shall maintain the roles: - Security Administrator.
**NDcPP22e:FMT_SMR.2.2**
The TSF shall be able to associate users with roles.
**NDcPP22e:FMT_SMR.2.3**
The TSF shall ensure that the conditions
- The Security Administrator role shall be able to administer the TOE locally;
- The Security Administrator role shall be able to administer the TOE remotely are satisfied.

### 5.1.5 Protection of the TSF (FPT)

#### 5.1.5.1 Protection of Administrator Passwords (NDcPP22e:FPT_APW_EXT.1)

**NDcPP22e:FPT_APW_EXT.1.1**
The TSF shall store administrative passwords in non-plaintext form.
**NDcPP22e:FPT_APW_EXT.1.2**
The TSF shall prevent the reading of plaintext administrative passwords.

#### 5.1.5.2 Failure with preservation of secure state (WLANASEP10:FPT_FLS.1)

**WLANASEP10: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.

#### 5.1.5.3 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys) (NDcPP22e:FPT_SKP_EXT.1)

**NDcPP22e:FPT_SKP_EXT.1.1**
The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

#### 5.1.5.4 Reliable Time Stamps (NDcPP22e:FPT_STM_EXT.1)

**NDcPP22e:FPT_STM_EXT.1.1**
The TSF shall be able to provide reliable time stamps for its own use.

**NDcPP22e:FPT_STM_EXT.1.2**
The TSF shall [***allow the Security Administrator to set the time, synchronise time with an NTP server***].

#### 5.1.5.5 TSF testing (NDcPP22e:FPT_TST_EXT.1)

**NDcPP22e:FPT_TST_EXT.1.1**
The TSF shall run a suite of the following self-tests [***during initial start-up (on power on), at the request of the authorised user***] to demonstrate the correct operation of the TSF: [**Software integrity test and AES, SHA, HMAC, DRBG, RSA, and ECDSA Known Answer Tests**].

#### 5.1.5.6 Extended: TSF Testing (WLANASEP10:FPT_TST_EXT.1)

**WLANASEP10:FPT_TST_EXT.1.1**
The TSF shall run a suite of the following self-tests during initial start-up (on power on) and [***at the request of the authorized user, at the conditions [when the TOE's configuration is reset]***] to demonstrate the correct operation of the TSF: [**Software integrity test and AES, SHA, HMAC, DRBG, RSA, and ECDSA Known Answer Tests**].

**WLANASEP10:FPT_TST_EXT.1.2**
The TSF shall provide the capability to verify the integrity of stored TSF executable code when it is loaded for execution through the use of the TSF-provided cryptographic service specified in FCS_COP.1(2).

#### 5.1.5.7 Trusted update (NDcPP22e:FPT_TUD_EXT.1)

**NDcPP22e:FPT_TUD_EXT.1.1**
The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software and [***no other TOE firmware/software version***].

**NDcPP22e:FPT_TUD_EXT.1.2**
The TSF shall provide Security Administrators the ability to manually initiate updates to TOE firmware/software and [***no other update mechanism***].

**NDcPP22e:FPT_TUD_EXT.1.3**
The TSF shall provide means to authenticate firmware/software updates to the TOE using a [***digital signature***] prior to installing those updates.

### 5.1.6 TOE access (FTA)

#### 5.1.6.1 TSF-initiated Termination (NDcPP22e:FTA_SSL.3)

**NDcPP22e:FTA_SSL.3.1**
The TSF shall terminate a remote interactive session after a Security Administrator-configurable time interval of session inactivity.

#### 5.1.6.2 User-initiated Termination (NDcPP22e:FTA_SSL.4)

**NDcPP22e:FTA_SSL.4.1**
The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

#### 5.1.6.3 TSF-initiated Session Locking (NDcPP22e:FTA_SSL_EXT.1)

**NDcPP22e:FTA_SSL_EXT.1.1**

The TSF shall, for local interactive sessions, [***terminate the session***] after a Security Administrator-specified time period of inactivity.

#### 5.1.6.4 Default TOE Access Banners (NDcPP22e:FTA_TAB.1)

**NDcPP22e:FTA_TAB.1.1**

Before establishing an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding use of the TOE.

#### 5.1.6.5 TOE Session Establishment (WLANASEP10:FTA_TSE.1)

**WLANASEP10:FTA_TSE.1.1**

Refinement: The TSF shall be able to deny establishment of a wireless client session based on TOE interface, time, day, [**wireless client's MAC address**].

### 5.1.7 Trusted path/channels (FTP)

#### 5.1.7.1 Inter-TSF trusted channel (NDcPP22e:FTP_ITC.1)

**NDcPP22e:FTP_ITC.1.1**

The TSF shall be capable of using [***IPsec***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [***authentication server, [NTP server]***] 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.

**NDcPP22e:FTP_ITC.1.2**

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

**NDcPP22e:FTP_ITC.1.3**

The TSF shall initiate communication via the trusted channel for [**audit logging, accessing an NTP server and accessing the authentication server**].

#### 5.1.7.2 Inter-TSF Trusted Channel (WLANASEP10:FTP_ITC.1)

**WLANASEP10:FTP_ITC.1.1**

Refinement: The TSF shall be capable of using IEEE 802.11-2012 (WPA2), IEEE 802.1X, [***IPsec***], and [***no other protocol***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: WLAN clients, audit servers, 802.1X authentication servers, and [**NTP server**] 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. (TD0271 applied)

#### 5.1.7.3 Trusted Path (NDcPP22e:FTP_TRP.1/Admin)

**NDcPP22e:FTP_TRP.1.1/Admin**

The TSF shall be capable of using [***TLS, HTTPS***] to provide a communication path between itself and authorized 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 provides detection of modification of the channel data.

