3e Technologies International

Wireless Network Access System

Security Target

22000225-701

Revision B

July 21, 2011

Version 2.0

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

Document ID Number: 22000225-701 Revision B

Contact:

3e Technologies International, Inc.

9715 Key West Avenue

5th Floor

Rockville, MD 20850 USA

Telephone: +1 (301) 670-6779

Fax: +1 (301) 670-6989

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

Email: mailto:info@3eti.com

Table of Contents

List of Tables and Figures

1 Security Target Introduction

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

1.1 Security Target References

ST Title: 3eTI Wireless Network Access System Security Target

ST Version: Revision 2.0

Vendor: 3e Technology International, Inc.

ST Publication Date: July 21, 2011

Keywords: Access system, authentication server, radio, RADIUS server, wireless, network, wireless local area network, wireless LAN, WLAN, 802.1X, 802.11

1.1.1 Document References

The following documents were used to develop the Security Target.

Table 1-1: US Government and Standards Document References

Reference	Document
[CC_PART1]	Common Criteria for Information Technology Security Evaluation-Part 1: Introduction and general model, July 2009, version 3.1R3, CCMB-2006-09-01
[CC_PART2]	Common Criteria for Information Technology Security Evaluation-Part 2: Security functional components, July 2009, version 3.1R3, CCMB-2007-09-02
[CC_PART3]	Common Criteria for Information Technology Security Evaluation-Part 2: Security assurance components, July 2009, version 3.1R3, CCMB-2007-09-03
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, version 3.1R3, CCMB-2007-09-004
[WLANPP]	US Government, Wireless Local Area Network (WLAN) Access System, Protection Profile for Basic Robustness Environments, July 25, 2007, Version 1.1
[PKE PP]	US Government Family of Protection Profiles: Public Key-Enabled Applications for Basic Robustness Environments, May 1 2007, Version 2.8
[FIPS PUB 140-2]	National Institute of Standards and Technology, FIPS PUB 140-2 Security Requirements for Cryptographic Modules, December 2002.
[FIPS PUB 186-3	Digital Signature Standard (DSS), June 2009
[NIST SP 800-56A]	NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”
[NIST SP 800-57]	NIST Special Publication 800-57, “Recommendation for Key Management”
[NIST SP 800-120]	NIST Special Publication 800-120, Recommendation for EAP Methods Used in Wireless Network Access Authentication, September 2009.
[IEEE 802.1X]	IEEE 802.1X-2004, “Standard for Local and metropolitan area networks, Port-Based Network Access Control, 2004
[IEEE 802.11]	IEEE 802.11-2007; Standard for Information Technology: Telecommunications and information exchange between systems: Local and metropolitan area networks: Specific requirements: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 802.11, March 2007
RFC 2865	Remote Authentication Dial In User Service (RADIUS), June 2000
RFC 3394	Advanced Encryption Standard (AES) Key Wrap Algorithm
RFC 5216	The EAP-TLS Authentication Protocol, March 2008

Table 1-2: 3eTI Document References

Reference	Document
AP UG	3e Technologies International Inc., AirGuard™ Wireless Access Point User's Guide, June 2008
[AP FSP]	EF Johnson Technology Inc., 3e-525/523 Access Points: Functional Specification and Software Security Architecture Document
[AP Authenticator DD]	3e Technologies International Inc, CC 802.1X Authenticator Design, 2010-Mar-31
[AP-523 FIPS]	3e Technologies International Inc., FIPS 140-2 Non-Proprietary Security Policy; Level 2 Validation; 3e-523-F2 & 3e-523-3 Secure Multi-function Wireless Data Points; HW Versions 1.0, 1.1, 1.2, 2.0; FW Versions 4.3.2 (to be updated)
[AP-525 FIPS]	TBD
[SS UG]	3e Technologies International, Inc.,3e-030-02 Security Server Version 4.0 Preliminary User's Guide, April 2010
[SS SRS]	3e Technologies International Inc., 3eTI Software Requirements Specification, 10123.001.03.11.01, 22 Feb 2010.
[SS FIPS]	3e Technologies International Inc., FIPS 140-2 Non-Proprietary Security Policy; 3e-030-2,Security Server Cryptographic Core (Version 4.0) (to be updated)

1.2 TOE References

TOE Identification: 3eTIAirguard™ Wireless Network Access System.

The TOE consists of the following products:

- 3e-525A-3 Access Point; Hardware Version 2.0(A) and 2.1, Firmware Version 4.4.0.00.80
- 3e-525A-3EP Access Point; Hardware Version 2.1, Firmware Version 4.4.0.00.80
- 3e-525A-3MP Access Point; Hardware Version 2.0(A) and 2.1, Firmware Version 4.4.0.00.80
- 3e-525V-3 Access Point; hardware version 2.0(A) and 2.1, Firmware Version 4.4.0.00.80
- 3e-525VE-4 Access Point; hardware version 2.0(A) and 2.1, firmware version 4.4.0.00.80
- 3e-523-F2 Access Point; hardware version 1.0, 1,1, 1.2, and 2.0; firmware version 4.4.0.00.70
- 3e-523-3 Access Point, hardware version 1.0, 1,1, 1.2, and 2.0; firmware version 4.4.0.00.70
- 3e-030-2 Security Server; software version 4.0.0.00.24

1.3 TOE Overview

The Target of Evaluation (TOE) includes the following 3eTI Airguard™ wireless LAN Access Points models: 3e-525A-3, 3e-525A-3EP, 3e-525A-3MP, 3e-525V-3, 3e-525VE-4, 3e-523-F2 and 3e-523-3. Differences between models are limited to enclosure, power options and the extra video components. All Access Points are ruggedized for use in industrial and external environments.

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

Table 1-3 3eTI Access Point Products Comparison

Model	Number of Radio	Radio Mode	Video Support	Comments
3e-525A-3	2	Access Point and Bridge	NO	
3e-525A-3EP	2	Access Point and Bridge	NO	Same as A-3 except higher power radio
3e-525A-3MP	2	Access Point and Bridge	NO	Same as A-3 except using mobile power adapter instead of Power of Ethernet adapter
3e-525V-3	2	Access Point and Bridge	YES	Same as A-3 with extra vedio board
3e-525VE-4	2	Access Point and Bridge	YES	Same as V-3 with a vedio board from different vendor
3e-523-3	1	Access Point or Bridge	NO	With ruggedized enclosure
3e-523-F2	1	Access Point or Bridge	NO	Same as 523-3, different enclosure

The TOE also includes the software-only 3e-030-2 Security Server component.

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

There are two evaluated configurations of the TOE:

1) **Access Point(s) and 3eTI Security Server:** This configuration includes the 3eTI Security Server component, which serves as the Authentication Server for TOE. This is the primary evaluated configuration.
2) **Access Point(s) only**: In this configuration, the 3eTI Security Server is not included, and the TOE relies upon an Authentication Server in the Operational Environment.

This ST claims conformance to the US Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007.

The TOE is evaluated at Evaluation Assurance Level (EAL) 4 augmented by ALC_FLR.2 Flaw reporting procedures.

1.3.1 Type of TOE

The TOE is a wireless LAN access system that performs 802.1X authentication of wireless clients.

This ST claims conformance to the US Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007.

1.3.2 Hardware, Firmware, and Software Required by the TOE

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

The TOE also includes the software only 3eTI 3e-030-2 Security Server.

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

- **Security Server Platform:** The platform for the software-only 3eTI Security Server is a standard Intel-based computer running a Linux or UNIX operating system.
- **RADIUS Server:** If the 3eTI Security Server is not included in the configuration, the TOE requires a RADIUS Server in the Operational Environment for authentication.
- **Wireless Clients:** All wireless client hosts connecting to the wired network from the wireless network.
- **Administrator Workstations:** Trusted administrators access the TOE through the HTTPS protocol.
- **Audit Servers:** The TOE relies upon the audit server for storage of audit records
- **NTP Servers:** The TOE relies upon an NTP server to provide reliable time

1.4 TOE Description

1.4.1 Acronyms

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

Table 1-4: Acronyms

Acronym	Definition
AES	Advanced Encryption Standard

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

Acronym	Definition
OTA	Over the Air
PKI	Public Key Infrastructure
PMK	Pairwise Master Keys
PP	Protection Profile
PSK	Pre-shared key
PSP	Public Security Parameter
PTK	Pair-wise Transient Key
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
RFC	Request for Comments
RSA	Rivest, Shamir, and Adleman
RSTP	Rapid Spanning Tree Protocol
SAR	Security Assurance Requirement
SDRAM	Synchronous Dynamic Random Access Memory
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA-1	US Secure Hash Algorithm 1
SIM	Subscriber Identify Module
SNMP	Simple Network Management Protocol
SOF	Strength of Function
SP	Security Parameter
SSID	Session Set ID
ST	Security Target
TCP	Transmission Control Protocol
TK	Temporal Key
TLS	Transport Layer Security
TOE	Target of Evaluation
TOI	Time of Interest (used in certificate processing)
TSF	TOE Security Function
TSP	TOE Security Policy
TTLS	Tunneled Transport Layer Security
UDP	User Datagram Protocol
WAN	Wide Area Network
WAP	Wireless Access Point
Wi-Fi	Wireless fidelity
WLAN	Wireless Local Area Network
WMM	Wi-Fi Multimedia
WPA2	Wi-Fi Protected Access Version 2

1.4.2 Terminology

The following terminology is used in the Security Target:

Table 1-5: Terms

Term	Definition
802.1X	The IEEE 802.1X standard provides a framework for many authentication types at the link layer.

Term	Definition
EAP	Extensible Authentication Protocol (EAP). It is a protocol that supports the communication of other authentication protocols. EAP uses its own start and end message to carry third-party messages between supplicants and an authentication server.
EAP-TLS	EAP-TLS (RFC 5216) stands for Extensible Authentication Protocol-Transport Layers Security. Transport Layer Security (TLS) provides a mechanism to use certificates for mutual authentication, integrity-protected cipher-suite negotiation, and key exchange between two endpoints.
Wireless Client	A device consisting of hardware and software used to provide a wirelessly interface to communicate with other wireless devices as defined by IEEE 802.11 STA behavior.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

1.4.3 TOE Description

The Target of Evaluation (TOE) is a system of wireless LAN Access Point products that includes one or more 3e-525A-3, 3e-525A-3EP, 3e-525A-3MP, 3e-525-V-3, 3e-525VE-4, 3e-523-F2 and 3e-523-3 Access Points (APs) and the optional 3eTI Security Server.

There are two evaluated configurations of the TOE:

1. **Access Point(s) and 3eTI Security Server:** In this configuration, the 3eTI Security Server is included, which serves as the Authentication Server for the TOE. This is the primary configuration of the TOE.
2. **Access Point(s) only**: In this configuration, the TOE does not include the 3eIT Security Server, and the TOE relies upon an Authentication Server in the Operational Environment.

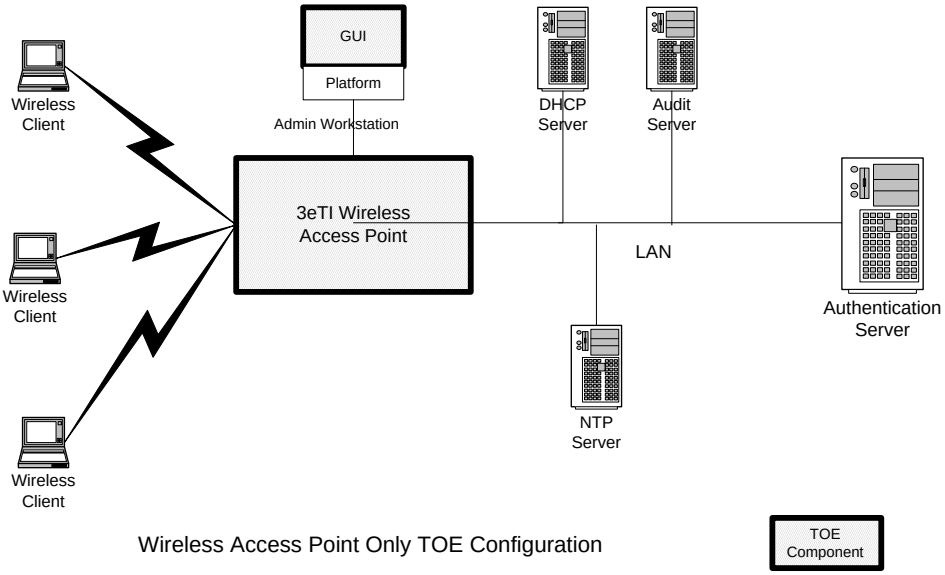
The Access Points require that a wireless client be authenticated before accessing the network and provides data encryption/decryption and integrity protection between the wireless link and the wired LAN. All Access Points are ruggedized devices intended for use in industrial and outdoor environments.

The 3eTI Security Server performs the Authentication Server (AS) function identified by IEEE 802.1x. The role of the AS is to verify the credentials of a wireless client known as the supplicant before the client is granted access to the network.

Figure 1-1 and Figure 1-2 below depict the two configurations of the TOE in their Operational Environments.

Figure 1-1 depicts an Access Point only TOE that relies upon an external RADIUS Authentication Server, an NTP Server and an Audit Server in its Operational Environment. The TOE may also be configured to interface with DHCP and SNMP Management Servers in the Operational Environment, but does not depend upon them to support its security functionality.

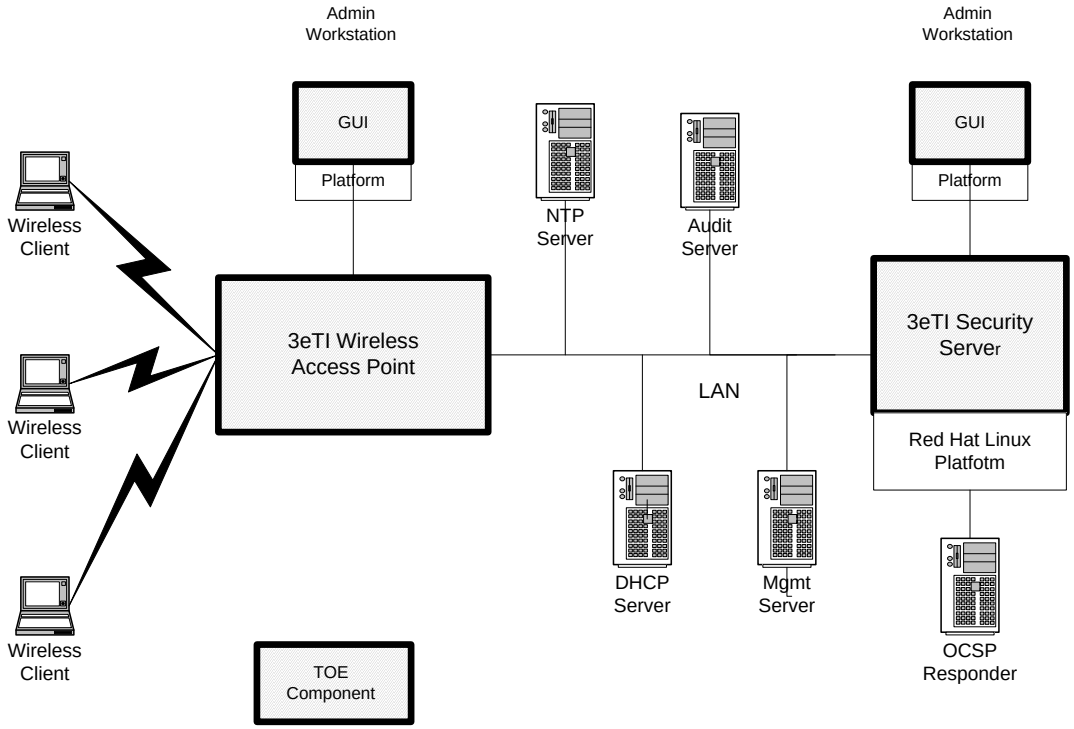
Figure 1-1: Wireless Access Point Only TOE Configuration



Wireless Access Point Only TOE Configuration

Figure 1-2 depicts a configuration of the TOE that includes the 3eTI Security Server. The 3eTI Security Server is installed on a Linux platform. The Security Server communicates with a Lightweight Directory Access Protocol (LDAP) Server to download CA certificates and Certificate Revocation Lists. If so configured, the Security Server can communicate with an Online Certificate Status Protocol (OCSP) Responder to determine if a user's certificate is still valid. The TOE also relies upon a NTP Server and Audit Server in the Operational Environment. The TOE may also be configured to interface with DHCP and SNMP Management Servers in the Operational Environment, but does not depend upon them to support its security functionality.

Figure 1-2: TOE Configuration with 3eTI Security Server



TOE Configuration with 3eTI Security Server

The sections below describe the components of the TOE:

1.4.4 Wireless Access Point (AP) TOE Component

The 3eTI 3e-525A-3, 3e-525A-3EP, 3e-525A-3MP, 3e-525V-3, 3e-525VE-4, 3e-523-F2 and 3e-523-3 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 also communicate among themselves through the secured channel.

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

Wireless communications between clients and APs are carried out using the IEEE 802.11 protocol standard. The 802.11 standard governs communication transmission for wireless devices. For this evaluation, the APs use 802.11a, 802.11b, and 802.11g 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 encryption algorithm must be set to AES_CCM in the evaluated configuration.

The APs have one or more RF interfaces and one or more Ethernet interfaces. All these interfaces are controlled by the software executing on the AP. The Access Points included in the TOE vary by the number of RF and Ethernet interfaces, antenna support and may or may not

contain an extra video board component; however the differences do not affect the security functionality claimed by the TOE.

The AP maintains a security domain containing all hardware and software of the appliance for its own execution. The AP maintains 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 AP. The AP provides 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 AP controls the actions and the manner in which external users may interact with its external interfaces. Thus the AP ensures 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 AP.

Wi-Fi Interoperability Certification

The 3e-523-3 and the 3e-525A-3 Access Points both completed their Wi-Fi Alliances certifications on in January 2010. The Wi-Fi Certification ID for the 3e-523-3 is WFA8556 and the Wi-Fi Certification ID for the 3e-525A-3 is WFA8557. They were both certified for the following IEEE standards:

- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11d

And the following Security:

- WPA™ - Enterprise, Personal
- WPA2™ - Enterprise, Personal
- EAP Type(s)
    - EAP-TLS
    - EAP-TTLS/MSCHAPv2
    - PEAPv0/EAP-MSCHAPv2
    - PEAPv1/EAP-GTC
    - EAP-SIM
    - EAP-AKA
    - EAP-FAST

The certificates may be viewed on the Wi-Fi website using the following links:

- http://certifications.wi-fi.org/pdf_certificate.php?cid=WFA8556
- http://certifications.wi-fi.org/pdf_certificate.php?cid=WFA8557

AP Hardware

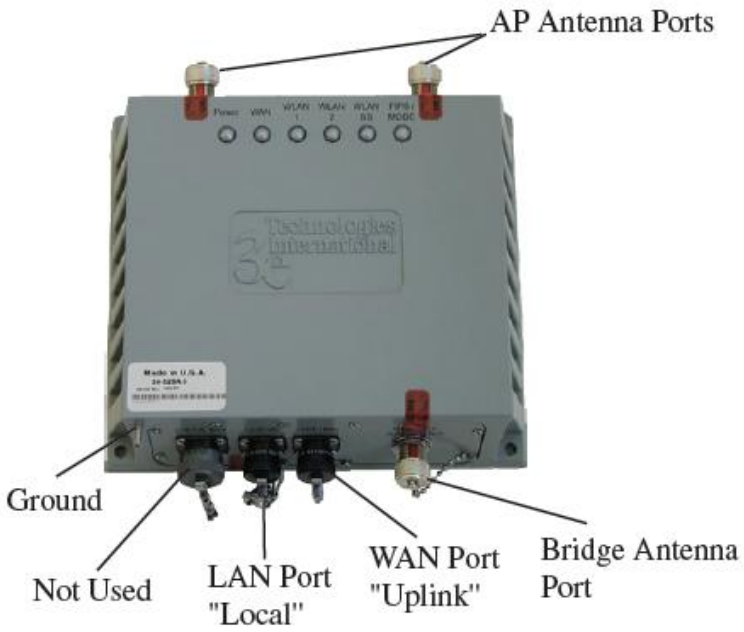
The AP software executes on the Intel XScale IPX425 network processor. On the 3e-525A3, 3e-525A-3MP, 3e-525A-3EP, 3e-525V-3, and 3e-525VE-4 AP models, the CPU is running at 533MHz mode. On the 3e-523-F2 and the 3e-523-3 appliance models, the same CPU runs at 266MHz. The platform includes an Intel IXP 425 Network processor chip with a cryptographic coprocessor. The Intel IXP 425 CPU implements two modes of execution: kernel mode and user mode.

The 3e-525A-3, 3e-525A-3EP, 3e-525A-3MP, 3e-525V-3 and 3e-525VE-4 appliances have two Ethernet ports with one used for the connection to the wired network (WAN Port) and the other used for the local management interface only (LAN Port). All remote management uses HTTPS via either the wired network port or the local management port. The 3e-523-F2 and 3e-523-3 APs have only one Ethernet interface for the wired network connection.

The 3e-525A-3, 3e-525A-3EP, 3e-525A-3MP, 3e-525V-3 and 3e-525VE-4 APs have two RF fixed-configuration interfaces, one functions as a IEEE 802.11 Access Point interface (AP) while the other is used for inter-access-point communication (Wireless Bridge). The AP interface features IEEE 802.11i security while the Wireless Bridge interface uses a secured communication channel with AES encryption. The 3e-523-F2 and 3e-523-3 AP have only one RF interface that behaves as an 802.11 Access Point.

Figure 1-3 below depicts the 3e-525A-3 Wireless Access Point as an example.

Figure 1-3: 3e-525A-3 Wireless Access Point



As shown in the figure above, the 3e-525A-3 contains two Access Point antenna ports and a Bridge antenna port, a wired WAN “uplink” port, a wired LAN “local” port, and a ground stub.

- **AP antenna ports** – The AP antenna ports are connected to one 802.11a/b/g radio for wireless connectivity to secure WLAN clients.

- **Bridge antenna port** – The Bridge antenna port is connected to a second radio for wireless bridging and mesh networking, which can occur at the same time as the AP antenna ports are wirelessly connected to WLAN clients.
- **LAN local port** – The LAN local port is used exclusively for management of the access point. It supports Ethernet 10/100 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 local management data is accepted.
- **WAN uplink port** – The WAN uplink port is intended to connect the 3e-525A-3 access point to the wired LAN. It also supports Ethernet 10/100 Mbps wired traffic in a full duplex configuration. The WAN port bridges all data between the wireless domain and the wired network.
- **Ground stub** – The ground stub provides a reference zero voltage for safety and stability.
- **FIPS Tapes** – Provides physical security and tampering evidence for FIPS compliance.

AP Software

The XScale processor implements two modes of execution: kernel mode and user mode.

The AP's operating system is MontaVista Embedded Linux with Kernel v2.4.

The TOE's security functionality is implemented by the following software sub-components in user space and kernel space.

User Space Sub-Components:

- OpenSSL Library
- HTTPS Daemon
- Web Management Application
- 802.11 Authenticator
- Security Parameter Manager

Kernel Space Sub-Components:

- Kernel Cryptographic Library
- Wireless Kernel Driver
- Ethernet Driver

1.4.4.1 OpenSSL Library

The OpenSSL Library version 0.9.7-beta3 is cross-complied as a runtime library. This library is installed as a runtime library so that other applications can link with it at runtime rather than having it statically linked with a particular application. The OpenSSL Library offers two major functions in the existing 525/523 AP platform:

1) It serves as a cryptographic engine by offering the following FIPS 140-2 validated cryptographic algorithms.

- Advanced Encryption Standard (AES)
- Rivest, Shamir, and Adleman (RSA)
- Secure Hash (SHA)
- Keyed-Hash Message Authentication (HMAC)

2) It offers TLS level APIs which are used by the HTTPS Daemon to setup the TLS session with remote web browsers.

1.4.4.2 HTTPS Daemon

The HTTPS Daemon acts as a TLS server to allow a remote TLS client to connect. After the proper setup of a TLS session, the TLS record protocol together with HTTP offers a secured channel for remote management of the AP device. The HTTPS Daemon is the owner of the following Public/Critical Security Parameters (PSP, CSP):

- Server side X.509 certificate (PSP).
- Server certificate private key file, private key password and TLS session keys (CSP).

The CSPs are stored using either encrypted form or a split knowledge procedure.

1.4.4.3 Web Management Application

The Web Management Application resides on top of the HTTPS session and offers remote management capability. It uses the locally stored User Name and Password to authenticate the remote management user. After a successful authentication, it reads/writes from the persistent storage area and displays configuration information excluding security parameters such as the bridge static AES key. When the Web Management Application reads/writes security parameters, it relies on the OpenSSL Library to provide the encryption/decryption tools needed to access the parameters in the encrypted form. The Web Management Application also directly interacts with system components such as the IP stack, the wireless AP driver, and the bridge driver through system calls and control interfaces to configure and manage the TOE behavior.

1.4.4.4 802.11 Authenticator (Authenticator)

The Authenticator provides IEEE 802.11i security functions to the 525/523 AP Access Point interface. It facilitates the 802.1X authentication between the wireless client and the RADIUS server (either the Security Server or a RADIUS server in the Operational Environment) by forwarding Extensible Authentication Protocol over LAN (EAPOL) messages from the client to the RADIUS server in RADIUS UDP format and vice versa. More importantly, the Authenticator performs the 802.11i 4-way handshake with the wireless client using either the Pairwise Master Key (PMK) learned from the RADIUS server during the 802.1X authentication process or if in Pre-Shared Key (PSK) mode, the administrator manually configures the PMK. During a successful 4-way handshake process, the client and AP each verify that the other is the holder of the PMK and use the information exchanged during the handshake to further derive the Pair-wise Transient Key (PTK) and Group-wise Transient Key (GTK). The PTK and GTK are installed on the AP driver by the Authenticator. The Authenticator zeroes out the PKT/GTK pair for the wireless client after they are installed on the AP driver, but maintains the PMK and its lifetime within the Authenticator.

1.4.4.5 Security Parameter Manager (SP Manager)

The Security Parameter Manager is in charge of managing Critical Security Parameters (CSPs). It will use the CSP encryption key that is stored using split knowledge procedure in non-volatile memory. All other CSPs are stored in flash in encrypted form. Other sub-components can read or write to the CSPs' storage only through the SP Manager.

1.4.4.6 Kernel Cryptographic Library

The Kernel Cryptographic Library wraps and extends the Intel XScale Crypto-coprocessor's library to offer the AES, SHA, and HMAC cryptographic algorithms to the kernel sub-components and drivers

1.4.4.7 Wireless Kernel Driver

The Wireless Kernel Driver is the major kernel sub-component of the 525/523 Access Points. It operates with an Atheros AR52xx chipset in 802.11 infrastructure mode.

The Wireless Kernel Driver performs encryption/decryption of wireless data to and from the wireless clients using the corresponding PTK/GTK key. In FIPS mode of operation, it uses AES in CCM mode with 128 bit key to provide data privacy and integrity. It also supports other 802.11 specific features such as Quality of Service (QoS) with Wi-Fi Multimedia (WMM) and Dynamic Frequency Selection (DFS).

The Wireless Kernel Driver also implements the 3eTI preparatory bridge setup protocol. The bridge driver has one static key to encrypt/decrypt all messages. By possessing the same manually configured key, wireless bridges can be setup between 525/523 APs. There is no explicit authentication process during the bridge link setup phase. After the wireless link setup at the bridge driver level, the Rapid Spanning Tree Protocol (RSTP) is run to trim the bridge link such that no layer 2 bridge loops exist. The data then flows with encryption and decryption at each hop. The same static key is shared across all hops within the wireless mesh network. The data is AES encrypted with SHA1 used as integrity guard.

1.4.4.8 Ethernet Driver

The Ethernet Driver supports communication over the Local Area Network (LAN) and Wide Area Network (WAN).

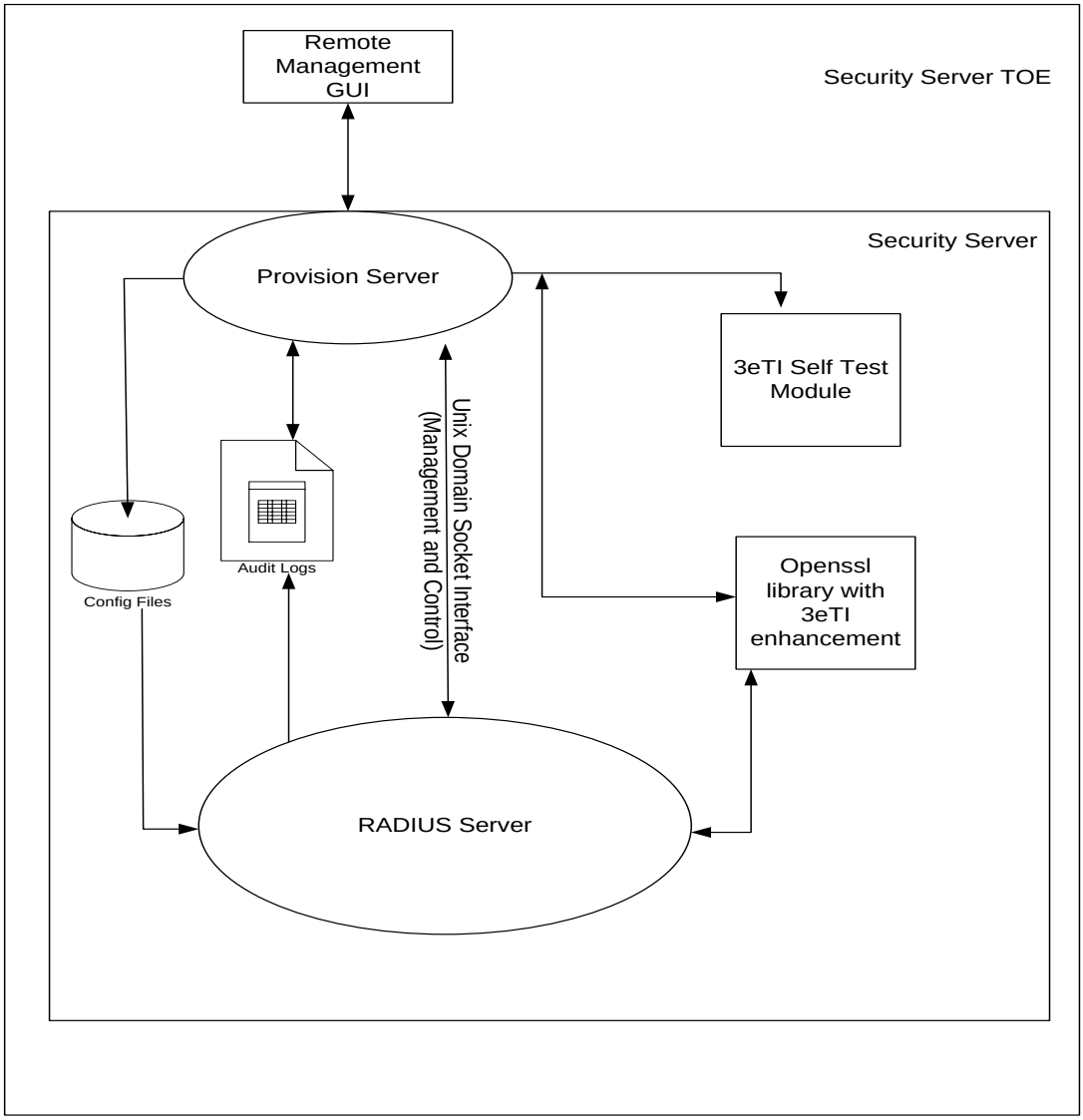
1.4.5 Security Server TOE Component

The Security Server TOE component is composed of software only. The Security Server is a software program that runs in the Operational Environment on a standard Intel-based computer running a Linux or UNIX operating system. Its FIPS 140 testing was performed on Red Hat Linux running on an Intel-based platform.

Security Server Sub-Components

Figure 1-4 below depicts the major sub-components of the Security Server.

Figure 1-4: Security Server TOE Components



The major executable sub-components of the Security Server are:

- RADIUS Server
- Provision Server
- Remote Management GUI
- Open SSL Library
- Self Test Module

1.4.5.1 RADIUS Server

The RADIUS Server acts as the 802.1X Authentication Server and provides the main functions of the Security Server. The RADIUS Server also provides the Certificate Path Verification (CPV) functionality.

1.4.5.2 Provision Server

The Provision Server is a process running on the Security Server platform, which offers the HTTPS service and handles the XML interface between the Remote Management GUI and the Security Server. The interface between Provision Server and the RADIUS Server is Unix Domain Socket (IPC) for management and control by the Provision Server.

1.4.5.3 Remote Management GUI

The Remote Management GUI is an Adobe flash based application running within a Web Browser. The interface between the Remote Management GUI and the Provision Server is XML message over HTTPS

1.4.5.4 OpenSSL Library

The OpenSSL Library with 3eTI enhancement (ECCDSA, ECCDH, and SHA2) is the cryptographic engine used by both the Provision Server and the RADIUS Server.

1.4.5.5 Self-Test Module

The Self-Test Module is a library that encapsulates the cryptographic algorithms' self-test and firmware integrity checks.

1.4.5.6 Audit Log Files

The Audit Log Files store the CC required auditable events.

1.4.5.7 Configuration Files

Configuration Files are used by the Provision Server to write persistent configuration information and by the RADIUS Server to retrieve configuration information.

1.4.6 Data

The data managed by the TOE can be categorized as:

- User data transmitted to and from wireless clients.
- Data used to configure, manage, and operate the TOE such as user accounts and authentication data, audit settings, and cryptographic parameters. This data is TSF data.
- Audit data produced by the TOE for security significant events. This is TSF data.

1.4.7 Users

The Access Point Component maintains the following security roles:

- Administrator
- Crypto-Officer
- Wireless user

The Security Server Component maintains the following security roles:

- Security Officer
- Remote user

1.4.8 Product Guidance

Table 1-6: Product Guidance

3e Technologies International, Inc., AirGuard™ Wireless Access Point User's Guide
3e Technologies International, Inc.,3e-030-02 Security Server Version 4.0 User's Guide

1.4.9 Physical Scope of the TOE

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

The TOE includes the following Access Points appliance models:

- 3e-525-A-3 Access Point; Hardware Version 2.0(A) and 2.1, Firmware Version 4.4
- 3e-525-A-3EP Access Point; Hardware Version 2.1, Firmware Version 4.4
- 3e-525A-3MP Access Point; Hardware Version 2.0(A) and 2.1, Firmware Version 4.4
- 3e-525-V-3 Access Point; hardware version 2.0(A) and 2.1, Firmware Version 4.4
- 3e-525-VE-4 Access Point; hardware version 2.0(A) and 2.1, firmware version 4.4
- 3e-523-F2 Access Point; hardware version 1.0, 1,1, 1.2, and 2.0; firmware version 4.4
- 3e-523-3 Access Point, hardware version 1.0, 1,1, 1.2, and 2.0; firmware version 4.4

The TOE also includes the software only 3eTI Security Server:

- 3e-030-2 Security Server

Figure 1-1 and Figure 1-2 in Section 1.4.3 depict the evaluated TOE configurations and the Operational Environment.

The Operational Environment components relied upon by the TOE and not included in the physical boundary include:

- **Wireless Client Hosts**: The wireless client hosts connecting to the wired network from the wireless network.
- **Administrator Management Hosts**: The TOE relies on remote access from a workstation via HTTPS for management functionality.
- **Audit Server**: The TOE relies upon an audit server for storage of audit.
- **NTP Server**: The TOE relies upon an NTP server to provide reliable.

If the TOE configuration includes the 3eTI Security Server, the Operational Environment includes:

- **Security Server Platform:** The platform for the software-only 3eTI Security Server is a standard Intel-based computer running a Linux or UNIX operating system.

If the TOE configuration does not include the 3eTI Security Server, the Operational Environment includes:

- **RADIUS Server**: The TOE relies on an external RADIUS Server for remote authentication of the wireless users.

1.4.10 Logical Scope of the TOE

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

1.4.10.1 Audit

The TOE generates auditable events for actions on the APs with the capability of selective audit record generation. The records of these events can be viewed within the TOE Management Interface or they can be exported to audit systems 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.

1.4.10.2 Cryptographic Services

The TOE implements the following cryptographic algorithms: AES, RSA, SHA, HMAC, and a random number generator.

1.4.10.3 User Data Protection

The Access Point Component provides user data protection by encrypting/decrypting authenticated user data between the wireless client and the Access Point.

The Security Server provides user data protection in the form of a certificate path validation capability that includes Certificate Revocation Lists checking and an Online Certificate Status Protocol client.

The TOE provides X.509 public key certificate verification.

1.4.10.4 Identification and Authentication

The TOE provides Identification and Authentication security functionality to ensure that all wireless clients/users and administrators are properly identified and authenticated before accessing TOE functionality. The wireless user can be authenticated either by the TOE (via the Security Server) or via a trusted RADIUS server in the Operational Environment. The administrator is authenticated locally with a username and password.

1.4.10.5 Management

The Web Management Application of the TOE provides the capabilities for an authorized administrator to modify, edit, and delete security parameters such as audit data, configuration data, and user authentication data. The Web Management Application also offers an authorized administrator the capability to manage security functions; for example: enable/disable certain audit functions, query and set encryption/decryption algorithms for network packets, change cryptographic keys and allow/disallow the use of a remote authentication server.

The Security Server is managed by the Remote Management GUI.

1.4.10.6 Protection of the TSF

The TOE protects the TSF by ensuring that no access is granted to TOE functions without authorization. By controlling a user session and the actions carried out during a user session, the TOE provides for non-bypassability and domain separation of functions. Internal testing of the TOE hardware and software against tampering ensures that all security functions are running and available before the TOE will accept any communications.