**NDcPP22e:FTP_TRP.1.2/Admin**

The TSF shall permit remote Administrators to initiate communication via the trusted path.

**NDcPP22e:FTP_TRP.1.3/Admin**

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

## 5.2 TOE Security Assurance Requirements

The SARs for the TOE are the components as specified in Part 3 of the Common Criteria. Note that the SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

| Requirement Class | Requirement Component |
|---|---|
| **ADV: Development** | ADV_FSP.1: Basic Functional Specification |
| **AGD: Guidance documents** | AGD_OPE.1: Operational User Guidance |
| | AGD_PRE.1: Preparative Procedures |
| **ALC: Life-cycle support** | ALC_CMC.1: Labelling of the TOE |
| | ALC_CMS.1: TOE CM Coverage |
| **ATE: Tests** | ATE_IND.1: Independent Testing â€“ Conformance |
| **AVA: Vulnerability assessment** | AVA_VAN.1: Vulnerability Survey |

**Table 3 Assurance Components**

### 5.2.1 Development (ADV)

#### 5.2.1.1 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.

### 5.2.2 Guidance documents (AGD)

#### 5.2.2.1 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 useraccessible 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.

#### 5.2.2.2 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.

### 5.2.3 Life-cycle support (ALC)

#### 5.2.3.1 Labelling 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 labelled 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.

#### 5.2.3.2 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.

### 5.2.4 Tests (ATE)

#### 5.2.4.1 Independent Testing â€“ 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.

### 5.2.5 Vulnerability assessment (AVA)

#### 5.2.5.1 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.

# 6. TOE Summary Specification

This chapter describes the security functions:

- Security audit
- Communication
- Cryptographic support
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

## 6.1 Security audit

The Security audit function satisfies the following security functional requirements:

**NDcPP22e:FAU_GEN.1:**

**WLANASEP10:FAU_GEN.1:**

The TOE is capable of generating log records for a wide range of security relevant and other events as they occur. The events that can cause an audit record to be logged include starting and stopping the audit function, Security Administrator's configuration of CSPs and security functions as well as all of the events identified in Table 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). For example, when the administrator creates, modifies or deletes the cryptographic keys, the key name will be logged in the event to identify the relevant key.

**NDcPP22e:FAU_GEN.2:**

All actions performed by the TOE are associated with a unique identifier such as administrator's user name, wireless client's MAC/IP address and NTP/RADIUS/Log server's IP address. 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.

**NDcPP22e:FAU_STG.3/LocSpace:**

The TOE allows the Security Administrator to configure a threshold number for audit storage warnings. Once the threshold number is reached, the TOE will generate audit logs about this event and optionally sends warning message to the administrator via Email.

**NDcPP22e:FAU_STG.1:**

**NDcPP22e:FAU_STG_EXT.1:**

The TOE stores audit logs locally with up to a fixed size of 256K bytes. Local password based authentication and authorization limits the access to the local audit log records. Only the Security Administrator can gain access to the local audit log records.