1.4.10.7 TOE Access

The TOE provides the following TOE Access functionality:

- Configurable MAC address and/or IP address filtering with remote management session establishment
- TSF-initiated session termination when a connection is idle for a configurable time period
- TOE Access Banners

1.4.10.8 Logical Dependencies on the Operational Environment

The TOE relies upon the Operational Environment for the following security functionality:

- Audit storage
- Cryptographic services on wireless clients and remote hosts
- Reliable time stamps from a Network Time Protocol (NTP) server
- Inter-TSF trusted channel on clients and remote hosts
- Identification and authentication on remote hosts (i.e., RADIUS server) when the Security Server is not included in the configuration.

1.4.10.9 Non-=Security Relevant Functionality

The 3e-525V-3 and 3e-525VE-4 AP appliances models have a video board within the physical enclosure of the unit and one or more analog video input ports. The video board digitizes the incoming analog video signals and sends the digitized video in the data payload through a wired Ethernet port and/or RF interfaces to the network. The data payload is encrypted over RF interfaces (bridge interface) to the WANas configured by an administrator, the video data is never sent over the AP-client interface to the wireless client. This functionality is irrelevant to the SFRs provided by the TOE. However, as an integrated product function, it does offer to carry digitized video over the secured wireless network.

2 Conformance Claims

2.1 Common Criteria Conformance

This ST claims conformance to Common Criteria for Information Technology Security Evaluation, Version 3.1R3, July 2009. International Standard – ISO/IEC 15408:2000.

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

2.2 Protection Profile Claim

This ST claims Demonstrable Conformance to the US Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007.

Demonstrable Compliance in CC v3.1 R3 is defined as follows:

> ***"Demonstrable conformance:*** there is no subset-superset type relation between the PP and the ST. The PP and the ST may contain entirely different statements that discuss different entities, use different concepts etc. However, the ST shall contain a rationale on why the ST is considered to be "equivalent or more restrictive" than the PP (see Section D.3). Demonstrable conformance allows a PP author to describe a common security problem to be solved and provide generic guidelines to the requirements necessary for its resolution, in the knowledge that there is likely to be more than one way of specifying a resolution. Demonstrable conformance is also suitable for a TOE type where several similar PPs already exist (or likely to exist in the future), thus allowing the ST author to claim conformance to all these PPs simultaneously, thereby saving work. "

Paragraph 445 provides additional details on what is required for *demonstrable* compliance in the following areas:

- Security Problem Definition
- Security Objectives
- Security Requirements

2.2.1 Security Problem Definition

Requirement: The conformance rationale in the ST shall demonstrate that the security problem definition in the ST is equivalent (or more restrictive) than the security problem definition in the PP. This means that:

- All TOEs that would meet the security problem definition in the ST also meet the security problem definition in the PP;
- All Operational Environments that would meet the security problem definition in the PP would also meet the security problem definition in the ST.

Conformance: This Security Target includes all of the threats, organizational security policies, and assumption statements described in the PP, verbatim. Therefore the security problem definition in this ST is equivalent to the security problem definition in the PP.

2.2.2 Security Objectives

Requirement: The conformance rationale in the ST shall demonstrate that the security objectives in the ST is equivalent (or more restrictive) than the security objectives in the PP. This means that:

- All TOEs that would meet the security objectives for the TOE in the ST also meet the security objectives for the TOE in the PP;
- All Operational Environments that would meet the security objectives for the Operational Environment in the PP would also meet the security objectives for the Operational Environment in the ST.

Conformance: This Security Target includes all of the Security Objectives from the PP verbatim. Therefore the security problem definition in this ST is equivalent to the security problem definition in the PP.

2.2.3 Security Requirements

Requirement: The ST shall contain all SFRs and SARs in the PP, but may claim additional or hierarchically stronger SFRs and SARs. The completion of operations in the ST must be consistent with that in the PP; either the same completion is used in the ST as that in the PP or one that makes the requirement more restrictive (the rules of refinement apply).

Conformance: This Security Target includes all of the Security Assurance Requirements from the PP with the additional security assurance requirements of EAL4 augmented by ALC_FLR.2 Flaw reporting procedures.

This Security Target includes all the Security Functional Requirements from the PP. The PP SFRs are augmented by the following SFRs for both TOE configurations:

- FAU_SAR.1 and FAU_SAR.3 Audit Review
- FCS_COP.1 (5) for the HMAC-SHA1 cryptographic operation that is provided by the TOE, but not specified in the PP.
- FIA_USB.1 was iterated to provide separate SFRs for the wireless user and the administrator.
- FTA_TSE.1 for MAC Address filtering upon connections

The SFRs claimed in Section 6 have been iterated for the two evaluated configurations: Wireless Access Point and Security Server Components; and Wireless Access Point Component only. There are some minor differences in the operation of the security functions between the two configurations. Therefore, it was felt that this presentation would be less confusing to the reader. The entire TOE fully meets all the SFRs in the PP for both configurations of the TOE as shown in Table 2-1 below.

Table 2-1: WLAN Access System PP Conformance

SFRs WLAN Access System PP	SFRs that apply to both TOE Configurations	SFRs that apply only to the TOE Configuration that includes the Security Sever
FAU_GEN.1 - Audit data generation	FAU_GEN.1 (1) - Audit data generation (Wireless Access Point)	FAU_GEN.1 (SS) – Audit data generation (Security Server)
FAU_GEN.2 - User identity association	FAU_GEN.2 (1) - User identity association (Wireless Access Point)	FAU_GEN.2 (SS) – User identity association (Security Server)
N/A	FAU_SAR.1 (1) – Audit review (Wireless Access Point)	FAU_SAR.1 (SS) Audit review (Security Server)
N/A	FAU_SAR.3 (1) – Selectable audit review (Wireless Access Point)	FAU_SAR.3 (SS) Selectable audit review (Security Server)
FAU_SEL.1 - Selective audit	FAU_SEL.1 (1) - Selective audit (Wireless Access Point)	FAU_SEL.1 (SS) – Selective Audit (Security Server)
FCS_BCM_(EXT).1 – Extended: Baseline Cryptographic Module	FCS_BCM_(EXT).1 – Extended: Baseline Cryptographic Module	FCS_BCM_(SS).1 – Extended: Security Server baseline cryptographic module
FCS_CKM.1 (1) - Cryptographic key generation (for symmetric keys)	FCS_CKM.1 (1) - Cryptographic key generation (for symmetric keys on Wireless Access Point)	FCS_CKM.1 (SS1) - Cryptographic key generation (for symmetric keys on Security Server)
FCS_CKM.1 (2) - Cryptographic key generation (for asymmetric keys)	FCS_CKM.1 (2) - Cryptographic key generation (for asymmetric keys on Wireless Access Point)	FCS_CKM.1 (SS2) - Cryptographic key generation (for asymmetric keys on Security Server)
FCS_CKM.2 - Cryptographic key distribution	FCS_CKM.2 (1) - Cryptographic key distribution (Wireless Access Point)	FCS_CKM.2 (SS) - Cryptographic key distribution (Security Server)
FCS_CKM_(EXT).2 - Extended: Cryptographic key handling and storage	FCS_CKM_(EXT).2 - Extended: Cryptographic key handling and storage	FCS_CKM_(SS).2 - Cryptographic key handling and storage on Security Server)
FCS_CKM.4 - Cryptographic key destruction	FCS_CKM.4 - Cryptographic key destruction (Wireless Access Point)	FCS_CKM.4 (SS) - Cryptographic key destruction (Security Server)
FCS_COP.1 (1) – Cryptographic Operation (Data encryption/decryption)	FCS_COP.1 (1) – Cryptographic Operation (Data encryption/decryption on Wireless Access Point)	FCS_COP.1 (SS1) – Cryptographic Operation (Data encryption/decryption on Security Server)
FCS_COP.1 (2) – Cryptographic Operation (Digital Signature)	FCS_COP.1 (2) – Cryptographic Operation (Digital Signature on Wireless Access Point)	FCS_COP.1 (SS2) – Cryptographic Operation (Digital Signature on Security Server)
FCS_COP.1 (3) – Cryptographic Operation (Hashing)	FCS_COP.1 (3) – Cryptographic Operation (Hashing on Wireless Access Point)	FCS_COP.1 (SS3) – Cryptographic Operation (Secure Hash on Security Server)
FCS_COP.1 (4) – Cryptographic Operation (Key agreement)	FCS_COP.1 (4) – Cryptographic Operation (Key agreement on Wireless Access Point)	FCS_COP.1 (SS4) - Cryptographic Operation (Key Agreement on Security Server)

SFRs WLAN Access System PP	SFRs that apply to both TOE Configurations	SFRs that apply only to the TOE Configuration that includes the Security Sever
NA	FCS_COP.1 (5) – Cryptographic Operation (HMAC on Wireless Access Point)	FCS_COP.1 (SS5) – Cryptographic Operation (HMAC on Security Server)
FCS_COP_(EXT).1 – Extended: Random Number Generation	FCS_COP_(EXT).1 – Extended: Random Number Generation	FCS_COP_(SS).1 – Extended: Security Server random number generation
FDP_PUD_(EXT).1 – Extended: Protection of User Data	FDP_PUD_(EXT).1 – Extended: Protection of User Data	N/A
N/A	N/A	FDP_CPD_(SS).1 Extended: Certificate path development
N/A	N/A	FDP_DAU_CPL_(SS).1 Extended: Certificate path initialisation – basic
N/A	N/A	FDP_DAU_CPV_(SS).1 Extended: Intermediate certificate processing - Basic
N/A	N/A	FDP_DAU_CPV_(SS).2 Extended: Certificate processing - basic
N/A	N/A	FDP_DAU_CPV_(SS).1 Extended: Certificate path output - basic
N/A	N/A	FDP_DAU_CRL_(SS).1 Extended: Basic CRL Checking
N/A	N/A	FDP_DAU_OCS_(SS).1 Extended: Basic OCSP Client
N/A	N/A	FDP_ITC_SIG_(SS).1 Extended: Import of PKI Signature
FDP_RIP.1 - Subset residual information protection	FDP_RIP.1 (1) - Subset residual information protection (Wireless Access Point)	FDP_RIP.1 (SS) – Subset Residual Information Protection (Security Server)
FIA_AFL.1 - Administrator authentication failure handling	FIA_AFL.1 (1) - Administrator authentication failure handling (Wireless Access Point)	FIA_AFL.1 (SS) – Authentication failure handling (Security Server Administrator)
FIA_ATD.1 (1) - Administrator attribute definition	FIA_ATD.1 (1) - Administrator attribute definition (Wireless Access Point)	FIA_ATD.1 (SS1) – Administrator attribute definition (Security Server)
FIA_ATD.1 (2) - User attribute definition	FIA_ATD.1 (2) - User attribute definition (Wireless Access Point)	FIA_ATD.1 (SS2) – User attribute definition (Security Server)
FIA_UAU.1 - Timing of local authentication	FIA_UAU.1 – Timing of local authentication	FIA_UAU.2 – User authentication before any action
FIA_UAU_(EXT).5 – Extended: Multiple authentication mechanisms	FIA_UAU_(EXT).5 – Extended: Multiple authentication mechanisms	FIA_UAU.5 – Multiple authentication mechanisms
FIA_UID.2 - User identification before any action	FIA_UID.2 (1) - User identification before any action (Wireless Access Point)	FIA_UID.2 (SS) – User identification before any action (Security Server)
FIA_USB.1 (1) - User-subject binding (Administrator)	FIA_USB.1 (1) - User-subject binding (Administrator on Wireless Access Point)	FIA_USB.1 (SS) –User-subject binding (Security Server Administrator)

SFRs WLAN Access System PP	SFRs that apply to both TOE Configurations	SFRs that apply only to the TOE Configuration that includes the Security Sever
FIA_USB.1 (2) - User-subject binding (Wireless User)	FIA_USB.1 (2) - User-subject binding (Wireless User on Wireless Access Point)	N/A
FMT_MOF.1 (1) - Management of security functions behavior (Cryptographic Function)	FMT_MOF.1 (1) - Management of security functions behavior (Wireless Access Point)	FMT_MOF.1 (SS) - Management of security functions behavior (Security Server)
FMT_MOF.1 (2) - Management of security functions behavior (Audit Record Generation)		
FMT_MOF.1 (3) - Management of security functions behavior (Authentication)		
FMT_MSA.2 - Secure security attributes	FMT_MSA.2 (1) - Secure security attributes (Wireless Access Point)	FMT_MSA.2 (SS) - Secure security attributes (Security Server)
FMT_MTD.1 (1) - Management of Audit Data	FMT_MTD.1 (1) - Management of TSF Data (Wireless Access Point)	FMT_MTD.1 (SS) - Management of TSF Data (Security Server)
FMT_MTD.1 (2) - Management of Authentication data (Administrator)		
FMT_MTD.1 (3) - Management of Authentication data (User)		
FMT_SMF.1 (1) - Specification of Management Functions (Cryptographic Functions)	FMT_SMF.1 (1) - Specification of Management Functions (Wireless Access Point)	FMT_SMF.1 (SS) - Specification of Management Functions (Security Server)
FMT_SMF.1 (2) - Specification of Management Functions (TOE Audit Record Generation)		
FMT_SMF.1 (3) - Specification of Management Functions (Cryptographic Key Data)		
FMT_SMR.1 - Security roles	FMT_SMR.1 (1) - Security roles (Wireless Access Point)	FMT_SMR.1 (SS) - Security roles (Security Server)
FPT_STM_(EXT).1 – Extended: Reliable time stamps	FPT_STM_(EXT).1 – Extended: Reliable time stamps	N/A
FPT_TST_(EXT).1 - Extended: TSF testing	FPT_TST_(EXT).1 - Extended: TSF testing	FPT_TST_(SS).1 - Extended Security Server testing
FPT_TST.1 (1)- TSF testing (for cryptography)	FPT_TST.1 (1)- TSF testing (for cryptography on Wireless Access Point)	FPT_TST.1 (SS1) - TSF testing (Security Server Cryptography
FPT_TST.1 (2) - TSF testing (for key generation components)	FPT_TST.1 (2) - TSF testing (for key generation components on Wireless Access Point)	FPT_TST.1 (SS2) - TSF testing (Security Server Key Generation Components)
FTA_SSL.3 - TSF-initiated termination	FTA_SSL.3 (1) - TSF-initiated termination (Wireless Access Point)	FTA_SSL.3 (SS) TSF-initiated termination (Security Server)
FTA_TAB.1 - Default TOE access banners	FTA_TAB.1 (1) - Default TOE access banners (Wireless Access Point)	FTA_TAB.1 (SS) Default TOE access banners (Security Server)
N/A	FTA_TSE.1 – TOE Session Establishment	N/A

SFRs WLAN Access System PP	SFRs that apply to both TOE Configurations	SFRs that apply only to the TOE Configuration that includes the Security Sever
FTP_ITC_(EXT).1 – Extended: Inter-TSF trusted channel	FTP_ITC_(EXT).1 Extended: Inter-TSF trusted channel	FTP_ITC_(SS).1 – Extended Security Server trusted channel
FTP_TRP.1 – Trusted Path	FTP_TRP.1 (1) Trusted Path (Wireless Access Point)	FTP_TRP.1 (SS) – Trusted Path (Security Server)

The following SFRs were not iterated for the Security Server, since they only apply to the Access Point component: FDP_PUD_(EXT).1, FIA_USB.1(2) for the wireless client, and FTA_TSE.1. In addition, FIA_UAU.1 is claimed for the Access Point component, whereas FIA_UAU.2 is claimed for the Security Server component.

The PP SFRs are augmented by the following SFRs only for the TOE configuration that includes the 3eTI Security Server.

- FDP_CPD_(SS).1 Extended: Certificate path development
- FDP_DAU_CPL_(SS).1 Extended: Certificate path initialisation – basic
- FDP_DAU_CPV_(SS).1 Extended: Intermediate certificate processing - Basic
- FDP_DAU_CPV_(SS).2 Extended: Certificate processing - basic
- FDP_DAU_CPV_(SS).1 Extended: Certificate path output - basic
- FDP_DAU_CRL_(SS).1 Extended: Basic CRL Checking
- FDP_DAU_OCS_(SS).1 Extended: Basic OCSP Client
- FDP_ITC_SIG_(SS).1 Extended: Import of PKI Signature

These SFRs were modeled on SFRs from the US Government Family of Protection Profiles for Public Key Enabled Applications.

The FMT SFRs: FMT_MOF.1, FMT_MTD.1, and FMT_SMF.1, have been iterated for the Access Point and for the Security Server. The iterations are now presented using a table, with one row for each iteration. It was found that many management functions were not included in the original PP and it would be impractical and confusing to the reader to specify all the management functionality provided by the TOE as separate SFRs. All the management functionality specified by the PP has been included in the ST.

The security requirements in this ST are more restrictive than the security requirements in the PP.

2.3 Package Claim

The TOE claims conformance to Evaluation Assurance Level (EAL) 4 augmented with ALC_FLR.2 Flaw reporting procedures.

3 Security Problem Definition

The Security Problem Definition defines:

a) IT related threats that the product is designed to counter;

b) Organizational security policies with which the product is designed to comply, and

c) Assumptions made on the Operational Environment and the method of use intended for the product.

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

3.1 Threats to Security

Table 3-1 below lists the threats to security.

Table 3-1: Threats to Security

#	Threat Name	Threat Definition
1	T.ACCIDENTAL_ADMIN_ ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
2	T.ACCIDENTAL_ CRYPTO_ COMPROMISE	A user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
3	T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
4	T.POOR_DESIGN	Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
5	T.POOR_IMPLEMENTATION	Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
6	T.POOR_TEST	The developer or tester performs insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may occur, resulting in incorrect TOE behavior being undiscovered leading to flaws that may be exploited by a mischievous user or program.
7	T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
8	T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).
9	T.UNATTENDED_ SESSION	A user may gain unauthorized access to an unattended session.
10	T.UNAUTHORIZED_ ACCESS	A user may gain access to services (either on the TOE or by sending data through the TOE) for which they are not authorized according to the TOE security policy.
11	T.UNAUTH_ADMIN_ACCESS	An unauthorized user or process may gain access to an administrative account.

Table 3-2 below lists the Basic Robustness threats not applicable to the TOE.

Table 3-2: Basic Robustness Threats NOT Applicable to the TOE

#	Threat Name	Threat Definition	Rationale for NOT Including this Threat
1	T.ACCIDENTAL_AUDIT_COMPROMISE	A user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	The storage/retrieval and review of audit records is provided by the Operational Environment. Hence, although this threat must be addressed within the Operational Environment, the functional requirements specified in this ST do not provide the functionality required to protect the audit records in the external environment. The fundamental threat must be met by protecting communications path that the audit records travel for storage and review.
2	T.UNIDENTIFIED_ ACTIONS	The administrator may not have the ability to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.	This threat is intended to require the FAU_SAA and FAU_ARP requirements and those requirements were deemed inappropriate for the basic robustness wireless access system TOE and how it is envisioned it will be administered.

3.2 Organization Security Policies

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

Table 3-3: Organizational Security Policies

#	Policy Name	Policy Definition
1	P.ACCESS_BANNER	The TOE shall display an initial banner for administrator logins describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
2	P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
3	P.CRYPTOGRAPHIC	The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.