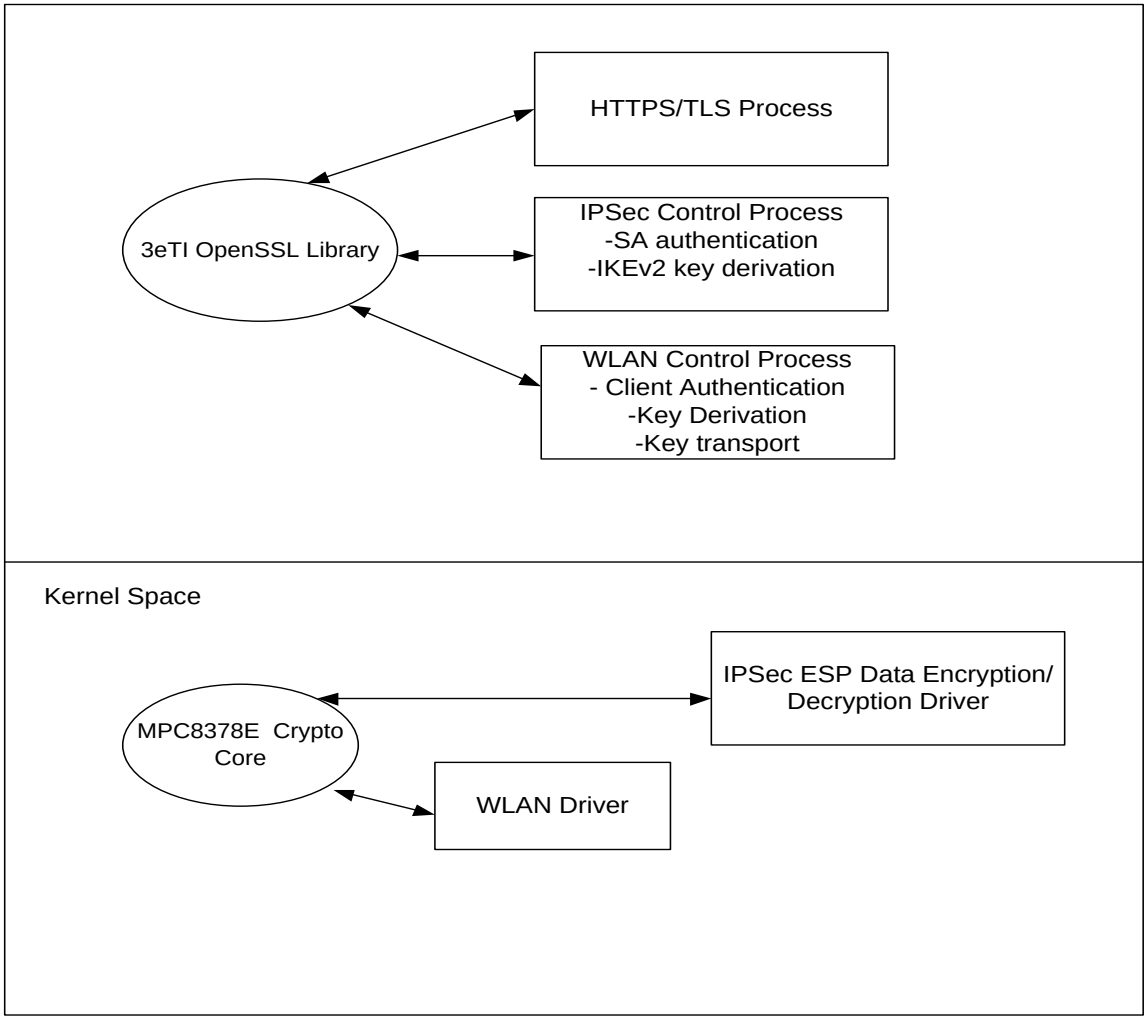
When the TOE is configured to export audit logs to an external SYSLOG server, it simultaneously sends the message to the server and local store. The TOE requires the external audit server and itself to be connected via an IPsec session. The Admin Guide provides details about the "Export Audit Logs" configuration. The TOE exports audit data over IPsec using AES128/256 bit encryption. Disconnection to external entities such as syslog server will result in log of communication error and attempt to re-establish secure channel. At no point, will plaintext be transmitted. The TOE does not implement an automatic synchronization mechanism between the local and remote audit storage.

When the audit log storage space is full, the TOE also provides the Authorized Administrator the option of overwriting "old" audit records rather than preventing auditable events.

## 6.2 Cryptographic support

There are two cryptographic engines within the TOE models as shown in the figure below. All models share the same hardware MPC8378E cryptographic core and OpenSSL library.

**Figure 6-1: 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 module use this library. 3eTI's OpenSSL provides the following cryptographic algorithms: AES, RSA, HMAC, SHS, ECDSA and DRBG.

The 3eTI OpenSSL Library represents not the entire OpenSSL Library, but the FIPS Object Module that is compiled into the larger OpenSSL Library. Because 3eTI has already compiled the FIPS Object Module and then links that same, identical Object Module into different versions of the larger OpenSSL library, the version of the larger OpenSSL Library is not relevant.

There is a FreeScale MPC8378E cryptographic core within the TOE as well. It provides cryptographic functions for the Linux kernel drivers. Wireless client data encryption/decryption functions using AES-CCMP is provided by this engine. IPsec ESP data encryption/decryption using AES-CBC with SHS or AES-GCM is provided by this engine. The MPC8378E cryptographic core provides the following cryptographic algorithms in FIPS mode: AES (CBC, GCM, CCM), HMAC, SHS.

The TOE utilizes version 2.0 of its OpenSSL Algorithm Implementation and version 1.0 of the MPC8378E cryptographic core in firmware version 5.1.0 of the TOE.

**Table 6-4: TOE CAVP Tested Algorithms**

| Algorithm | Cert No. | SFR Mapping |
|---|---|---|
| **3eTI OpenSSL** | | |
| AES (CBC, 128, 256 bits key) | 2060 | FCS_COP.1/DataEncryption |
| AES-KW | 2060 | FCS_CKM.2(3) |
| CVL KAS ECC | 1357 | FCS_CKM.2 |
| ECDSA, KeyPairGen, sign/verify with P256, P384 and P521 | 415<br>303 | FCS_COP.1/SigGen<br>FCS_CKM.1 |
| SHS (SHA-1, SHA-256, SHA-384, SHA-512) | 1801 | FCS_COP.1/Hash |
| HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512) | 1253 | FCS_COP.1/KeyedHash |
| RSA key generation (2048 bits) | 2568 | FCS_CKM.1 |
| RSA sign/verify (2048 bits) | 1491 | FCS_COP.1/SigGen |
| DSA key generation (2048 bits) | 1255 | FCS_CKM.1 |
| DRBG NIST SP800-90 with one independent hardware-based noise source of 256 bits of non-deterministic (CTR_DRBG (AES)) | 822 | FCS_RBG_EXT.1 |
| **MPC8378E Cryptographic Core** | | |
| AES (CBC 128, 256 bits; CCM 128, 256 bits) | 2078 | FCS_COP.1/DataEncryption |
| AES (GCM 128, 256 bits) | 2105 | FCS_COP.1/DataEncryption |
| HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512) | 1259 | FCS_COP.1/KeyedHash |
| SHS (SHA-1, SHA-256, SHA-384, SHA-512) | 1807 | FCS_COP.1/Hash |

As shown in Figure 6.1, the 3eTI OpenSSL library provides cryptographic services to the TOE's application modules. The IPsec module uses the OpenSSL library during the IKEv2 SA authentication and key establishment. The Wireless Access Point module uses the library's cryptographic service during the client's authentication and the IEEE 802.11i 4-way handshake key establishment. The MPC 8378E cryptographic core provides services for fast path data encryption. For IPsec, this module provides the IPsec ESP encryption with AES-GCM or AES-CBC-HMAC-SHS. For WLAN data communication between the TOE and the wireless client, this core provides AES-CCM encryption/decryption service.

**NDcPP22e:FCS_CKM.1:**

The TOE support RSA, DSA, and ECDSA key generation. The key generation is used by the TOE when it creates a Certificate Signing Request (CSR) to apply for a certificate from the Certificate Authority (CA). The TOE enforces the key size of 2048 or greater for RSA and DSA key pairs and supports NIST curves P256, P384 and P521 for ECDSA key pairs. The TOE implements FFC schemes using Diffie-Hellman group 14. The TOE implementation of Diffie-Hellman group 14 (2048 MODP) meets RFC 3526, Section 3. The scheme is used by IPsec IKEv2.

**WLANASEP10:FCS_CKM.1(2):**

The symmetric key of size 128 bits 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 ISO/IEC 18031:2011DRBG random bits generator. 802.11-2012 specified cryptographic key derivation algorithm [PRF-384] is strictly followed by the TOE. The TOE is Wi-Fi Alliance certified (Certification ID: WFA56890) to prove the correctness of key derivation and interoperability between the TOE and other commercial Wi-Fi products.

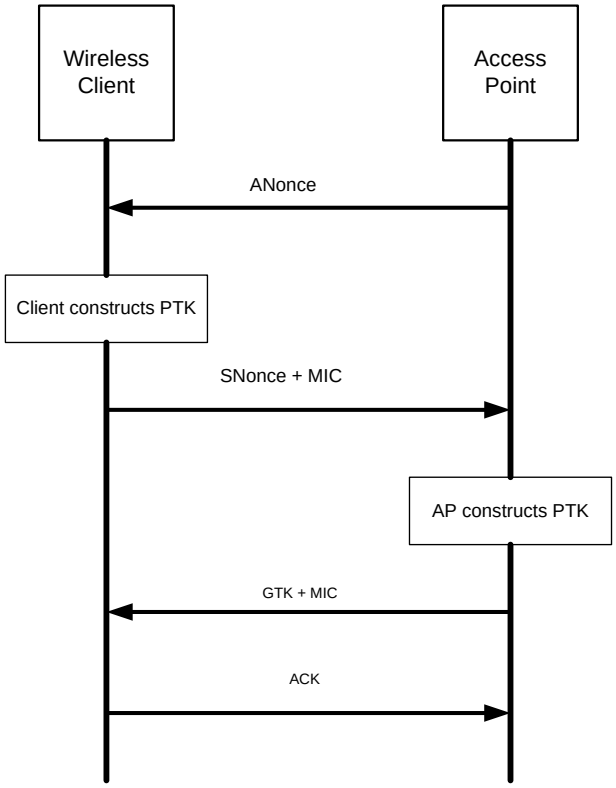
End-to-end wireless encryption between the TOE and the wireless client is implemented using WPA2. The PMK is generated by the RADIUS Server in coordination with the wireless client, encrypted by the IPsec tunnel, and passed

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 6-2 below.

**Figure 6-2: 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 distributes the Group Temporal Key (GTK) by using AES Key Wrap in an EAPOL-Key frame that meets RFC 3394 for AES Key Wrap and 802.11-2012 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.

**NDcPP22e:FCS_CKM.2:**

The TOE acts as both receiver and sender for RSA-based key establishment Diffie-Hellman based and Elliptic Curve Diffie-Hellman (ECDH) key establishment in cryptographic operations.

| Scheme | SFR | Service |
|---|---|---|
| RSA | FCS_TLSS_EXT.1 | Administration, Syslog and NTP |
| Diffie-Hellman | FCS_TLSS_EXT.1 | Administration |
| ECDH | FCS_IPSEC_EXT.1 | Syslog and NTP |
| Diffie-Hellman (Group 14) | FCS_IPSEC_EXT.1 | Syslog and NTP |

.

**WLANASEP10:FCS_CKM.2(2)**

**WLANASEP10:FCS_CKM.2(3):**

The TSF's key material, such as the Pair-wise Master Key (PMK) for Wireless Protected Access (WPA2) is distributed by the 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 protects the PMK from exposure.

The TSF distribute Group Temporal Key (GTK) by using AES Key Wrap in an EAPOL-Key frame that meets NIST SP 800-38F and IEEE 802.11-2012 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 Figure 6-2 illustrates the GTK distribution.
The TOE has a configurable GTK timeout value. At the configured time expiration, the TOE will update each client with the GTK using the AES key wrap mechanism just described.

**NDcPP22e:FCS_CKM.4:**

Table 6- below lists all the keys and CSPs used and managed by the TOE.