#	Policy Name	Policy Definition
4	P.CRYPTOGRAPHY_VALIDATED	Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).
5	P.ENCRYPTED_CHANNEL	The TOE shall provide the capability to encrypt/decrypt wireless network traffic between the TOE and those wireless clients that are authorized to join the network.
6	P.NO_AD_HOC_NETWORKS	In accordance with the DOD Wireless Policy, there will be no ad hoc 802.11 or 802.15 networks allowed.

3.3 Secure Usage Assumptions

Table 3-4 below lists the secure usage assumptions.

Table 3-4: Secure Usage Assumptions

#	Name	Assumption
1	A.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance.
2	A.NO_GENERAL_PURPOSE	There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
3	A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
4	A.TOE_NO_BYPASS	Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.

4 Security Objectives

This section defines TOE security objectives and objectives for the Operational Environment. The section also provides a rationale that the objectives are suitable for the Security Problem Definition.

4.1 Security Objectives for the TOE

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

Table 4-1: Security Objectives

#	Name	TOE Security Objective
1	O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events associated with users.
2	O.CORRECT_TSF_OPERATION	The TOE will provide the capability to verify the correct operation of the TSF.
3	O.CRYPTOGRAPHY	The TOE shall provide cryptographic functions to maintain the confidentiality and allow for detection of modification of user data that is transmitted between physically separated portions of the TOE, or outside of the TOE.
4	O.CRYPTOGRAPHY_VALIDATED	The TOE will use NIST FIPS 140-1/2 validated cryptomodules for cryptographic services implementing NIST-approved security functions and random number generation services used by cryptographic functions.
5	O.DISPLAY_BANNER	The TOE will display an advisory warning prior to establishing an administrator session regarding use of the TOE prior to permitting the use of any TOE services that requires authentication.
6	O.MANAGE	The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
7	O.MEDIATE	The TOE must mediate the flow of information to and from wireless clients communicating via the TOE in accordance with its security policy.
8	O.RESIDUAL_ INFORMATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.
9	O.SELF_PROTECTION	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
10	O.TIME_STAMPS	The TOE shall obtain reliable time stamps.
11	O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.
12	O.ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure management.

13	O.CONFIGURATION_ IDENTIFICATION	The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly.
14	O.DOCUMENTED_ DESIGN	The design of the TOE is adequately and accurately documented.
15	O.PARTIAL_ FUNCTIONAL_TESTING	The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.
16	O.VULNERABILITY_ ANALYSIS	The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.

Table 4-2 lists additional security objectives for the TOE when the TOE includes the Security Server.

Table 4-2: Additional TOE Security Objectives when TOE Includes Security Server

#	Name	TOE Security Objective
17	OSS.CERTIFCATE PATH_VALIDATION	The TOE shall provide the capability of validating the certificate path for OSI X.509 certificates.
18	OSS.AUTHENTICATION SERVER	The TOE shall provide an 802.1X compliant RADIUS Server.
19	OSS.SIGNATURE_VERIFICATION	The TOE shall provide the capability of verifying rDSA and ecDSA digital signatures.

4.2 Security Objectives for the Operational Environment

The WLAN PP uses the term “IT Environment” rather than CC Version 3 term of “Operational Environment”.

Table 4-3 below lists the Security Objectives for the Operational Environment.

The WLAN PP uses the term “IT Environment” rather than CC Version 3 term of “Operational Environment”.

Table 4-3: Security Objectives for the Operational Environment

#	Name	Security Objective
1	OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information and the authentication credentials.
2	OE.AUDIT_REVIEW	The IT Environment will provide the capability to selectively view audit information.
3	OE.MANAGE	The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
4	OE.NO_EVIL	Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.
5	OE.NO_GENERAL_PURPOSE	There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.

6	OE.PHYSICAL	The environment provides physical security commensurate with the value of the TOE and the data it contains.
7	OE.PROTECT_MGMT_COMMS	The environment shall protect the transport of audit records to the audit server, remote network management, and authentication server communications with the TOE and time service in a manner that is commensurate with the risks posed to the network.
8	OE.RESIDUAL_INFORMATION	The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.
9	OE.SELF_PROTECTION	The environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
10	OE.TIME_STAMPS	The TOE IT environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.
11	OE.TOE_ACCESS	The environment will provide mechanisms that support the TOE in providing a user's logical access to the TOE.
12	OE.TOE_NO_BYPASS	Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.

4.3 Security Objectives Rationale

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

4.3.1 Threats Rationale

Table 4-4 below shows that all threats are countered by security objectives.

Table 4-4: Threats Countered by Security Objectives

#	Threat	Security Objectives
1	T_ACCIDENTAL _ADMIN_ERROR	O.ADMIN_GUIDANCE helps to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is insecure. O.MANAGE also contributes to mitigating this threat by providing administrators the capability to view and manage configuration settings. For example, if the administrator made a mistake when configuring the set of permitted users' authentication credentials, providing the capability to view the lists of authentication credentials affords them the ability to review the list and discover any mistakes that might have been made. OE.NO_EVIL contributes to mitigating this threat by ensuring that the administrators are non-hostile and are trained to appropriately manage and administer the TOE. OE.NO_GENERAL_PURPOSE also helps to mitigate this threat by ensuring that there can be no accidental errors due to the introduction of unauthorized software or data, by ensuring that there are no general-purpose or storage repository applications available on the TOE.

#	Threat	Security Objectives
2	T.ACCIDENTAL _CRYPTO _COMPROMISE	O.RESIDUAL_INFORMATION; OE.RESIDUAL_INFORMATION contributes to the mitigation of this threat by ensuring that any residual data is removed from network packet objects and ensuring that cryptographic material is not accessible once it is no longer needed. O.SELF_PROTECTION ensures that the TOE will have adequate protection from external sources and that all TSP functions are invoked. OE.SELF_PROTECTION ensures that the TOE Operational environment will have protection similar to that of the TOE.
3	T.MASQUERADE	O.TOE_ACCESS mitigates this threat by controlling logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanism, this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE. Finally, the TOE includes requirements that ensure protected channels are used to authenticate wireless users and to communicate with critical portions of the TOE Operational Environment. OE.TOE_ACCESS supports TOE authentication by providing an authentication server in the TOE Operational Environment. The environment also includes requirements that ensure protected channels are used to communicate with critical portions of the TOE Operational Environment. OE.TOE_NO_BYPASS contributes to mitigating this threat by ensuring that wireless clients must be configured for all information flowing between a wireless client and another client or other host on the network without passing through the TOE.
4	T.POOR_DESIGN	O.CONFIGURATION_IDENTIFICATION plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE's design documentation and the ability to report and resolve security flaws. O.DOCUMENTED_DESIGN counters this threat, to a degree, by requiring that the TOE be developed using sound engineering principles. The use of a high level design and the functional specification ensure that developers responsible for TOE development understand the overall design of the TOE. This in turn decreases the likelihood of design flaws and increases the chance that accidental design errors will be discovered. ADV_RCR.1 ensures that the TOE design is consistent across the High Level Design and the Functional Specification. O.VULNERABILITY_ANALYSIS_TEST ensures that the TOE has been analyzed for obvious vulnerabilities and that any vulnerabilities found have been removed or otherwise mitigated, this includes analysis of any probabilistic or permutational mechanisms incorporated into a TOE claiming conformance to this PP.

#	Threat	Security Objectives
5	T.POOR _IMPLEMENTATION	O.CONFIGURATION_IDENTIFICATION plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE's design. This ensures that changes to the TOE are performed in structure manner and tracked. O.PARTIAL_FUNCTIONAL_TESTING ensures that the developers provide evidence and demonstration that all security functions perform as specified through independent sample testing. O.VULNERABILITY_ANALYSIS_TEST ensures that the TOE has been analyzed and tested to demonstrate that it is resistant to obvious vulnerabilities.
6	T.POOR_TEST	O.CORRECT_ TSF_OPERATION provides assurance that the TSF continues to operate as expected in the field. O.PARTIAL_FUNCTIONAL_TESTING increases the likelihood that any errors that do exist in the implementation will be discovered through testing. O.VULNERABILITY_ANALYSIS_TEST addresses this concern by requiring a vulnerability analysis be performed in conjunction with testing that goes beyond functional testing. This objective provides a measure of confidence that the TOE does not contain security flaws that may not be identified through functional testing. O.DOCUMENTED_DESIGN. Helps to ensure that the TOE's documented design satisfies the security functional requirements. In order to ensure the TOE's design is correctly realized in its implementation, the appropriate level of functional testing of the TOE's security mechanisms must be performed during the evaluation of the TOE.
7	T.RESIDUAL_DATA	O.RESIDUAL_INFORMATION and OE.RESIDUAL_INFORMATION contributes to the mitigation of this threat by ensuring that any residual data is removed from network packet objects and ensuring that cryptographic material is not accessible once it is no longer needed.
8	T.TSF_COMPROMISE	O.MANAGE mitigates this threat by restricting access to administrative functions and management of TSF data to the administrator. OE.MANAGE ensures that the administrator can view security relevant audit events. O.RESIDUAL_INFORMATION and OE.RESIDUAL_INFORMATION contributes to the mitigation of this threat by ensuring that any residual data is removed from network packet objects and ensuring that cryptographic material is not accessible once it is no longer needed. O.SELF_PROTECTION requires that the TOE environment be able to protect itself from tampering and that the security mechanisms in the TOE cannot be bypassed. Without this objective, there could be no assurance that users could not view or modify TSF data or TSF executables. OE.SELF_PROTECTION ensures that the TOE Operational Environment will have protection similar to that of the TOE.
9	T.UNATTENDED _SESSION	The only sessions that are established with the TOE are anticipated to be administrative sessions. Hence, this threat is restricted to administrative sessions. The termination of general user sessions is expected to be handled by the Operational Environment. O.TOE_ACCESS helps to mitigate this threat by including mechanisms that place controls on administrator sessions. Administrator sessions are dropped after an administrator defined time period of inactivity. Dropping the connection of a session (after the specified time period) reduces the risk of someone accessing the machine where the session was established, thus gaining unauthorized access to the session.

#	Threat	Security Objectives
10	T.UNAUTHORIZED _ACCESS	O.MEDIATE works to mitigate this threat by ensuring that all network packets that flow through the TOE are subject to the information flow policies. O.TOE_ACCESS and OE.TOE ACCESS. The TOE requires authentication prior to gaining access to certain services on or mediated by the TOE. O.SELF_PROTECTION and OE.SELF_PROTECTION. The TSF and its environment must ensure that all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services. O.MANAGE and OE.MANAGE. The TOE and its environment restrict the ability to modify the security attributes associated with the TOE to the administrator. These objectives ensure that no other user can modify the information flow policy to bypass the intended TOE security policy. OE.TOE_NO_BYPASS contributes to mitigating this threat by ensuring that wireless clients must be configured to use the wireless access system for all information flowing between a wireless client and any other host on the network. If the clients are properly configured, any information passing through the TOE will be inspected to ensure it is authorized by TOE polices. OSS.CERTIFCATE_PROCESSING contributes to mitigating this threat by supporting a strong authentication mechanism. OSS AUTHENTICATION_SERVER contributes to mitigating this threat by supporting a strong authentication mechanism OSS.SIGNATURE_VERIFICATION contributes to mitigating this threat by supporting a strong authentication mechanism
11	T.UNAUTH _ADMIN_ACCESS	O.ADMIN_GUIDANCE helps to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is not secure. O.MANAGE and OE.MANAGE mitigate this threat by restricting access to administrative functions and management of TSF data to the administrator. O.TOE_ACCESS and OE.TOE_ACCESS helps to mitigate this threat by including mechanisms to authenticate TOE administrators and place controls on administrator sessions. OE.NO_EVIL helps to mitigate this threat by ensuring that the TOE administrators have guidance that instructs them in how to administer the TOE in a secure manner.

4.3.2 Policy Rationale

Table 4-5 below shows that all policies are addressed by objectives.

Table 4-5: Policies Mapped to Objectives

#	Policy	Objectives
1	P.ACCESS_BANNER	O.DISPLAY_BANNER satisfies this policy by ensuring that the TOE displays an administrator configurable banner that provides all users with a warning about unauthorized use of the TOE. A banner will be presented for all TOE services that allow direct access to the TOE. In other words, it will be required for all administrative actions. The presentation of banners prior to actions that take place as a result of the passing of traffic through the TOE is assumed to be provided by the Operational Environment.
2	P.ACCOUNTABILITY	O.AUDIT_GENERATION addresses this policy by providing the administrator with the capability of configuring the audit mechanism to record the actions of a specific user, or review the audit trail based on the identity of the user. Additionally, the administrator's ID is recorded when any security relevant change is made to the TOE (e.g. access rule modification, start-stop of the audit mechanism, establishment of a trusted channel, etc.). OE.AUDIT_PROTECTION provides protected storage of TOE and Operational Environment audit data in the environment. OE.AUDIT_REVIEW Further supports accountability by providing mechanisms for viewing and sorting the audit logs O.MANAGE ensures that access to administrative functions and management of TSF data is restricted to the administrator. OE.MANAGE ensures that the administrator can manage audit functionality in the TOE Operational Environment. O.TIME_STAMPS plays a role in supporting this policy by requiring the TOE to provide a reliable time stamp (via an external NTP server). The audit mechanism is required to include the current date and time in each audit record. All audit records that include the user ID, will also include the date and time that the event occurred. OE.TIME_STAMPS ensures that the TOE Operational Environment provides time services. O.TOE_ACCESS and OE.TOE_ACCESS support this policy by controlling logical access to the TOE and its resources. This objective ensures that users are identified and authenticated so that their actions may be tracked by the administrator. OSS.CERTIFCATE_PROCESSING supports this policy by supporting a non-repudiation mechanism. OSS AUTHENTICATION_SERVER supports this policy by providing authentication of remote user. OSS.SIGNATURE_VERIFICATION supports this policy by supporting a non-repudiation mechanism.
3	P.CRYPTOGRAPHY	O.CRYPTOGRAPHY satisfies this policy by requiring the TOE to implement NIST FIPS validated cryptographic services. These services will provide confidentiality and integrity protection of TSF data while in transit to remote parts of the TOE. O.RESIDUAL_INFORMATION satisfies this policy by ensuring that cryptographic data are cleared according to FIPS 140-1/2.

#	Policy	Objectives
4	P.CRYPTOGRAPHY_ VALIDATED	O.CRYPTOGRAPHY satisfies this policy by requiring the TOE to implement NIST FIPS validated cryptographic services. These services will provide confidentiality and integrity protection of TSF data while in transit to remote parts of the TOE. O.CRYPTOGRAPHY_VALIDATED satisfies this policy by requiring that all cryptomodules for cryptographic services be NIST 140-1/2 validated. This will provide assurance that the NIST-approved security functions and random number generation will be in accordance with NIST and validated according the FIPS 140-1/2
5	P.ENCRYPTED _CHANNEL	O.CRYPTOGRAPHY and O.CRYPTOGRAPHY_VALIDATED satisfy this policy by requiring the TOE to implement NIST FIPS validated cryptographic services. These services will provide confidentiality and integrity protection of TSF data while in transit to wireless clients that are authorized to join the network. O.MEDIATE further allows the TOE administrator to set a policy to encrypt all wireless traffic. OE.PROTECT_MGMT_COMMS provides that the audit records, remote network management information and authentication data will be protected by means of a protected channel in the environment.
6	P.NO_AD_HOC_NET WORKS	O.MEDIATE works to support this policy by ensuring that all network packets that flow through the TOE are subject to the information flow policies. OE.TOE_NO_BYPASS supports this policy by ensuring that wireless clients must be configured to use the wireless access system for all information flowing between a wireless client and any other host on the network. If the clients are properly configured, any information passing through the TOE will be inspected to ensure it is authorized by TOE polices.

4.3.3 Assumptions Rationale

Table 4-6 below shows that all assumptions are addressed by objectives for the Operational Environment.

Table 4-6: Assumptions Addressed by Objectives for the Operational Environment

#	Assumption	Objective for the Operational Environment
1	A.NO_EVIL	The OE.NO_EVIL objective ensures that administrators are non-hostile, appropriately trained and follow all administrator guidance.
2	A.NO_GENERAL PURPOSE	The OE.NO_GENERAL_PURPOSE objective ensures that there are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
3	A.PHYSICAL	The OE.PHYSICAL objective ensures that the environment provides physical security commensurate with the value of the TOE and the data it contains.
4	A.TOE_NO_BYPASS	The OE.TOE_NO_BYPASS objective ensures that wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.

4.3.4 TOE Objectives Mapped to Threats and Policies

Table 4-7 below shows that every Security Objective for the TOE can be traced to at least one threat or organizational security policy.

Table 4-7: TOE Objectives Traced to Threats and Policies Matrix

		O.ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.CRYPTOGRAPHY_VALIDATED	O.CONFIGURATION_IDENTIFICATION	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPH	O.DISPLAY_BANNER	O.DOCUMENTED_DESIGN	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_TESTING	O.RESIDUAL_INFORMATION	O.SELF_PROTECTION	O.TIME_STAMPS	O.TOE_ACCESS	O.VULNERABILITY_ANALYSIS_TEST	OSS.CERTIFICATE_PATH_PROCESSOMG	OSS.AUTHENTICATION_SERVER	OSS.SIGNATURE_VERIFCATION
#	Threat or Policy	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	T.ACCIDENTAL_ADMIN_ ERROR	X								X										
2	T.ACCIDENTAL_ CRYPTO_ COMPROMISE												X	X						
3	T.MASQUERADE															X				
4	T.POOR_DESIGN				X				X								X			
5	T.POOR_IMPLEMENTATION				X							X					X			
6	T.POOR_TEST					X			X			X					X			
7	T.RESIDUAL_DATA												X							
8	T.TSF_COMPROMISE									X			X	X						
9	T.UNATTENDED_ SESSION															X				
10	T.UNAUTHORIZED_ ACCESS									X	X			X		X		X	X	X
11	T.UNAUTH_ADMIN_ACCESS	X								X						X				
1	P.ACCESS_BANNER							X												
2	P.ACCOUNTABILITY		X							X					X	X		X	X	X
3	P.CRYPTOGRAPHY						X						X							
4	P.CRYPTOGRAPHY _VALIDATED			X			X													
5	P.ENCRYPTED_CHANNEL			X			X				X									
6	P.NO_AD_HOC_NETWORKS										X									

4.3.5 Objectives for Operational Environment mapped to Threats, Policies, and Assumptions

Table 4-8 below shows that every Security Objective for the Operational Environment can be traced to at least one threat, organizational security policy, or assumption.