**Table 6-2: 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 Security Admin and Admin role operators |
| Firmware verification key | ECDSA public key | Embedded in firmware at compile time. Firmware upgrade is through encrypted | Not output | Plaintext in flash | Zeroized when firmware is upgraded. | Used for firmware digital signature verification |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | (using TLS session key) | | | | |
| 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 |
| **RBG Keys/CSPs** | | | | | | |
| **Key/CSP** | **Type** | **Generation/ Input** | **Output** | **Storage** | **Zeroization** | **Use** |
| DRBG CTR V | 32-byte value | 32 bytes from /dev/random file, /dev/random is populated by hardware noise generator | Not output | Plaintext in RAM | Zeroized every time a new random number is generated using the FIPS DRBG after it is used. | Used as CTR V value for FIPS DRBG. |
| DRBG CTR Key | 32-byte value | 32 bytes from /dev/random file, /dev/random is populated by hardware noise generator | Not output | Plaintext in RAM | Zeroized every time a new random number is generated using the FIPS DRBG after it is used. | Used as CTR key for FIPS 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 Security Admin and Admin TLS/HTTPS interfaces. |
| TLS session key for encryption | AES (128/256) | Not input, derived using TLS protocol | Not output | Plaintext in RAM | Zeroized when a page of the web UI is served after it is used. | Used to protect TLS/HTTPS session. |
| **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 |
| **IPsec Keys** | | | | | | |
| DH Private Key | 2048 bits private key | Generated | Not output | Plaintext in RAM | Zeroized when no | IKE v2 SA setup |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | longer used | |
| 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), 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_GCM (128, 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 GMK) | Output encrypted (using KEK) | Plaintext in RAM | Zeroized when local antennae 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 | 802.11i GTK |

The zeroization technique is to write all 0xa5, then 0x5a, 0xff and finally all zeros to the memory location where the key is stored in non-volatile storage. A read-verify is performed after the zeroization. The technique is implemented in the firmware that uses Linux file system APIs. The TOE does not store keys in EEPROM. For keys stored in RAM, a single overwrite of all zeroes is performed. IPsec authentication certificate's private keys are encrypted with the corresponding private key passwords. The passwords are stored as plain text in flash and they are zeroized the same way as described above.

**WLANASEP10:FCS_COP.1(1):**

**NDcPP22e:FCS_COP.1/DataEncryption:**

AES is implemented with key sizes of 128, and 256 bits in Cipher Block Chaining (CBC) mode and Galois Counter Mode (GCM) and 128 bits in CCMP mode. 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 the TOE's TLS interface, AES_CBC with 128 or 256 bits key is used. 3eTI's MPC8378E Cryptographic Core provides AES_GCM and AES_CBC services for IPsec data encryption. 128 and 256 bits keys are supported. AES_CCM with 128 bits is provided by the MPC8378E core for WLAN data packets encryption/decryption.

Table 6-1 lists the AES mode and key sizes; all AES algorithm implementations are NIST CAVP validated.

**NDcPP22e:FCS_COP.1/Hash:**

The TSF supports SHA-1, SHA-256, SHA-384, and SHA-512 for secure hashing. See Table 6-1 for details. The security hashing functions are used in IPsec IKEv2 and ESP to provide data packet integrity.

**NDcPP22e:FCS_COP.1/KeyedHash:**

The TOE's OpenSSL Library and the MPC8378E cryptographic core both implement HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512, keyed-hash message authentication supporting digest sizes: 160, 256, 384, and 512 bits and key size of 160 bits, 256 bits, 384 and 512 bits implemented to meet ISO/IEC 9797-

2:2011, Section 7 “MAC Algorithm 2. The block size is 512 bits for HMAC-SHA-1, HMAC-SHA-256 and 1024 bits for HMAC-SHA-384, and HMAC-SHA-512 and the output size is the same as the underlying hash function.

**NDcPP22e:FCS_COP.1/SigGen:**

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 RSA (2048 bits) or ECDSA with key size 256, 384, and 521 bits using NIST curve P256, P384 and P521 certificate for IPsec SA authentication. Table 6-1 lists RSA and ECDSA CAVP validation certificate numbers.

**NDcPP22e:FCS_HTTPS_EXT.1:**

The Web UI with remote administration station is always TLS/HTTPS. The HTTPS implementation is fully compliant with RFC 2818. The TOE acts as an HTTPS server and waits for client connections 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.

**NDcPP22e:FCS_IPSEC_EXT.1:**

The TOE implements IPsec protocol in full compliance with IETF RFCs as specified by NDcPP22e. Within the TOE, the NTP client uses an IPsec tunnel for communications with an NTP server. The TOE uses IPsec to protect communications with the remote log server as well.

The TOE supports IKEv2 only as defined by RFCs 5996 and always attempts NAT traversal, hence an administrator need not configure either. During the Security Association (SA) setup phase, the TOE supports the following DH groups:

- ecp384
- ecp256
- modp2048

If the administrator selects “auto negotiation” from IPsec “Cipher Suites” configuration Web UI, then the groups listed above will be send to the IPsec peer during the IKEv2 negotiation. If “Suite B GCM128” is selected, then the TOE will use ecp256 group. If “Suite B GCM256” is selected, then the TOE will use ecp384 group.

The TOE chooses and enforces the group and AES cipher to make sure that the SA confidentiality strength is equivalent or greater than the configured ESP confidentiality strength. For example, the TOE (when configured for “Auto Negotiation”) will reject any ESP proposal with an AES key length greater than the negotiated IKE AES key length. Similarly, administrator selection of “Suite B GCM128” or similar ciphers ensure the TOE will enforce a single, prescribed set of modes to make sure that the parents IPsec SA confidentiality strength is equal or greater than the child SA’s strength.

| **Mode** | **IKE (openssl library)** | | | | **ESP (Hardware encryption)** | |
|---|---|---|---|---|---|---|
| | **Encryption** | **Integrity** | **Pseudo Random Function** | **DH Group** | **Encryption** | **Integrity (where applicable)** |
| Suite B GCM 128 | aes128cbc | sha256 | sha256 | ecp256 | aes128gcm128 | - |

The TOE uses ISO/IEC 18031:2011 DRBG to generate the nonce and “x” in each DH group with lengths of 112 (for DH group 14), 128 (for DH group 19 and 192 (for DH group 20). 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-128

SHA-512, SHA-384, SHA-256 and SHA1 are used to provide payload data integrity. X.509 certificates with rDSA 2048 bits or larger key or ECDSA 256, 384, and 521 bits key with NIST P256, P384 and P521 are used for IPsec tunnel authentication with its peer.

The TOE supports IPsec tunnel mode and transport mode which allows the payload of packets to be encrypted. The TOE requires no administrative configuration and negotiates either depending on the peer. The TOE uses IPsec standard encapsulating Security Payload (ESP) protocol to provide authentication, encryption and anti-replay services. It uses the following ciphers to encrypt the IPsec data payload:

1. GCM mode with Nonce length of 128, 96 and 64 bits
   - AES-GCM-128
   - AES-GCM-256
2. CBC mode with HMAC-SHA-512, HMAC-SHA-384, HMAC-SHA-256 and HMAC-SHA1 as integrity
   - AES-CBC-128
   - AES-CBC-256

If the administrator chooses “Auto Negotiation” for IPsec, the TOE will send cipher list ranked with the highest security first to its peer. For example, the IKE integrity list will be sent as: SHA-512, SHA-384, SHA-256 and SHA1. It’s expected that the peer will pick the strongest one it could support. There is no need to explicitly configure security hashing functions in the IPsec configuration.

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.

The TOE allows the Security Administrator to configure the IKEv2 SA and child SA lifetime by minutes (20-1440, default 180) and the TOE additionally allows the Administrator to configure child SA lifetime by number of bytes (90 to 2047Kb, 0 for unlimited) or by number of data packets (192 to 2097151K, 0 for unlimited).

The TOE supports X.509 certificate for IPsec mutual authentication. RSA certificate with 2048 bits, ECDSA certificates with 256, 384, and 521 bits key is supported implementing NIST curves P256, P384 and P521. When certificates are used for authentication, the Distinguished Name (DN), IP Address and Fully Qualified Domain Name (FQDN) are verified to ensure the certificate is valid and is from a valid entity. These reference identifiers in the certificate are compared with the expected reference identifiers (as specified by an administrator) and deemed valid if the attribute types are the same and the values are the same and as expected.

The TOE can be configured to use pre-shared key for IPsec authentication as well. The security administrator first selects “Pre-Shared Key” under “Authentication” when configuring the IPsec tunnel via the Web UI, then enters the pre-shared key manually.

The TOE’s IPsec Security Policy Database (SPD) is dynamically configured based upon the trusted paths IPsec is used to protect. For example, the TOE uses IPsec to protect a remote syslog trusted path. In this instance, records are written into the SPD to protect packets passing between the TOE and the remote syslog server based on source address, destination address, protocol and port number. When protecting remote syslog trusted path, the SPD will have record matching ingress UDP traffic with source address and port corresponding to the remote syslog server. Additionally, the SPD will have record matching egress traffic with destination address and port corresponding to the remote syslog server. Traffic passing through the security boundary and matching either of these two records will be classified as “PROTECTED” using IPsec transport mode. Traffic that does not match any records in the SPD but does match the local firewall access list will be allows to “BYPASS” the security boundary unperturbed. Traffic

that does not match any records in the SPD will be "DISCARDED". Additional records are written into the SPD when additional trusted paths are configured for IPsec protection (i.e. remote audit log, NTP and RADIUS server).

**NDcPP22e:FCS_NTP_EXT.1:**

The TOE has a running NTP daemon to synchronize the local time with an external NTP server. The NTP daemon supports NTP v4 (RFC 5905). IPsec tunnel is setup between the TOE and NTP server to protect the integrity and privacy of the time source.

**NDcPP22e:FCS_RBG_EXT.1:**

The TOE implements RBG as defined ISO/IEC 18031:2011 using CTR_DRBG (AES). The entropy source is a 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 reads 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.

**NDcPP22e:FCS_TLSS_EXT.1:**

The TOE's HTTPS server supports TLS version 1.2 only and will deny connection requests from TLS clients with a lower version. It supports 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 username and passwords. If the failure count reaches the configured threshold, the TLS/HTTPS session will be terminated by the TLS/HTTPS server. The Diffie-Hellman group 14 with parameters of size 2048 bits is used for the key agreement.

## 6.3 Identification and authentication

The Identification and authentication function satisfies the following security functional requirements:

**WLANASEP10:FIA_8021X_EXT.1:**

When a wireless user attempts to associate to a given network, they must first associate with an Access Point (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 TOE. The TOE functions as Authenticator

as defined by 802.1X-2010. The TOE strictly follows the port-based network control model as defined in section 7.1 of 802.1X-2010.