Table 4-8: Objectives for the Operational Environment Traced to Threats, Policies, and Assumptions

#	Objective for the Environment	Threats, Policies and Assumptions
1	OE.AUDIT_PROTECTION	P.ACCOUNTABILITY
2	OE.AUDIT_REVIEW	P.ACCOUNTABILITY
3	OE.MANAGE	T.UNAUTH_ADMIN_ACCESS T.TSF_COMPROMISE P.ACCOUNTABILITY
4	OE.NO_EVIL	A.NO_EVIL T.ACCIDENTAL_ADMIN_ERROR T.UNAUTH_ADMIN_ACCESS
5	OE.NO_GENERAL_PURPOSE	A.NO_GENERAL_PURPOSE T.ACCIDENTIAL_ADMIN_ERROR
6	OE.PHYSICAL	A.PHYSICAL
7	OE.PROTECT_MGMT_COMMS	P.ENCRYPTED_CHANNEL
8	OE.RESIDUAL_INFORMATION	T.ACCIDENTAL_CRYPO_COMPROMISE T.RESIDUAL_DATA T.TSF_COMPROMISE
9	OE.SELF_PROTECTION	T.ACCIDENTAL_CRYPO_COMPROMISE T.TSF_COMPROMISE T.UNAUTHORIZED_ACCESS
10	OE.TIME_STAMPS	P.ACCOUNTABILITY
11	OE.TOE_ACCESS	T.MASQUERADE T.UNAUTHORIZED_ACCESS T.UNAUTH_ADMIN_ACCESS P.ACCOUNTABILITY
12	OE.TOE_NO_BYPASS	A.TOE_NO_BYPASS T.MASQUERADE T.UNAUTHORIZED_ACCESS P.NO_AD_HOC_NETWORKS

5 Extended Components Definition

5.1 Wireless Access Point Extended Components Definition

All of the extended components for the access system have been taken from the U. S. Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007.

The extended components are denoted by adding "_(EXT)" in the component name.

Note: The WLAN PP uses the term "IT Environment" rather than "Operational Environment".

Note: Typographical and formatting errors in the extended SFRs from the WLAN PP have also been corrected.

Table 5-1: Wireless Access Point Extended Components

SFR Class	Item #	SFR ID	SFR Title
FCS	1	FCS_BCM_(EXT).1	Baseline cryptographic module
	2	FCS_CKM_(EXT).2	Cryptographic key handling & storage
	3	FCS_COP_(EXT).1	Random number generation
FDP	4	FDP_PUD_(EXT).1	Protection of User Data
FIA	5	FIA_UAU_(EXT).5	Multiple authentication mechanisms
FPT	6	FPT_STM_(EXT).1	Reliable time stamps
	7	FPT_TST_(EXT).1	TSF testing
	8	FTP_ITC_(EXT).1	Inter-TSF trusted channel

5.1.1 Class FCS: Cryptographic support

See Section 10 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3

5.1.1.1 FCS_BCM_(EXT).1 – Extended: Baseline Cryptographic Module

5.1.1.1.1 Family: Baseline Cryptographic Modules (FCS_BCM)

This family defines the validation and certification of the cryptographic modules implemented in the TOE.

5.1.1.1.2 Management

The following actions could be considered for the management functions in FMT:

- There are no management activities foreseen.

5.1.1.1.3 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- There are no auditable events foreseen.

5.1.1.1.4 Definition

FCS_BCM_(EXT).1 – Extended: Baseline Cryptographic Module

Hierarchical to: No other components.

Dependencies: None.

FCS_BCM_(EXT).1.1 All FIPS-approved cryptographic functions implemented by the TOE shall be implemented in a cryptomodule that is FIPS 140-2 validated, and perform the specified cryptographic functions in a FIPS-approved mode of operation. The FIPS 140-2 validation shall include an algorithm validation certificate for all FIPS-approved cryptographic functions implemented by the TOE.

FCS_BCM_(EXT).1.2 All cryptographic modules implemented in the TOE ***[***

selection:

(1) Entirely in hardware shall have a minimum overall rating of FIPS PUB 140-2, Level 3,

(2) Entirely in software shall have a minimum overall rating of FIPS PUB 140-2, Level 1; also meet FIPS PUB 140-2, Level 3 for selections Roles, Services and Authentication; and Design Assurance. The logical interfaces used for the input and output of plaintext cryptographic key components, authentication data, and CSPs shall be logically separated from all other interfaces using a trusted path or AS02.16 must be satisfied; where "trusted path" is interpreted to include a communications channel established using a FIPS 140-2 Level 2 cryptographic module and the HTTPS protocol between the cryptomodule and the external IT entity.

(3) As a combination of hardware and software shall have a minimum overall rating of FIPS PUB 140-2, Level 1 and also meet FIPS PUB 140-2, Level 3 for the following: Roles, Services and Authentication; and Design Assurance. The logical interfaces used for the input and output of plaintext cryptographic key components, authentication data, and CSPs shall be logically separated from all other interfaces using a trusted path or AS02.16 must be satisfied; where "trusted path" is interpreted to include a communications channel established using a FIPS 140-2 Level 2 cryptographic module and the HTTPS protocol between the cryptomodule and the external IT entity.

]

5.1.1.1.5 Rationale

FCS_BCM_(EXT).1 is based on PD-0164. It deviates from the original U. S. Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007 since the original FIPS 140-2 level requirement on Crypto Module is not always attainable.

This extended requirement is necessary since the CC does not provide a means to specify a cryptographic baseline of implementation.

5.1.1.2 FCS_CKM_(EXT).2 – Extended: Cryptographic Key Handling and Storage

5.1.1.2.1 Family: Cryptographic key management (FCS_CKM)

See Section 10.1 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.1.1.2.2 Management

The following actions could be considered for the management functions in FMT:

- There are no management activities foreseen.

5.1.1.2.3 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Success and failure of the activity.
- Basic: The object attribute(s) and object value(s) excluding any sensitive information (e.g. secret or private keys).

5.1.1.2.4 Definition

FCS_CKM_(EXT).2 – Extended: Cryptographic Key Handling and Storage

Hierarchical to: No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation

FCS_CKM.4 Cryptographic key destruction

FCS_CKM_(EXT).2.1 The TSF shall perform a key error detection check on each transfer of key (internal, intermediate transfers).

FCS_CKM_(EXT).2.2 The TSF shall store persistent secret and private keys when not in use in encrypted form or using split knowledge procedures.

FCS_CKM_(EXT).2.3 The TSF shall destroy non-persistent cryptographic keys after a cryptographic administrator-defined period of time of inactivity.

FCS_CKM_(EXT).2.4 The TSF shall prevent archiving of expired (private) signature keys.

5.1.1.2.5 Rationale

FCS_CKM_(EXT).2 is taken from the U. S. Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007.

This extended requirement is necessary since the CC does not specifically provide components for key handling and storage.

5.1.1.3 FCS_COP_(EXT).1 – Extended: Random number generation

5.1.1.3.1 Family: Cryptographic operation (FCS_COP)

See Section 10.2 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.1.1.3.2 Management

The following actions could be considered for the management functions in FMT:

- There are no management activities foreseen.

5.1.1.3.3 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Success and failure, and the type of cryptographic operation.
- Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.

5.1.1.3.4 Definition

FCS_COP_(EXT).1 – Extended: Random number generation

Hierarchical to: No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP_(EXT).1.1 The TSF shall perform all random number generation (RNG) services in accordance with a FIPS-approved RNG **[assignment: one of the RNGS specified in FIPS 140-2 Annex C]** seeded by ***[selection:***

(1) one or more independent hardware-based entropy sources, and/or

(2) one or more independent software-based entropy sources, and/or

(3) a combination of hardware-based and software-based entropy sources.]

FCS_COP_(EXT).1.2 The TSF shall defend against tampering of the random number generation (RNG) / pseudorandom number generation (PRNG) sources.

5.1.1.3.5 Rationale

FCS_COP_(EXT).1 is taken from the U. S. Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007.

This extended requirement is necessary since the CC cryptographic operation components address only specific algorithm types and operations requiring specific key sizes.

5.1.2 Class FDP: User data protection

See Section 11 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3

5.1.2.1 FDP_PUD_(EXT).1 – Extended: Protection of User Data

5.1.2.1.1 Family: Protection of User Data (FDP_PUD)

This family defines what user data is encrypted and decryption by the TSF when encryption is enabled.

5.1.2.1.2 Management

The following actions could be considered for the management functions in FMT:

- There are no management activities foreseen.

5.1.2.1.3 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- There are no auditable events foreseen.

5.1.2.1.4 Definition

FDP_PUD_(EXT).1 – Extended: Protection of User Data

Hierarchical to: No other components.

Dependencies: FCS_COP_(EXT).2 Extended: Random number generation

FDP_PUD_(EXT).1.1 When the administrator has enabled encryption, the TSF shall:

a) Encrypt authenticated user data transmitted to a wireless client from the radio interface of the wireless access system using the cryptographic algorithm(s) specified in FCS_COP_(EXT).2;

b) Decrypt authenticated user data received from a wireless client by the radio interface of the wireless access system using the cryptographic algorithm(s) specified in FCS_COP_(EXT).2.

5.1.2.1.5 Rationale

FDP_PUD_(EXT).1 is taken from the U. S. Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007.

This extended requirement is necessary because the Common Criteria IFC/AFC requirements do not accommodate access control policies that are not object/attribute based. The FDP_PUD_(EXT).1 requirement allows the administrator to determine whether or not to encrypt authenticated user data.

5.1.3 Class FIA: Identification and authentication

See Section 12 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.1.3.1 FIA_UAU_(EXT).5 – Extended: Multiple authentication mechanisms

5.1.3.1.1 Family: User authentication (FIA_UAU)

See Section 12.4 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.1.3.1.2 Management

The following actions could be considered for the management functions in FMT:

- The management of authentication mechanisms;
- The management of the rules for authentication.

5.1.3.1.3 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: The final decision on authentication;
- Basic: The result of each activated mechanism together with the final decision.

5.1.3.1.4 Definition

FIA_UAU_(EXT).5 – Extended: Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: None.

FIA_UAU_(EXT).5.1 The TSF shall provide local authentication, and a remote authentication mechanism to perform user authentication.

FIA_UAU_(EXT).5.2 The TSF shall, at the option of the administrator, invoke the remote authentication mechanism for administrators and wireless LAN users.

5.1.3.1.5 Rationale

FIA_UAU_(EXT).5 is taken from the U. S. Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007.

This extended requirement is needed for local administrators because there is concern over whether or not existing CC requirements specifically require that the TSF provide authentication. Authentication provided by the TOE is implied by other FIA_UAU requirements and is generally assumed to be a requirement when other FIA_UAU requirements are included in a TOE. In order to remove any potential confusion about this PP, an extended requirement for authentication has been included. This PP also requires the IT environment to provide an authentication server to be used for authentication of remote users. It is important to specify that the TSF must provide the means for local administrator authentication in case the TOE cannot communicate with the authentication server. In addition, the TOE must provide the portions of the authentication mechanism necessary to obtain and enforce an authentication decision from the IT environment.

5.1.4 Class FPT: Protection of the TSF

See Section 15 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.1.4.1 FPT_STM_(EXT).1 – Extended: Reliable time stamps

5.1.4.1.1 Family: Time stamps (FPT_STM)

See Section 15.10 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.1.4.1.2 Management

The following actions could be considered for the management functions in FMT:

- Management of the time.

5.1.4.1.3 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: changes to the time;
- Detailed: providing a timestamp.

5.1.4.1.4 Definition

FPT_STM_(EXT).1 – Extended: Reliable time stamps

Hierarchical to: No other components.

Dependencies: None.

FPT_STM_(EXT).1.1 The TSF shall be able to provide reliable time stamps, synchronized via an external time source, for its own use.

5.1.4.1.5 Rationale

FPT_STM_(EXT).1 is taken from the U. S. Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007.

This extended requirement is needed since the FPT_STM.1 requirement as specified in CC Version 3.1 R3 does not require that the time stamps provided by the TOE be synchronized via an external time source.

5.1.4.2 FPT_TST_(EXT).1 – Extended: TSF Testing

5.1.4.2.1 Family: TSF self test (FPT_TST)

See Section 15.14 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3

5.1.4.2.2 Management

The following actions could be considered for the management functions in FMT:

- Management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions;
- Management of the time interval if appropriate.

5.1.4.2.3 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Basic: Execution of the TSF self tests and the results of the tests.

5.1.4.2.4 Definition

FPT_TST_(EXT).1 – Extended: TSF Testing

Hierarchical to: No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FPT_TST_(EXT).1.1 The TSF shall run a suite of self tests during the initial start-up and also either periodically during normal operation, or at the request of an authorized administrator to demonstrate the correct operation of the TSF.

FPT_TST_(EXT).1.2 The TSF shall provide authorized administrators with the capability to verify the integrity of stored TSF executable code through the use of the TSF-provided cryptographic services.

5.1.4.2.5 Rationale

FPT_TST_(EXT).1 is taken from the U. S. Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007.

This extended requirement is needed since the FPT_TST.1 requirement as specified in CC Version 3.1 R3 does not require that the integrity of the TSF executable code be verified by the TSF's cryptographic functionality.

5.1.5 Class FTP: Trusted path/channels

See Section 18 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.1.5.1 FTP_ITC_(EXT).1 – Extended: Inter-TSF trusted channel

5.1.5.1.1 Family: Inter-TSF trusted channel (FTP_ITC)

See Section 18.1 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.1.5.1.2 Management

The following actions could be considered for the management functions in FMT:

- Configuring the actions that require trusted channel, if supported.

5.1.5.1.3 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Failure of the trusted channel functions.
- Minimal: Identification of the initiator and target of failed trusted channel functions.
- Basic: All attempted uses of the trusted channel functions.
- Basic: Identification of the initiator and target of all trusted channel functions.

5.1.5.1.4 Definition

FTP_ITC_(EXT).1 – Extended: Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: None.

FTP_ITC_(EXT).1.1 The TOE shall provide an encrypted communication channel between itself and entities in the TOE IT Environment that is logically distinct from other communication

channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC_(EXT).1.2 The TSF shall permit the TSF, or the IT Environment entities to initiate communication via the trusted channel.

FTP_ITC_(EXT).1.3 The TSF shall initiate communication via the trusted channel for all authentication functions, remote logging, time, ***[selection:*** **[assignment: communications with authorized IT entities determined by the ST author]*, none].***

5.1.5.1.5 Rationale

FTP_ITC_(EXT).1 is taken from the U. S. Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007.

This extended requirement is necessary because the existing trusted channel requirement is written with the intent of protecting communication between distributed portions of the TOE rather than between the TOE and its trusted IT environment.

5.2 Security Server Extended Components Definition

This section defines the extended requirements for the Security Server, when it is included in the TOE.

To avoid confusion, the extension "_(SS)" is used for the Security Server extended requirements, whereas "_(EXT)" is used for the Wireless Access Point extended requirements.

Extended components for the Security Server have been modeled on components from the U.S. Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007 (WLAN PP), the US Government Family of Protection Profiles for Public Key Enabled Applications, and CC Part2.

Table 5-2: Security Server Extended Components

SFR Class	Item #	SFR ID	SFR Title
FCS	1	FCS_BCM_(SS).1	Extended: Baseline cryptographic module
	2	FCS_COP_(SS).1	Extended: Random number generation
FDP	3	FDP_CPD_(SS).1	Extended: Certificate path development
	4	FDP_DAU_CPL_(SS).1	Extended: Certificate path initialisation – basic
	5	FDP_DAU_CPV_(SS).1	Extended: Intermediate certificate processing - basic
	6	FDP_DAU_CPV_(SS).2	Extended: Certificate processing - basic
	7	FDP_DAU_CPV_(SS).1	Extended: Certificate path output - basic
	8	FDP_DAU_CRL_(SS).	Extended: Basic CRL Checking
	9	FDP_DAU_OCS_(SS).1	Extended: Basic OCSP Client
	10	FDP_ITC_SIG_(SS).1	Extended: Import of PKI Signature
FPT	11	FPT_TST_(SS).1	Extended: Security server testing
FTP	12	FTP_ITC_(SS).1	Extended: Security server trusted channels

5.2.1 Class FCS: Cryptographic support

See Section 10 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.2.1.1 FCS_BCM_(SS).1 – Extended: Baseline Cryptographic Module

5.2.1.1.1 Family: Baseline Cryptographic Modules (FCS_BCM)

This family defines the validation and certification of the cryptographic modules implemented in the TOE.

5.2.1.1.2 Management

The following actions could be considered for the management functions in FMT:

- There are no management activities foreseen.

5.2.1.1.3 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- There are no auditable events foreseen.

5.2.1.1.4 Definition

FCS_BCM_(SS).1 – Extended: Baseline Cryptographic Module

Hierarchical to: No other components.

Dependencies: None.

FCS_BCM_(SS).1.1 All FIPS-approved cryptographic functions implemented by the Security Server shall be implemented in a cryptomodule that is FIPS 140-2 validated, and perform the specified cryptographic functions in a FIPS-approved mode of operation. The FIPS 140-2 validation shall include an algorithm validation certificate for all FIPS-approved cryptographic functions implemented by the TOE.

FCS_BCM_(SS).1.2 All cryptographic modules implemented in the Security Server ***[***

selection:

(1) Entirely in hardware shall have a minimum overall rating of FIPS PUB 140-2, Level 3,

(2) Entirely in software shall have a minimum overall rating of FIPS PUB 140-2, Level 1; also meet FIPS PUB 140-2, Level 3 for selections Roles, Services and Authentication; and Design Assurance. The logical interfaces used for the input and output of plaintext cryptographic key components, authentication data, and CSPs shall be logically separated from all other interfaces using a trusted path or AS02.16 must be satisfied; where "trusted path" is interpreted to include a communications channel established using a FIPS 140-2 Level 2 cryptographic module and the HTTPS protocol between the cryptomodule and the external IT entity.

(3) As a combination of hardware and software shall have a minimum overall rating of FIPS PUB 140-2, Level 1 and also meet FIPS PUB 140-2, Level 3 for the following: Roles, Services and Authentication; and Design Assurance. The logical interfaces used for the input and output of plaintext cryptographic key components, authentication data, and CSPs shall be logically separated from all other interfaces using a trusted path or AS02.16 must be satisfied; where "trusted path" is interpreted to include a communications channel established using a FIPS 140-2 Level 2 cryptographic module and the HTTPS protocol between the cryptomodule and the external IT entity.

]

5.2.1.1.5 Rationale

FCS_BCM_(EXT).1 is based on PD-0164. It deviates from the original U. S. Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007 since the original FIPS 140-2 level requirement on Crypto Module is not always attainable.

This extended requirement is necessary since the CC does not provide a means to specify a cryptographic baseline of implementation.

5.2.1.2 FCS_CKM_(SS).2 – Extended: Cryptographic Key Handling and Storage

5.2.1.2.1 Family: Cryptographic key management (FCS_CKM)

See Section 10.1 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.2.1.2.2 Management

The following actions could be considered for the management functions in FMT:

- There are no management activities foreseen.

5.2.1.2.3 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Success and failure of the activity.
- Basic: The object attribute(s) and object value(s) excluding any sensitive information (e.g. secret or private keys).

5.2.1.2.4 Definition

FCS_CKM_(SS).2 – Extended: Cryptographic Key Handling and Storage

Hierarchical to: No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM_(SS).2.1 The Security Server shall perform a key error detection check on each transfer of key (internal, intermediate transfers). The TOE performs an odd parity check on every transfer of key material, both internal and intermediate key transfers.

FCS_CKM_(SS).2.2 The Security Server shall store persistent secret and private keys when not in use in encrypted form or using split knowledge procedures.

FCS_CKM_(SS)_2.3 The Security Server shall destroy non-persistent cryptographic keys after a cryptographic administrator-defined period of time of inactivity.