Once the wireless client and the TOE have negotiated the required security methods, the authentication phase of the process is initiated. The TOE acts as 802.1X authenticator and provides remote EAP-TLS authentication pass through to the RADIUS server. The TOE implements the Authenticator's state machine and counters as defined in section 8.9 & 8.10 of 802.1X-2010. The TOE's authenticator module strictly enforces EAPOL PDU format as defined in section 11 of 802.1X-2010. The TOE's authenticator implementation uses all 8021.X-2010 mandatory definitions. No optional or non-conformance definitions of 802.1X are implemented. The TOE is Wi-Fi Alliance certified for WPA2 interoperability. The interoperability tests include many EAP methods, among which EAP-TLS is included.

The TOE establishes IPsec tunnel with the RADIUS server to protect the EAPOL data packets between itself and the RADIUS server. The IPsec tunnel is also used to protect the PMK sent by the RADIUS server as part of RADIUS Access-Accept message. During this 802.1x authentication state, the TOE 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.

**NDcPP22e:FIA_AFL.1-:**

**WLANASEP10:FIA_AFL.1:**

For an administrator's remote authentication attempt, if the administrator's authentication fails, the TOE's failure counter will be incremented. Once the failure counter reaches the configured threshold, the TOE's HTTPS server will refuse connection from this end point for an administrator. The authentication failure threshold is configurable by an authorized security administrator with a maximum value of 8, the default value is 3. Once a connection is refused, the administrator would have to re-login after the configurable lockout time period has elapsed, at which point the login failure counter would be reset to 0 by then. The default lockout period is 10 minutes and is configurable between ranges of 0-90 minutes.

In order to ensure that remote administrator authentication failures do not lead to a situation where no administrator access is available, an administrator account with local access can be configured. When the administrator authenticates to the TOE via local management port, the TOE only checks for username and password regardless of the account status (locked or expired) so administrator can't get locked out through the local port.

**NDcPP22e:FIA_PMG_EXT.1:**
The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and the following special characters: ***'!',*** *'@', '#', '$', '%', '^', '&', '*', '(' , ')'* . Minimum password length is settable by the Authorized Administrator and can be configured for minimum password lengths of 8 to 30 characters. Additionally, the TOE supports password lengths up to 32 characters long. The TOE will truncate passwords that are longer than 32 characters when creating a user or changing passwords for an existing user.

**WLANASEP10:FIA_PSK_EXT.1:**

The TOE uses pre-shared keys for IPsec. The TOE accepts IPsec PSK keys between 16 and 32 characters in length. The TOE also supports PSK for wireless client authentication. The pre-shared key for wireless client is between 8 and 63 characters. The pre-shared keys must be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"). Note that the '&' character is not supported for WPA2 pre-shared keys, but it is supported for IPsec pre-shared keys.

For IPsec, the TOE conditions the text-based pre-shared keys using the SHA-1, SHA-256, and SHA-384 hash algorithm and can accept bit based pre-shared keys. For WPA2, the TOE only accepts text based PSKs that are transformed into bit-based PSKs. Text-based keys are conditioned using PBKDF2, as specified in 802.11i.

**WLANASEP10:FIA_UAU.6:**

An administrative user is required to re-authenticate when he/she changes password, and following a TSF-initiated locking as described in any of the FTA_SSL requirements in this ST.

**NDcPP22e:FIA_UAU.7:**

When a user is entering their password information, the password is obscured such that no observer could read the password off the screen.

**NDcPP22e:FIA_UAU_EXT.2:**

**NDcPP22e:FIA_UIA_EXT.1:**

The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed except for the login banner that is displayed prior to user authentication and any network packets as configured by the authorized administrator may flow through the TOE.

The administrator logs on the TOE through either dedicated local Ethernet port or over WAN Ethernet port to access the Web UI. The Web UI is accessible over HTTPS only and the TOE supports TLS 1.2. There is no local access such as a serial console port. A local protected network must be established for local connections.

A successful authentication is determined by a successful username and password combination after the HTTPS connection. An incorrect password will result in a failed authentication attempt. The TOE does not provide a reason for failure in the cases of a login failure. The TOE supports local authentication using a local user database.

**NDcPP22e:FIA_X509_EXT.1/Rev:**

**NDcPP22e:FIA_X509_EXT.2:**

**NDcPP22e:FIA_X509_EXT.3:**

The TOE uses X.509 certificates for IPsec authentications. The TOE can be configured with the certificates and their corresponding private key by security administrator or by creating CSRs and importing the CA signed CSRs to the TOE. The security administrator can load and delete certificates for usage of IPsec authentication, load and delete CAs, intermediated CAs and CRLs. Certificates are validated as part of the authentication process when they are presented to the TOE and when they are loaded into the TOE. The TOE checks that the basicConstraints extension and CA flag are set to TRUE for all CA certificates before their acceptance. During the IPsec authentication using X509 certificate, the TOE develops a certificate path from a trust anchor configured by security administrator which is fully compliant with RFC 5280. When a certificate chain is received from a peer, the TOE processes the certificate chain path until the first trusted certificate, or trust point, is reached. The TOE uses CRL that have been preloaded by the administrator to validate the peer certificates, and the TOE will accept as valid, a certificate for which the administrator has not loaded a CRL. Failure by the TOE to establish the certification path to a trust anchor will lead to the successful establishment of this IPsec trusted channel.