Application Note: The cryptographic administrator must have the ability to set a threshold of inactivity after which non-persistent keys must be destroyed in accordance with FCS_CKM.4.

FCS_CKM_(SS).2.4 The Security Server shall prevent archiving of expired (private) signature keys.

5.2.1.2.5 Rationale

FCS_CKM_(SS).2 is taken from the U. S. Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007.

This extended requirement is necessary since the CC does not specifically provide components for key handling and storage.

5.2.1.3 FCS_COP_(SS).1 – Extended: Random number generation

5.2.1.3.1 Class FCS: Cryptographic key management

See Section 10 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.2.1.3.2 Family: Cryptographic operation (FCS_COP)

See Section 10.2 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.2.1.3.3 Management

The following actions could be considered for the management functions in FMT:

- There are no management activities foreseen.

5.2.1.3.4 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Success and failure, and the type of cryptographic operation.
- Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.

5.2.1.3.5 Definition

FCS_COP_(SS).1 – Extended: Random number generation

Hierarchical to: No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP_(SS).1.1 The Security Server shall perform all random number generation (RNG) services in accordance with a FIPS-approved RNG **[assignment: one of the RNGS specified in FIPS 140-2 Annex C]** seeded by ***[selection:***

a) one or more independent hardware-based entropy sources, and/or

b) one or more independent software-based entropy sources, and/or

c) a combination of hardware-based and software-based entropy sources.]

FCS_COP_(SS).1.2 The Security Server shall defend against tampering of the random number generation (RNG) / pseudorandom number generation (PRNG) sources.

5.2.1.3.6 Rationale

FCS_COP_(SS).1 is taken from the U. S. Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007.

This extended requirement is necessary since the CC cryptographic operation components address only specific algorithm types and operations requiring specific key sizes.

5.2.2 Class FDP: User data protection

See Section 11 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3 for a description of the FDP class.

All of the extended requirements in the FDP Class for the Security Server were taken from the US Government Protection Profile for Public-Key Enabled Applications for Basic Robustness Environments (PKE PP).

The requirements from the following packages of the PKE PP were included in this Security Target:

- Certificate Path Validation – Basic Package
- Certificate Revocation List (CRL) Validation Package
- Online Certificate Status Protocol (OCSP) Client Package
- PKI Signature Verification Package

The PKE PP specifies the following FMT SFRs for the IT environment.

- Management of the audit function
- Management of security attributes
- Static attribute initialization
- Management of I&A data
- Management of Authentication data
- Management of I&A attempts
- Management of Trust Anchors
- Management of Time

These requirements have been incorporated into the Security Management (FMT) SFRs for the Security Server

Audit requirements for each SFR are as specified by the Audit Package of the PKE PP and have been included with the definitions of the extended SFR components in this section and as assignments for the Security Server FAU_GEN.1 (SS) Audit Generation component.

5.2.2.1 Introduction to Certificate Path Validation – Basic Package

The following SFRs are from the Certification Path Validation – Basic Package of the PKE PP.

- *FDP_CPD_(SS).1 Certification path development*
- *FDP_DAU_CPI_(SS).1 Certification path initialisation -- basic*
- *FDP_DAU_CPV_(SS).1 Extended: Certificate processing - basic*
- *FDP_DAU_CPV_(SS).2 Intermediate certificate processing -- basic*
- *FDP_DAU_CPO_(SS).1) Certification path output -- basic*

The text below is taken from the PKE PP. The text states the purpose of the package and explains the relationship between the SFRs in the package.

> *"The functions in this package address the validation of the certification path. Certification path development is also a part of this package. It is realized that the most likely implementations consist of developing a path (using a variety of techniques) and then validating the certification path. It is further recognized that certification path validation generally consists of validating certificates starting with the one certified by a trust anchor and ending with the one issued to the subscriber of interest. However, in order to be implementation neutral, this package does not mandate any ordering of certification path development and certification validation processes. A compliant implementation will only need to meet the security requirements specified in this package.*
>
> *"All processing defined is X.509 and PKIX compliant. The certification path validation in these standards is procedural, but in keeping with the spirit of functional specification, certification path validation requirements are specified using non-procedural techniques.*
>
> *"From certification path processing perspective, certificates can be of up to three types:*
>
> - *Self-signed trust anchor certificate: The trust anchor can be in the form of a self-signed certificate. The trust anchor is used to obtain the Distinguished Name (DN), public key, algorithm identifier, and the public key parameters (if applicable). This package permits validation of trust anchor if it is in the form of self-signed certificate, including validating signature and verifying that the self-signed certificate validity period has not expired.*
> - *Intermediate certificates: These are the certificates issued to the CAs. All certificates in a certification path are intermediate certificates, except the last one.*
> - *End certificate: This is the last certificate in the certification path and is issued to the subscriber of interest. This is typically an end-entity (i.e., not a CA) certificate. However, this package permits that certificate to be a CA certificate also.*
>
> *"This package processes the following security related certificate extensions checks:*
>
> - *no-check,*
> - *keyUsage,*

- *extendedKeyUsage, and*
- *basicConstraints.*

"This PKE PP family provides the capability to validate path as of a user-defined time called TOI which can be current time or earlier.

"If revocation checking is selected, this package may depend on one or both of OCSP Client and CRL validation packages."

The definitions of the Security Functional Requirements have been copied from the PKE along with the text of all the selections and assignment to be completed by the ST author. The selections and assignments are completed in Section 6 Security Requirements.

5.2.2.2 FDP_CPD_(SS).1 Extended: Certification path development

5.2.2.2.1 Family: Certificate Path Development (FDP_CPD)

This family specifies the steps for building a trusted path between the trust anchor and the end certificate.

5.2.2.2.2 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Success or failure to build path and for success, matching rules bypassed.

5.2.2.2.3 Definition

FDP_CPD_(SS).1 Extended: Certification path development

Hierarchical to: No other components.

Dependencies: None

FDP_CPD_(SS).1.1 The Security Server shall develop a certification path from a trust anchor provided by ***[selection of one or more by the ST author: user; administrator,*** **[assignment by the ST author: other role defined]*]*** to the subscriber using matching rules for the following subscriber certificate fields or extensions: ***[selection of one or more by the ST author: distinguished name, subject alternative names, subject key identifier, subject public key algorithm, certificate policies,*** **[assignment by the ST author: other certificate fields or extensions]*].***

FDP_CPD_(SS).1.2 The Security Server shall develop the certification path using the following additional matching rule: ***[selection of one by the ST author:***

a) none,

b) keyUsage extension has nonRepudiation bit set,

c) keyUsage extension has digitalSignature bit set,

d) keyUsage extension has keyEncipherment bit set,

e) key Usage extension has keyAgreement bit set].

FDP_CPD_(SS).1.3 The Security Server shall develop the certification path using the following additional matching rule ***[selection of one by the ST author:***

a) none,

b) extendedKeyUsage extension contains EFS or anyExtendedKeyUsage OID,

c) extendedKeyUsage extension contains SCL or anyExtendedKeyUsage OID,

d) extendedKeyUsage extension contains code signing or anyExtendedKeyUsage OID,

e) extendedKeyUsage extension contains OCSP signing or anyExtendedKeyUsage OID,

f) [assignment by the ST author: other extended key usage OID related matching rules]*].*

FDP_CPD_(SS).1.4 The Security Server shall bypass any matching rules except ***[selection of one or more by the ST author: distinguished name, subject alternative names, subject key identifier, subject public key algorithm, certificate policies,*** **[assignment by the ST author: other certificate fields or extensions],** ***none]*** if additional certification paths are required.

Application Note: In FDP_CPD_(SS).1.2, the assignment nonRepudiation should be used if the path is being developed for signature verification; the assignment digitalSignature should be used if the path is being developed for entity authentication; the assignment keyEncipherment, should be used if the path is being developed for encryption certificate using a key transfer algorithm (e.g., RSA); the assignment keyAgreement should be used if the path is being developed for encryption certificate using a key calculation algorithm (e.g., DH, ECDH).

In FDP_CPD_(SS).1.3, the selection of the matching rule should be made depending on the PKE application requirement. anyExtendedKeyUsage is a match for any application.

5.2.2.2.4 Rationale

This SFR was taken from the Certification Path Validation – Basic Package of the Public-Key Enabled Applications (PKE PP) for Basic Robustness Environments.

This requirement had to be explicitly stated because the CC does not contain requirements that are defined to be compliant with ISO X.509 and IETF RFC 3280.

5.2.2.3 FDP_DAU_CPI_(SS).1 Extended: Certification path initialisation -- basic

5.2.2.3.1 Family: Data Authentication (FDP_DAU)

See Section 11.3 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3 for the behavior of the FDP_DAU family.

5.2.2.3.2 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- There are no auditable events foreseen.

5.2.2.3.3 Definition

FDP_DAU_CPI_(SS).1 Extended: Certification path initialisation -- basic

Hierarchical to: No other components.

Dependencies:

FCS_COP.1

FPT_STM.1

FDP_DAU_CPI_(SS).1.1 The Security Server shall use the trust anchor provided by ***[selection of one or more by the ST author: user, administrator*, [assignment by the ST author: other role(s) defined]*].***

FDP_DAU_CPI_(SS).1.2 The Security Server shall obtain the time of interest called "TOI' from a reliable source ***[selection of one by the ST author: local environment,* [assignment by ST author: other sources defined by ST author]*].***

FDP_DAU_CPI_(SS).1.3 The Security Server shall perform the following checks on the trust anchor ***[selection of one or more by the ST author:***

- ***a) None;***
- ***b) Subject DN and Issuer DN match;***
- ***c) Signature verifies using the subject public key and parameter (if applicable) from the trust anchor;***
- ***d) notBefore field in the trust anchor <= TOI;***
- ***e) notAfter field in the trust anchor => TOI]***

FDP_DAU_CPI_(SS).1.4 The Security Server shall derive from the trust anchor ***[selection of one or more by the ST author: subject DN, subject public key, subject public key algorithm object identifier, subject public key parameters]***

Application Note: While the PP requires the environment to provide accurate time to required precision, the ST author can choose other sources of accurate time

5.2.2.3.4 Rationale

This SFR was taken from the Certification Path Validation – Basic Package of the Public-Key Enabled Applications (PKE PP) for Basic Robustness Environments.

This requirement had to be explicitly stated because the CC does not contain requirements that are defined to be compliant with ISO X.509 and IETF RFC 3280.

5.2.2.4 FDP_DAU_CPV_(SS).1 Extended: Certificate processing - basic

5.2.2.4.1 Family: Data authentication (FDP_DAU)

See Section 11.3 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3 for the behavior of the FDP_DAU family.

5.2.2.4.2 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Success or failure of certificate processing and for failure, reason(s) for failure.
- Bypass of revocation status checking

5.2.2.4.3 Definition

FDP_DAU_CPV_(SS).1 Extended: Certificate processing - basic

Hierarchical to: No other components.

Dependencies:

FCS_COP.1

FPT_STM.1

[FDP_DAU_OCS_(SS).1 or

FDP_DAU_CRL_(SS).1]

FDP_DAU_CPV_(SS).1.1 The Security Server shall reject a certificate if any of the following checks fails:

a) Use parent-public-key, parent-public-key-algorithm-identifier, and parent-public-key-parameters to verify the signature on the certificate;

b) notBefore field in the certificate < = TOI;

c) notAfter field in the certificate > = TOI;

d) issuer field in the certificate = parent-DN; or

e) Security Server is able to process all extensions marked critical

FDP_DAU_CPV_(SS).1.3 The Security Server shall bypass the revocation check if the revocation information is not available.

FDP_DAU_CPV_(SS).1.4 The Security Server shall reject a certificate if the revocation status using ***[selection of one or more by the ST author: CRL, OCSP]*** demonstrates that the certificate is revoked.

FDP_DAU_CPV_(SS).1.5 The Security Server shall update the public key parameters state machine using the following rules:

a) Obtain the parameters from the subjectPublickeyInfo field of certificate if the parameters are present in the field; else

b) Retain the old parameters state if the subject public key algorithm of current certificate and parent public key algorithm of current certificate belong to the same family of algorithms, else

c) Set parameters = “null”.

Application Note: While each certificate is expected to be checked using only one of the revocation mechanisms, each certificate in a certification path can be checked using different revocation mechanism. That is why the selection is one or more.

5.2.2.4.4 Rationale

This SFR was based on the FDP on the FDP_DAU_CPV_(SS).1 from the Certification Path Validation – Basic Package of the Public-Key Enabled Applications (PKE PP) for Basic Robustness Environments. Element 1.2 was deleted and element 1.3 was updated to specify the TOE behavior correctly.

This requirement had to be explicitly stated because the CC does not contain requirements that are defined to be compliant with ISO X.509 and IETF RFC 3280.

5.2.2.5 FDP_DAU_CPV_(SS).2 Extended: Intermediate certificate processing -- basic

5.2.2.5.1 Family: Data authentication (FDP_DAU)

See Section 11.3 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3 for the behavior of the FDP_DAU family.

5.2.2.5.2 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Success or failure of certificate processing and for failure, reason(s) for failure.

5.2.2.5.3 Definition

FDP_DAU_CPV_(SS).2 Extended: Intermediate certificate processing -- basic

Hierarchical to: No other components.

Dependencies: FDP_DAU_CPV_(SS).1

FDP_DAU_CPV_(SS).2.1 The Security Server shall reject an intermediate certificate if any of the following additional checks fails:

a) basicConstraints field is present with cA = TRUE;

b) pathLenConstraint is not violated; or

c) if a critical keyUsage extension is present, keyCertSign bit is set

5.2.2.5.4 Rationale

This SFR was taken from the Certification Path Validation – Basic Package of the Public-Key Enabled Applications (PKE PP) for Basic Robustness Environments.

This requirement had to be explicitly stated because the CC does not contain requirements that are defined to be compliant with ISO X.509 and IETF RFC 3280.

5.2.2.6 FDP_DAU_CPO_(SS).1) Extended: Certification path output -- basic

5.2.2.6.1 Family: Data authentication (FDP_DAU)

See Section 11.3 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3 for the behavior of the FDP_DAU family.

5.2.2.6.2 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- There are no auditable events foreseen.

5.2.2.6.3 Definition

FDP_DAU_CPO_(SS).1) Extended: Certification path output -- basic

Hierarchical to: No other components.

Dependencies: FDP_DAU_CPV_(SS).1

FDP_DAU_CPO_(SS).1.1 The Security Server shall output certification path validation failure if any certificate in the certification path is rejected.

FDP_DAU_CPO_(SS).1.2 The Security Server shall output the following variables from the end certificate: subject DN, subject public key algorithm identifier, subject public key, critical keyUsage extension.

FDP_DAU_CPO_(SS).1.3 The Security Server shall output the following additional variables from the end certificate ***[selection of one or more by the ST author: certificate, subject alternative names, extendedKeyUsage,*** **[assignment by the ST author: other information]*].***

FDP_DAU_CPO_(SS).1.4 The Security Server shall output the subject public key parameters from the certification path parameter state machine.

5.2.2.6.4 Rationale

This SFR was taken from the Certification Path Validation – Basic Package of the Public-Key Enabled Applications (PKE PP) for Basic Robustness Environments.

This requirement had to be explicitly stated because the CC does not contain requirements that are defined to be compliant with ISO X.509 and IETF RFC 3280.

5.2.2.7 FDP_DAU_CRL_(SS).1 Extended: Basic CRL Checking

This component is from the Certificate Revocation List (CRL) Validation Package of the PKE PP. The PKE PP provides the following the introduction to the package.

> *"This package is used for validating a CRL. This version of the document does not require processing of CRL issuing distribution point (IDP) CRL or delta CRL. Future versions may include that capability by codifying Annex B of X.509 standard.*
>
> *"It should be noted that this package may be used to process a CRL that is pointed to by a CRL Distribution Point (CRLDP) extension in a certificate as long as the CRL is a full CRL, indicated by the absence of IDP and deltaCRLIndicator extensions.*
>
> *"This package permits the use of the same public key for CRL signature verification as the one used for verifying the signature on the certificate, but does not mandate it. In other words, a compliant implementation can use that or develop a certification path. If the compliant implementation develops a certification path, then CPV – Basic and other CPV packages may also be applicable, depending upon the implementation..*
>
> *"The ST author can assign additional rules to process Issuing Distribution Point CRL and Delta CRL."*

5.2.2.7.1 Family: Data authentication (FDP_DAU)

See Section 11.3 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3 for the behavior of the FDP_DAU family.

5.2.2.7.2 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Rejection of CRL and reason for rejection

- Override of time checks

5.2.2.7.3 Definition

FDP_DAU_CRL_(SS).1 Extended: Basic CRL Checking

Hierarchical to no other component

Dependencies:

FCS_BCM_(SS).1

FPT_STM.1

FDP_DAU_CRL_(SS).1.1 The Security Server shall obtain the CRL from ***[selection of one or more by the ST author: local cache, repository, location pointed to by the CRL DP in public key certificate of interest, user,*** **[assignment: other locations defined by the ST author]*].***

FDP_DAU_CRL_(SS).1.2 The Security Server shall obtain the trusted public key, algorithm, and public key parameters of the CRL issuer.

FDP_DAU_CRL_(SS).1.3 The Security Server shall invoke the cryptographic module to verify signature on the CRL using trusted public key, algorithm, and public key parameters of the CRL issuer.

FDP_DAU_CRL_(SS).1.4 The Security Server shall verify that if a critical keyUsage extension is present in CRL issuer certificate, cRLSign bit in the extension is set in the certificate.

FDP_DAU_CRL_(SS).1.5 The Security Server shall match the issuer field in the CRL with what it assumes to be the CRL issuer.

FDP_DAU_CRL_(SS).1.6 The Security Server shall reject the CRL if all of the following are true:

a) Time check are not overridden;

b) ***[selection of one by the ST author: always, TOI > thisUpdate + x where x [selection: =0, is provided by [selection by the ST author: user, administrator,*** **[assignment by the ST author: other role(s) defined]** ***]]];*** and

c) ***[selection of one by the ST author: always, TOI > nextUpdate + x if nextUpdate is present and where x [selection: =0, is provided by [selection by the ST author: user, administrator,*** **[assignment by the ST author: other role(s) defined]** ***]]].***

FDP_DAU_CRL_(SS).1.7 The Security Server shall permit ***[selection by the ST author: user, administrator,*** **[assignment by the ST author: other role(s) defined],** ***none]*** to override time checks.

FDP_DAU_CRL_(SS).1.8 The Security Server shall reject CRL if the CRL contains “critical” extension(s) that Security Server does not process.

FDP_DAU_CRL_(SS).1.9 The Security Server shall perform the following additional checks ***[selection of one or more by the ST author:***

a) none,

b) [assignment by ST author: other rule(s)]*].*

Application Note: The trusted public key, algorithm, and public key parameters of the CRL issuer should normally be the same as those used for verifying signature on the certificate being

checked for revocation. If not, at least certificate path development – basic can be used to obtain the public key.

5.2.2.7.4 Rationale

This SFR was modeled on the Certificate Revocation List (CRL) Package of the Public-Key Enabled Applications (PKE PP) for Basic Robustness Environments.