The TOE allows the security administrator to view the certificates and CAs. The TOE's Web UI will display the certificates' name, subject name, issuer name, valid-start date, expiration date.

## 6.4 Security management

The Security management function satisfies the following security functional requirements:

**NDcPP22e:FMT_MOF.1/Functions:**

**NDcPP22e:FMT_MOF.1/Services:**

**NDcPP22e:FMT_MTD.1/CoreData:**

**NDcPP22e:FMT_MTD.1/CryptoKeys:**

**NDcPP22e:FMT_SMF.1:**

**NDcPP22e:FMT_SMR.2:**

The Web Management Application over HTTP/TLS provides capabilities for the authorized administrator to manage cryptographic, audit, and authentication functions and data. The Web Management Application also provides the interfaces for the authorized administrator to start and stop the IPsec and Wireless Access Mode services (details of the configuration are in the Admin Guide).

The TOE provides three roles: Security Administrator, Non-security Administrator, and user (Peer Device). Security Administrator and Administrator can only access the TOE through Web Application through TLS/HTTPS. Upon successful authentication with the TOE, the Security Administrator can manage TSF data as shown in the table below.

**Table 6-5: Management of TSF Data**

| Service and Purpose | Details | Security Administrator (referred to as Crypto officer in guidance) | Non-Security 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. Configure email if audit log is full. | X | |
| Key zeroization via reboot | | 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 | |
| HTTPS Management | Load HTTPS server certificate and private key. | X | |
| Key Generation | Create asymmetric key pairs and X509v3 Certificate Signing Request. | X | X |

No GUI interfaces are accessible to the user prior to authentication. The TOE enforces authentication then enables the TSF data configuration interfaces. The Non-security administrators have no access to those TSF data configuration interfaces.

**WLANASEP10:FMT_SMR.1:**

By default, the TOE disallows wireless client devices to access the TOE's Web UI interface. For each wireless client that successfully authenticates with the TOE and obtains an IP address, the TOE will use its MAC address and IP address to build an entry in the TOE's access table to disallow the client's access to the TOE's Web UI.

## 6.5 Protection of the TSF

**NDcPP22e:FPT_APW_EXT.1:**

**NDcPP22e:FPT_SKP_EXT.1:**

The authentication passwords are stored in PKCS5 format in the TOE. All other CSPs are stored in encrypted format in the TOE on non-volatile memory. The file system that holds the hashed password and encrypted CSPs are made read-only during runtime to avoid data corruption. None of the files or CSPs are available through any external interfaces to users/administrators. The Web UI allows the security administrator to input keys/passwords to the TOE with no output capabilities.

**NDcPP22e:FPT_STM_EXT.1:**

The TOE has a running NTP daemon to synchronize the local time with an external NTP server. An 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.

**WLANASEP10:FPT_FLS.1:**

**NDcPP22e:FPT_TST_EXT.1:**

**WLANASEP10:FPT_TST_EXT:**

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 or at security administrator's request 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_GCM encrypt/decrypt KAT
- AES_CCM encrypt/decrypt KAT
- SHA-1, SHA256, SHA384, SHA512 KAT
- HMAC SHA-1, SHA256, SHA384, SHA512 KAT

3eTI OpenSSL library Power-on self-tests:

- HMAC SHA-1, SHA256, SHA384, SHA512 KAT
- SHA-1, SHA256, SHA384, SHA512 KAT
- FIPS 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 the device is powered on, the first thing done by the bootloader is to check its own integrity. If the integrity is broken, the firmware won't boot. Firmware integrity is performed at firmware boot up. Both firmware and bootloader are digitally signed with ECDSA. These tests are sufficient to demonstrate the TOE has not been corrupted and its cryptographic functions are operating properly.

**NDcPP22e:FPT_TUD_EXT.1:**

Security Administrators can query the currently active TOE version via the Web UI by going to the System Administration -> Help screen. When a new version of firmware is released, the customers are notified by 3eTI's customer service department, normally via e-mail. If a customer desires to get a copy of the new firmware, the customer will be provided with an URL link to the secured download site together with a onetime valid username and password.

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 device'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.

## 6.6 TOE access

**NDcPP22e:FTA_SSL.3:**

**NDcPP22e:FTA_SSL.4:**

**NDcPP22e:FTA_SSL_EXT.1:**

The Web UI 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 UI 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. The administrator can log out of the TOE by clicking on the Logout button. The TOE returns the user back to the login screen. That essentially terminates the session.

**NDcPP22e:FTA_TAB.1:**

The Web UI displays a customizable TOE access banner to the remote/local administrative user before the user can log into the system.

**WLANASEP10:FTA_TSE.1:**

The TOE implements wireless client MAC address filtering functions. The security administrator can specify white list (allow) or black list (deny) or both. The list's attributes are client WiFi MAC address, time (hour, minute, and second) 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 Basic Service Set (BSS).

## 6.7 Trusted path/channels

**NDcPP22e:FTP_ITC.1:**

**WLANASEP10:FTP_ITC.1:**

The TOE provides 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. The TOE establishes WPA2 with 802.1x EAP-TLS connections with wireless clients and uses IPsec for communications with authentication servers.

**NDcPP22e:FTP_TRP.1/Admin:**

All remote administrative communications take place over a secure encrypted TLS session. The HTTPS/TLS implementation allows web browser clients to connect to the TOE's HTTPS server. The remote users are able to initiate TLS communications with the TOE.