This requirement had to be explicitly stated because the CC does not contain requirements that are defined to be compliant with ISO X.509 and IETF RFC 3280.

5.2.2.8 FDP_DAU_OCS_(SS).1 Extended: Basic OCSP Client

This component is from the Online Certificate Status Protocol (OCSP) Client Package of the PKE PP. The PKE PP provides the following the introduction to the package.

> *"This package allows for making Online Certificate Status Protocol (OSCP) requests and validating OCSP responses. This package permits the use of the OCSP Responder as a trust anchor, as the CA, or an end entity authorized to sign OCSP responses. The ST author can assign additional rules to process OCSP extensions. If the OCSP implementation establishes trust in the OCSP responder by performing Certificate Path Validation, then CPV – Basic and other CPV packages may also be applicable, depending upon the implementation,"*

5.2.2.8.1 Family: Data authentication (FDP_DAU)

See Section 11.3 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3 for the behavior of the FDP_DAU family.

5.2.2.8.2 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Rejection of OCSP response and reason for rejection
- Override of time checks

5.2.2.8.3 Definition

FDP_DAU_OCS_(SS).1 Extended: Basic OCSP Client

Hierarchical to: No other component

Dependencies:

FCS_BCM_(SS).1

FPT_STM.1

FDP_DAU_OCS_(SS).1.1 The Security Server shall formulate the OCSP requests in accordance with PKIX RFC 2560.

FDP_DAU_OCS_(SS).1.2 The Security Server shall obtain the public key, algorithm, and public key parameters of the OCSP Responder from ***[selection of one by the ST author: trust anchor, certificate signing CA, OCSP responder certificate,*** **[assignment by ST author: other sources]*].***

FDP_DAU_OCS_(SS).1.3 The Security Server shall invoke the cryptographic module to verify signature on the OCSP response using trusted public key, algorithm, and public key parameters of the OCSP responder.

FDP_DAU_OCS_(SS).1.4 The Security Server shall verify that if the OCSP responder certificate contains extendedKeyUsage extension, the extension contains the PKIX OID for ocsp-signing or the anyExtendedKeyUsage OID.

FDP_DAU_OCS_(SS).1.5 The Security Server shall match the responderID in the OCSP response with the corresponding information in the responder certificate

FDP_DAU_OCS_(SS).1.6 The Security Server shall match the certID in a request with certID in singleResponse.

FDP_DAU_OCS_(SS).1.7 The Security Server shall reject the OCSP response for an entry if all of the following are true:

a) time checks are not overridden;

b) ***[selection of one by the ST author: always, TOI > producedAt + x where x [selection: =0, is provided by [selection by the ST author: user, administrator,*** **[assignment by the ST author: other role(s) defined]** ***]]];***

c) ***[selection of one by the ST author: always, TOI > thisUpdate for entry + x where x [selection: =0, is provided by [selection by the ST author: user, administrator,*** **[assignment by the ST author: other role(s) defined]** ***]]]; and***

d) ***[selection of one by the ST author: always, TOI > nextUpdate for entry + x if nextUpdate is present and where x [selection: =0, is provided by [selection by the ST author: user, administrator,*** **[assignment by the ST author: other role(s) defined]** ***]]].***

FDP_DAU_OCS_(SS).1.8 The Security Server shall reject OCSP response if the response contains “critical” extension(s) that Security Server does not process.

FDP_DAU_OCS_(SS).1.9 The Security Server shall perform the following additional checks ***[selection of one or more by the ST author:***

a) none,

b) request nonce = response nonce,

c) **[assignment by ST author: other rule(s)]** ***].***

FDP_DAU_OCS_(SS).1.10 The Security Server shall permit ***[selection of one or more by the ST author: user, administrator,*** **[assignment by the ST author: other role(s) defined],** ***none]*** to override time checks.

FDP_DAU_OCS_(SS).1.11 The Security Server shall reject OCSP response if the response contains “critical” extension(s) that Security Server does not process.

5.2.2.8.4 Rationale

This SFR was modeled on the Online Certificate Status Protocol Client Package of the Public-Key Enabled Applications (PKE PP) for Basic Robustness Environments.

This requirement had to be explicitly stated because the CC does not contain requirements that are defined to be compliant with ISO X.509 and IETF RFC 3280.

5.2.2.9 FDP_ITC_SIG_(SS).1 Extended: Import of PKI Signature

This SFR comes from the PKI Signature Verification package of the PKE PP. The PKE PP provides the following introduction to the PKI Signature Verification package.

> *"The PKI Signature Verification Package processes and verifies the signature information, and invokes a cryptographic module to verify digital signatures. This package is dependent upon the Certification Path Validation – Basic package. The signature verification package uses the Certification Path Validation package data as input."*

5.2.2.9.1 Family: Import from outside of the TOE (FDP_ITC)

See Section 11.7 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3 for a description of the behavior of the FDP_ITC family.

5.2.2.9.2 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- There are no auditable events foreseen.

5.2.2.9.3 Definition

FDP_ITC_SIG_(SS).1 Extended: Import of PKI Signature

Hierarchical to: No other component.

Dependencies: None.

FDP_ITC_SIG_(SS).1.1 The Security Server shall use the following information from the signed data ***[selection of one or more by the ST author: hashing algorithm, signature algorithm, signer public key certificate, signer DN, signer subject alternative name, signer subject key identifier,* [assignment by the ST author: other information]** ***]*** during signature verification.

5.2.2.9.4 Rationale

This SFR was taken from the PKI Signature Verification Package of the Public-Key Enabled Applications (PKE PP) for Basic Robustness Environments.

This requirement had to be explicitly stated because the CC does not contain a requirement that addresses digital signature verification.

5.2.3 Class FPT: Protection of the TSF

See Section 15 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3 for a description of the FPT class.

5.2.3.1 FPT_TST_(SS).1 – Extended: Security Server TSF Testing

5.2.3.1.1 Family: TSF Self Test (FPT_TST)

See Section 15.14 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3 for the behavior of the FPT_TST family.

5.2.3.1.2 Management

The following actions could be considered for the management functions in FMT:

- Management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions;
- Management of the time interval if appropriate.

5.2.3.1.3 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Basic: Execution of the TSF self tests and the results of the tests.

5.2.3.1.4 Definition

FPT_TST_(SS).1 – Extended: Security Server TSF Testing

Hierarchical to: No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FPT_TST_(SS).1.1 The Security Server shall run a suite of self-tests during the initial start-up and also either periodically during normal operation, or at the request of an authorized administrator to demonstrate the correct operation of the TSF.

FPT_TST_(SS).1.2 The Security Server shall provide authorized administrators with the capability to verify the integrity of stored TSF executable code through the use of the TSF-provided cryptographic services.

5.2.3.1.5 Rationale

FPT_TST_(SS).1 is taken from the U. S. Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007.

This extended requirement is needed since the FPT_TST.1 requirement as specified in CC Version 3.1 R3 does not require that the integrity of the TSF executable code be verified by the TSF's cryptographic functionality.

5.2.4 Class FTP: Trusted path/channels

See Section 18 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3

5.2.4.1 FTP_ITC_(SS).1 – Extended: Security Server trusted channels

5.2.4.1.1 Family: Inter-TSF trusted channel (FTP_ITC)

See Section 18.1 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3 for the behavior of the FDP_ITC family.

5.2.4.1.2 Management

The following actions could be considered for the management functions in FMT:

- Configuring the actions that require trusted channel, if supported.

5.2.4.1.3 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Failure of the trusted channel functions.
- Minimal: Identification of the initiator and target of failed trusted channel functions.
- Basic: All attempted uses of the trusted channel functions.
- Basic: Identification of the initiator and target of all trusted channel functions.

5.2.4.1.4 Definition

FTP_ITC_(SS).1 – Extended: Security Server trusted channels

Hierarchical to: No other components.

Dependencies: None.

FTP_ITC_(SS).1.1 The Security Server shall provide an encrypted communication channel between itself and entities in the TOE IT Environment that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC_(SS).1.2 The Security Server shall permit The Security Server, or the IT Environment entities to initiate communication via the trusted channel.

FTP_ITC_(SS).1.3 The Security Server shall initiate communication via the trusted channel for communication with OCSP responder.

5.2.4.1.5 Rationale

FTP_ITC_(SS).1 needed to be extended because the Security Server provides both internal trusted channels to other TOE components and external trusted channels to trusted components in the Operational Environment depending upon the configuration of the TOE.

6 Security Requirements

The following conventions have been applied in this document:

- **Security Functional Requirements** – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
- **Iteration**: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a reference in parenthesis placed at the end of the component. For example FIA_ATD.1 (1) and FIA_ATD.1 (2) indicate that the ST includes two iterations of the FIA_ATD.1 requirement, (1) and (2). The convention of (SS) is used for the iteration of components for the Security Server in Section 6.2, since these components may either be inside or outside of the TOE depending upon whether or not the 3eTI Security Server is used as the Authentication Server. Wireless Access Point SFRs from Part 2 that are also SFRs for the Security Server component of the TOE are iterated with a (1), even if they occur only once in the set of SFRs for the Wireless Access Point.
- **Assignment**: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., **[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**: are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text***.
- **Application notes** provide additional information for the reader, but do not specify requirements. Application notes are denoted by italicized text.

Note: Operations (i.e., assignments, selections and refinements) already completed in the Wireless Access Point Protection Profile are not identified by special formatting in this Security Target.

6.1 Wireless Access Point Security Functional Requirements

In this section, explicitly stated Security Functional Requirements (i.e., those not found in Part 2 of the CC) are identified "_(EXT)" in the component name.

The Access System security functional requirements are listed in the following table. All SFRs are based on requirements defined in Part 2 of the Common Criteria or the U. S. Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007.

Table 6-1: Wireless Access Point Security Functional Requirements

Functional Class	Functional Components	#
Security Audit (FAU)	FAU_GEN.1 (1) - Audit data generation (Wireless Access Point)	1
	FAU_GEN.2 (1) - User identity association (Wireless Access Point)	2
	FAU_SAR.1 (1) – Audit review (Wireless Access Point)	3
	FAU_SAR.3 (1) – Selectable audit review (Wireless Access Point)	4
	FAU_SEL.1 (1) - Selective audit (Wireless Access Point)	5
Cryptographic Support	FCS_BCM_(EXT).1 – Extended: Baseline Cryptographic Module	6

Functional Class	Functional Components	#
(FCS)	FCS_CKM.1 (1) - Cryptographic key generation (for symmetric keys on Wireless Access Point)	7
	FCS_CKM.1 (2) - Cryptographic key generation (for asymmetric keys on Wireless Access Point)	8
	FCS_CKM.2 (1) - Cryptographic key distribution (Wireless Access Point)	9
	FCS_CKM_(EXT).2 - Extended: Cryptographic key handling and storage	10
	FCS_CKM.4 (1) - Cryptographic key destruction (Wireless Access Point)	11
	FCS_COP.1 (1) – Cryptographic Operation (Data encryption/decryption on Wireless Access Point)	12
	FCS_COP.1 (2) – Cryptographic Operation (Digital Signature on Wireless Access Point)	13
	FCS_COP.1 (3) – Cryptographic Operation (Hashing on Wireless Access Point)	14
	FCS_COP.1 (4) – Cryptographic Operation (Key agreement on Wireless Access Point)	15
	FCS_COP.1 (5) – Cryptographic Operation (HMAC on Wireless Access Point)	16
	FCS_COP_(EXT).1 – Extended: Random Number Generation	17
User Data Protection (FDP)	FDP_PUD_(EXT).1 – Extended: Protection of User Data	18
	FDP_RIP.1 (1) - Subset residual information protection (Wireless Access Point)	19
Identification and Authentication (FIA)	FIA_AFL.1 (1) - Administrator authentication failure handling (Wireless Access Point)	20
	FIA_ATD.1 (1) - Administrator attribute definition (Wireless Access Point)	21
	FIA_ATD.1 (2) - User attribute definition (Wireless Access Point)	22
	FIA_UAU.1 (1) – Timing of local authentication	23
	FIA_UAU_(EXT).5 – Extended: Multiple authentication mechanisms	24
	FIA_UID.2 (1) - User identification before any action (Wireless Access Point)	25
	FIA_USB.1 (1) - User-subject binding (Administrator on Wireless Access Point)	26
	FIA_USB.1 (2) - User-subject binding (Wireless User on Wireless Access Point)	27
Security Management (FMT)	FMT_MOF.1 (1) - Management of security functions behavior (Wireless Access Point)	28
	FMT_MSA.2 (1) - Secure security attributes (Wireless Access Point)	29
	FMT_MTD.1 (1) - Management of TSF Data (Wireless Access Point)	30
	FMT_SMF.1 (1) - Specification of Management Functions (Wireless Access Point)	31
	FMT_SMR.1 (1) - Security roles (Wireless Access Point)	32
Protection of TSF (FPT)	FPT_STM_(EXT).1 – Extended: Reliable time stamps	33
	FPT_TST_(EXT).1 - Extended: TSF testing	34
	FPT_TST.1 (1)- TSF testing (for cryptography on Wireless Access Point)	35
	FPT_TST.1 (2) - TSF testing (for key generation components on Wireless Access Point)	36
TOE Access (FTA)	FTA_SSL.3 (1) - TSF-initiated termination (Wireless Access Point)	37
	FTA_TAB.1 (1) - Default TOE access banners (Wireless Access Point)	38
	FTA_TSE.1 – TOE Session Establishment	39

Functional Class	Functional Components	#
Trusted Path/Channels (FTP)	FTP_ITC_(EXT).1 (1) Extended: Inter-TSF trusted channel	40
	FTP_TRP.1 (1) Trusted Path (Wireless Access Point)	41

6.1.1 Security Audit (FAU) Requirements

6.1.1.1 FAU_GEN.1 (1) Audit data generation (Wireless Access Point)

FAU_GEN.1.1 (1) The TSF shall be able to generate an audit record of the following auditable events:

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

b) All auditable events for the minimum level of audit; and

c) **[All auditable events as shown in Table 6-2];**

Table 6-2: Auditable Events (Wireless Access Point)

#	Requirement	Auditable Events	Additional Audit Record Contents
1	FAU_GEN.1 (1)	None	N/A
2	FAU_GEN.2 (1)	None	N/A
3	FAU_SAR.1 (1)	None	N/A
4	FAU_SAR.3 (1)	None	N/A
5	FAU_SEL.1 (1)	All modifications to the audit configuration that occur while the audit collection functions are operating	The identity of the Administrator/Crypto-Officer performing the function
6	FCS_BCM_(EXT).1	None	N/A
7	FCS_CKM.1 (1)	Success and Failure of the cryptographic activity	The identity of the Administrator/Crypto-Officer performing the function
8	FCS_CKM.1 (2)	Success and Failure of the cryptographic activity	The identity of the Administrator/Crypto-Officer performing the function
9	FCS_CKM.2 (1)	Success and failure of the cryptographic activity	The identity of the Administrator/Crypto-Officer performing the function
10	FCS_CKM_(EXT).2	Error(s) detected during cryptographic key transfer	If available – the authentication credentials of subjects with which the invalid key is shared
11	FCS_CKM.4 (1)	Success and failure of the cryptographic activity	If available - the identity of the Administrator/Crypto-Officer performing the function
12	FCS_COP.1 (1)	None	N/A
13	FCS_COP.1 (2)	None	N/A
14	FCS_COP.1 (3)	None	N/A
15	FCS_COP.1 (4)	None	N/A
16	FCS_COP.1 (5)	None	N/A
17	FCS_COP_(EXT).1	None	N/A

#	Requirement	Auditable Events	Additional Audit Record Contents
18	FDP_PUD_(EXT).1	Enabling or disabling TOE encryption of wireless traffic	The identity of the Administrator/Crypto-Officer performing the function
19	FDP_RIP.1 (1)	None	N/A
20	FIA_AFL.1 (1)	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g., disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal)	None
21	FIA_ATD.1 (1)	None	N/A
22	FIA_ATD.1 (2)	None	N/A
23	FIA_UAU.1	Use of the authentication mechanism (success or failure)	User identity The TOE SHALL NOT record invalid passwords in the audit log
24	FIA_UAU_(EXT).5	Failure to receive a response from the remote authentication server	Identification of the Authentication server that did not reply
25	FIA_UID.2 (1)	None	N/A
26	FIA_USB.1 (1)	Unsuccessful binding of user security attributes to a subject	None
27	FIA_USB.1 (2)	Unsuccessful binding of user security attributes to a subject	None
28	FMT_MOF.1 (1)	Changing the TOE encryption algorithm including the selection not to encrypt communications Start or Stop of audit record generation Changes to the TOE remote authentication settings; Changes to the threshold of failed authentication attempts; Changes to the session lock timeframe	Encryption algorithm selected (or none) The identity of the Administrator/Crypto-Officer performing the function
29	FMT_MSA.2 (1)	All offered and rejected values for security attributes	None
30	FMT_MTD.1 (1)	Changes to the set of rules used to pre-select audit events. Changes to the TOE authentication credentials (administrator) Changes to the TOE authentication credentials (user)	The identity of the Administrator/Crypto-Officer performing the function The TOE SHALL NOT record authentication credentials in the audit log.
31	FMT_SMF.1 (1)	None	N/A
32	FMT_SMR.1 (1)	Modifications to the group of users that are part of a role	This event is logged in the System Log only.
33	FPT_STM_(EXT).1	Changes to the time	None
34	FPT_TST_(EXT).1	Execution of the self test	Success or Failure of test
35	FPT_TST.1 (1)	Execution of the self test	Success or Failure of test

#	Requirement	Auditable Events	Additional Audit Record Contents
36	FPT_TST.1 (2)	Execution of the self test	Success or Failure of test
37	FTA_SSL.3 (1)	TSF Initiated Termination User inactivity causing Termination is logged in the APs	Termination of an interactive session by the session locking mechanism.
38	FTA_TAB.1 (1)	None	N/A
39	FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism.	None
40	FTP_ITC_(EXT).1	Initiation/Closure of a trusted channel	Identification of the remote entity with which the channel was attempted/created; Success or failure of the event
41	FTP_TRP.1 (1)	Initiation of a trusted channel	Identification of the remote entity with which the channel was attempted/created; Success or failure of the event

FAU_GEN.1.2 (1) 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 (if applicable), and the outcome (success or failure) of the event; and

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

6.1.1.2 FAU_GEN.2 (1) User identity association (Wireless Access Point)

FAU_GEN.2.1 (1) For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_SAR.1 (1) Audit review (Wireless Access Point)

FAU_SAR.1.1 (1) The TSF shall provide **[administrators]** with the capability to read **[all audit information]** from the audit records.

FAU_SAR.1.2 (1) The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.4 FAU_SAR.3 (1) Selectable audit review (Wireless Access Point)

FAU_SAR.3.1 (1) The TSF shall provide the ability to apply **[selection]** of audit data based on **[start time, end time, MAC address, and record ID].**

6.1.1.5 FAU_SEL.1 (1) Selective audit (Wireless Access Point)

FAU_SEL.1.1 (1) The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) user identity, event type

b) device interface, wireless client identity

6.1.2 Cryptographic Support (FCS) Requirements

6.1.2.1 FCS_BCM_(EXT).1 Extended: Baseline Cryptographic Module (Wireless Access Point)

FCS_BCM_(EXT).1.1 All FIPS-approved cryptographic functions implemented by the TOE shall be implemented in a cryptomodule that is FIPS 140-2 validated, and perform the specified cryptographic functions in a FIPS-approved mode of operation. The FIPS 140-2 validation shall include an algorithm validation certificate for all FIPS-approved cryptographic functions implemented by the TOE.

FCS_BCM_(EXT).1.2 All cryptographic modules implemented in the TOE:

> ***[As a combination of hardware and software shall have a minimum overall rating of FIPS PUB 140-2, Level 1 and also meet FIPS PUB 140-2, Level 3 for the following: Roles, Services and Authentication; and Design Assurance. The logical interfaces used for the input and output of plaintext cryptographic key components, authentication data, and CSPs shall be logically separated from all other interfaces using a trusted path or AS02.16 must be satisfied; where "trusted path" is interpreted to include a communications channel established using a FIPS 140-2 Level 2 cryptographic module and the HTTPS protocol between the cryptomodule and the external IT entity.].***

6.1.2.2 FCS_CKM.1 (1) Cryptographic key generation (for symmetric keys in Wireless Access Point))

FCS_CKM.1.1 (1) The TSF shall generate symmetric cryptographic keys using a FIPS-Approved Random Number Generator as specified in FCS_COP_(EXT).1, and provide integrity protection to generated symmetric keys in accordance with NIST SP 800-57 “Recommendation for Key Management” Section 6.1.

6.1.2.3 FCS_CKM.1 (2) Cryptographic key generation (for asymmetric keys in Wireless Access Point)

FCS_CKM.1.1 (2) The TSF shall generate asymmetric cryptographic keys in accordance with the mathematical specifications of the FIPS-approved or NIST-recommended standard **[FIPS 186-3],** using a domain parameter generator and a **[FIPS-Approved Random Number Generator as specified in FCS_COP_(EXT).1]** in a cryptographic key generation scheme that meets the following:

- The TSF shall provide integrity protection and assurance of domain parameter and public key validity to generated asymmetric keys in accordance with NIST SP 800-57 “Recommendation for Key Management” Section 6.1.
- Generated key strength shall be equivalent to, or greater than, a symmetric key strength of 128 bits using conservative estimates.

6.1.2.4 FCS_CKM.2 (1) Cryptographic key distribution (Wireless Access Point)

FCS_CKM.2.1 (1) The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method ***[Manual (Physical) Method and Automated (Electronic) Method]*** that meets the following:

- NIST Special Publication 800-57, "Recommendation for Key Management" Section 8.1.5
- NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"

6.1.2.5 FCS_CKM_(EXT).2 Extended: Cryptographic Key Handling and Storage (Wireless Access Point)

FCS_CKM_(EXT).2.1 The TSF shall perform a key error detection check on each transfer of key (internal, intermediate transfers). The TOE performs an odd parity check on every transfer of key material, both internal and intermediate key transfers.

FCS_CKM_(EXT).2.2 The TSF shall store persistent secret and private keys when not in use in encrypted form or using split knowledge procedures.

FCS_CKM_(EXT)_2.3 The TSF shall destroy non-persistent cryptographic keys after a cryptographic administrator-defined period of time of inactivity.

Application Note: The cryptographic administrator must have the ability to set a threshold of inactivity after which non-persistent keys must be destroyed in accordance with FCS_CKM.4.

FCS_CKM_(EXT).2.4 The TSF shall prevent archiving of expired (private) signature keys.

6.1.2.6 FCS_CKM.4 (1) Cryptographic key destruction (Wireless Access Point)

FCS_CKM.4.1 (1) The TSF shall destroy cryptographic keys in accordance with a cryptographic key zeroization method that meets the following:

a) Key zeroization requirements of FIPS PUB 140-2, "Security Requirements for Cryptographic Modules"

b) Zeroization of all plaintext cryptographic keys and all other critical cryptographic security parameters shall be immediate and complete.

c) The TSF shall zeroize each intermediate storage area for plaintext key/critical cryptographic security parameter (i.e., any storage, such as memory buffers, that is included in the path of such data) upon the transfer of the key/critical cryptographic security parameter to another location.

d) For non-volatile memories other than EEPROM and Flash, the zeroization shall be executed by overwriting three or more times using a different alternating data pattern each time.

e) For volatile memory and non-volatile EEPROM and Flash memories, the zeroization shall be executed by a single direct overwrite consisting of a pseudo random pattern, followed by a read-verify.

6.1.2.7 FCS_COP.1 (1) Cryptographic Operation (Data encryption/decryption in Wireless Access Point)

FCS_COP.1.1 (1) The cryptomodule shall perform encryption and decryption using the FIPS-approved security function AES algorithm operating in **[AES_CCM and AES_ECB Mode]** and cryptographic key size of ***[128 bits, 192 bits, and 256 bits].***

6.1.2.8 FCS_COP.1 (2) Cryptographic Operation (Digital Signature in Wireless Access Point)

FCS_COP.1.1 (2) The TSF shall perform cryptographic signature services using the FIPS-approved security function ***[RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of* [2048 bits]*]*** that meets NIST Special Publication 800-57, "Recommendation for Key Management."

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

FCS_COP.1.1 (3) The TSF shall perform cryptographic hashing services using the FIPS-approved security function Secure Hash Algorithm and message digest size of ***[256 bits, 384 bits, and 512 bits].***

6.1.2.10 FCS_COP.1 (4) Cryptographic Operation (Key agreement in Wireless Access Point)

FCS_COP.1.1 (4) The TSF shall perform cryptographic key agreement services using the FIPS-approved security function as specified in NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" ***[*[Finite Field-based key agreement algorithm] *and cryptographic key sizes (modulus) of* [2048 bits]*]*** that meets NIST Special Publication 800-57, "Recommendation for Key Management."

6.1.2.11 FCS_COP.1 (5) Cryptographic Operation (HMAC)

FCS_COP.1.1 (5) The TSF shall perform **[hash-keyed message authentication]** in accordance with a specified cryptographic algorithm **[FIPS approved HMAC Algorithm]** and cryptographic key sizes **[160 bits]** that meet the following **[FIPS 198]*.***

6.1.2.12 FCS_COP_(EXT).1 Extended: Random Number Generation (Wireless Access Point)

FCS_COP_(EXT).1.1 The TSF shall perform all random number generation (RNG) services in accordance with a FIPS-approved RNG **[Digital Signature Standard]** seeded by ***[one or more independent software-based entropy sources.]***

> *Application Note: The full FIPS 140-2 Reference from Annex C is as follows: "National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 27, 2000 with Change Notice – Appendix 3.2."*

FCS_COP_(EXT).1.2 The TSF shall defend against tampering of the random number generation (RNG)/ pseudorandom number generation (PRNG) sources.

6.1.3 User Data Protection (FDP) Requirements

6.1.3.1 FDP_PUD_(EXT).1 Extended: Protection of User Data

FDP_PUD_(EXT).1.1 When the administrator has enabled encryption, the TSF shall:

- Encrypt authenticated user data transmitted to a wireless client from the radio interface of the wireless access system using the cryptographic algorithm(s) specified in FCS_COP_(EXT).2;
- Decrypt authenticated user data received from a wireless client by the radio interface of the wireless access system using the cryptographic algorithm(s) specified in FCS_COP_(EXT).2.

6.1.3.2 FDP_RIP.1 (1) Subset residual information protection (Wireless Access Point)

FDP_RIP.1.1 (1) The TSF shall ensure that any previous information content of a resource is made unavailable upon the ***[allocation of the resource to]*** the following objects: network packet objects

6.1.4 Identification and Authentication (FIA) Requirements

6.1.4.1 FIA_AFL.1 (1) Administrator authentication failure handling (Wireless Access Point)

FIA_AFL.1.1 (1) **Refinement:** The TSF shall detect when an administrator configurable positive integer within the range of **[3-10]** unsuccessful authentication attempts occur related to remote administrators logging on to the ***Wireless Access Point.***

FIA_AFL.1.2 (1) **Refinement:** When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall prevent **the administrator *from performing activities remotely that require authentication*** until an action is taken by a local Administrator.

6.1.4.2 FIA_ATD.1 (1) Administrator Attribute Definition (Wireless Access Point)

FIA_ATD.1.1 (1) The TSF shall maintain the following minimum list of security attributes belonging to individual administrators: password, **[username and role].**

6.1.4.3 FIA_ATD.1 (2) User Attribute Definition (Wireless Access Point)

FIA_ATD.1.1 (2) The TSF shall maintain the following minimum list of security attributes belonging to individual remotely authenticated users: ***[user ID, host MAC address, and authentication credentials].***

6.1.4.4 FIA_UAU.1 (1) Timing of local authentication

FIA_UAU.1.1 (1) The TSF shall allow **[the passing of authentication data to and from the remote authentication server]** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 (1) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.5 FIA_UAU_(EXT).5 Extended: Multiple authentication mechanisms (Wireless Access Point)

FIA_UAU_(EXT).5.1 (1) The TSF shall provide local authentication, and a remote authentication mechanism to perform user authentication.

FIA_UAU_(EXT).5.2 (1) The TSF shall, at the option of the administrator, invoke the remote authentication mechanism for administrators and wireless LAN users.

6.1.4.6 FIA_UID.2 (1) User identification before any action (Wireless Access Point)

FIA_UID.2.1 (1) The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.7 FIA_USB.1 (1) User-subject binding (Administrator in Wireless Access Point)

FIA_USB.1.1 (1) The TSF shall associate the following administrator user security attributes with subjects acting on the behalf of that user: **[username, password, role].**

FIA_USB.1.2 (1) The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users**: [upon successful authentication to the TOE].**

FIA_USB.1.3 (1) The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **[administrators may change their own passwords].**

6.1.4.8 FIA_USB.1 (2) User-subject binding (Wireless User in Wireless Access Point)

FIA_USB.1.1 (2) The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **[user ID, host MAC address].**

FIA_USB.1.2 (2) The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **[a wireless user will have a user ID and MAC address associated with their session after successful authentication with the TOE].**

FIA_USB.1.3 (2) The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **[the wireless user may make no changes to their own attributes].**

6.1.5 Security Management (FMT) Requirements

6.1.5.1 FMT_MOF.1 (1) Management of security functions behavior (Wireless Access Point)

FMT_MOF.1.1 (1) The TSF shall restrict the ability to **[determine the behaviour of a function as described in second column of Table 6-3]** the functions **[listed in the first column of Table 6-3]** to **[the authorised roles identified in the third column of Table 6-3].**

Table 6-3: Management of Security Functions (Wireless Access Point)

Function	Management Capability	Authorized Role
Audit	Pre-selection of the events which trigger an audit record,	Crypto Officer
	Start and stop of the audit function	Administrator and Crypto Officer
	Query audit	Crypto Officer
Cryptographic Services	Load a key	Crypto Officer
	Delete/zeroize a key	Crypto Officer
	Set a key lifetime	Crypto Officer
	Set the cryptographic algorithm	Crypto Officer
	Set the TOE to encrypt or not to encrypt wireless transmissions	Crypto Officer
	Execute self tests of TOE hardware and the cryptographic functions	Crypto Officer
	Query and set the encryption/decryption of network packets	Crypto Officer
User Data Protection	Query, set, modify, and delete the cryptographic keys and key data	Crypto Officer
Identification and Authentication (I&A)	Allow or disallow the use of an authentication server	Crypto Officer
	Set the number of authentication failures that must occur before the TOE takes action to disallow future logins	Crypto Officer
Time	Manage Time	Administrator and Crypto Officer
Self Test	Execute tests of TOE hardware, cryptographic functions, and cryptographic keys	Crypto Officer
	Enable/disable testing of TOE hardware, cryptographic functions, cryptographic keys	Crypto Officer
TOE Access	Set the length of time a session may remain inactive before it is terminated	Crypto Officer
	Set the TOE Access Banner	Administrator and Crypto Officer
	Enable or disable Filtering by MAC address	Administrator and Crypto Officer
	Configure filtering by MAC address	Administrator and Crypto Officer

6.1.5.2 FMT_MSA.2 (1) Secure security attributes (Wireless Access Point)

FMT_MSA.2.1 (1) The TSF shall ensure that only secure values are accepted for security attributes.

6.1.5.3 FMT_MTD.1 (1) Management of TSF Data (Wireless Access Point)

FMT_MTD.1.1 (1) The TSF shall restrict the ability to **[perform operations as listed in Table 6-4]** on the **[TSF data listed in Table 6-4]** to **[the authorised role specified in the last column of Table 6-4].**

Table 6-4: Management of TSF Data (Wireless Access Point)

Class	Operations	TSF Data	Authorized Role

Audit	Modify, query, clear, create the set of rules used to pre-select	Audit rules	Administrator
I&A	Query, modify, delete, clear, create	Authentication credentials	Administrator
I&A	Query, modify, delete, clear, create	User identification credentials	Administrator
I&A	Modify	Their own authentication credentials	Administrator, Crypto Officer, Wireless User

6.1.5.4 FMT_SMF.1 (1) Specification of Management Functions (Wireless Access Point)

FMT_SMF.1.1 (1) The TSF shall be capable of performing the following management functions: **[as listed in Table 6-3 and Table 6-4].**

6.1.5.5 FMT_SMR.1 (1) Security roles (Wireless Access Point)

FMT_SMR.1.1 (1) The TSF shall maintain the roles: **[**

- **Administrator,**
- **Crypto-Officer, and**
- **Wireless user.]**

Application Note: The Administrator and Crypto-Officer are both authorized administrators.

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

6.1.6 Protection of TSF (FPT) Requirements

6.1.6.1 FPT_STM_(EXT).1 Extended: Reliable time stamps

FPT_STM_(EXT).1.1 The TSF shall be able to provide reliable time stamps, synchronized via an external time source, for its own use.

6.1.6.2 FPT_TST_(EXT).1 Extended: TSF Testing

FPT_TST_(EXT).1.1 The TSF shall run a suite of self-tests during the initial start-up and also either periodically during normal operation, or at the request of an authorized administrator to demonstrate the correct operation of the TSF.

FPT_TST_(EXT).1.2 The TSF shall provide authorized administrators with the capability to verify the integrity of stored TSF executable code through the use of the TSF-provided cryptographic services.

6.1.6.3 FPT_TST.1 (1) TSF Testing (for cryptography on Wireless Access Point)

FPT_TST.1.1 (1) The TSF shall run a suite of self tests in accordance with FIPS PUB 140-2 and Appendix C of this profile during initial start-up (on power on), at the request of the cryptographic administrator (on demand), under various conditions defined in section 4.9.1 of FIPS 140-2, and periodically (at least once a day) to demonstrate the correct operation of the following cryptographic functions:

a) Key error detection;

b) Cryptographic algorithms;

c) RNG/PRNG

FPT_TST.1.2 (1) The TSF shall provide authorized cryptographic administrator with the capability to verify the integrity of TSF data related to the cryptography by using TSF-provided cryptographic functions.

FPT_TST.1.3 (1) The TSF shall provide authorized cryptographic administrator with the capability to verify the integrity of stored TSF executable code related to the cryptography by using TSF-provided cryptographic functions.

6.1.6.4 FPT_TST.1 (2) TSF Testing (for key generation components on Wireless Access Point))

FPT_TST.1.1 (2) The TSF shall perform self tests immediately after generation of a key to demonstrate the correct operation of each key generation component. If any of these tests fails, that generated key shall not be used, the cryptographic module shall react as required by FIPS PUB 140-2 for failing a self-test, and this event will be audited.

FPT_TST.1.2 (2) The TSF shall provide authorized cryptographic administrators with the capability to verify the integrity of TSF data related to the key generation by using TSF-provided cryptographic functions.

FPT_TST.1.3 (2) The TSF shall provide authorized cryptographic administrators with the capability to verify the integrity of stored TSF executable code related to the key generation by using TSF-provided cryptographic functions.

6.1.7 TOE Access (FTA) Requirements

6.1.7.1 FTA_SSL.3 (1) TSF-initiated termination (Wireless Access Point)

FTA_SSL.3.1 (1) The TSF shall terminate a local interactive or wireless session after an administrator configurable time interval of user inactivity.

6.1.7.2 FTA_TAB.1 (1) Default TOE access banners (Wireless Access Point)

FTA_TAB.1.1 (1) Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

6.1.7.3 FTA_TSE.1 TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on **[MAC Address].**

6.1.8 Trusted Path/Channels (FTP) Requirements

6.1.8.1 FTP_ITC_(EXT).1 (1) Extended: Inter-TSF trusted channel

FTP_ITC_(EXT).1.1 (1) The TOE shall provide an encrypted communication channel between itself and entities in the TOE IT Environment that is logically distinct from other communication

channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC_(EXT).1.2 (1)The TSF shall permit the TSF, or the IT Environment entities to initiate communication via the trusted channel.

FTP_ITC_(EXT).1.3 (1) The TSF shall initiate communication via the trusted channel for all authentication functions, remote logging, time, ***[none].***

6.1.8.2 FTP_TRP.1 (1) Trusted path (Wireless Access Point)

FTP_TRP.1.1 (1) The TSF shall provide a communication path between itself and wireless users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification, replay or disclosure.

FTP_TRP.1.2 (1) The TSF shall permit wireless client devices to initiate communication via the trusted path.

FTP_TRP.1.3 (1) The TSF shall require the use of the trusted path for wireless user authentication and **[administrator authentication]**.

6.2 Security Server Security Functional Requirements

In this section, explicitly stated Security Functional Requirements (i.e., those not found in Part 2 of the CC) are identified "_(SS)" in the component name.

Table 6-5: Security Functional Requirements for the Security Server

Functional Class	Functional Components	Extended?	Refined?	#
Security Audit (FAU)	FAU_GEN.1 (SS) – Audit data generation (Security Server)	No	Yes	1
	FAU_GEN.2 (SS) – User identity association (Security Server)	No	Yes	2
	FAU_SAR.1 (SS) Audit review (Security Server)	No	Yes	3
	FAU_SAR.3 (SS) Selectable audit review (Security Server)	No	Yes	4
	FAU_SEL.1 (SS) – Selective Audit (Security Server)	No	Yes	5
Cryptographic Support (FCS)	FCS_BCM_(SS).1 – Extended: Security Server baseline cryptographic module	Yes	No	6
	FCS_CKM.1 (SS1) - Cryptographic key generation (for symmetric keys on Security Server)	No	Yes	7
	FCS_CKM.1 (SS2) - Cryptographic key generation (for asymmetric keys on Security Server)	No	Yes	8
	FCS_CKM.2 (SS) - Cryptographic key distribution (Security Server)	No	Yes	9
	FCS_CKM_(SS).2 - Cryptographic key handling and storage on Security Server)	Yes	No	10
	FCS_CKM.4 (SS) - Cryptographic key destruction (Security Server)	No	Yes	11
	FCS_COP.1 (SS1) – Cryptographic Operation (Data encryption/decryption on Security Server)	No	Yes	12
	FCS_COP.1 (SS2) – Cryptographic Operation (Digital Signature on Security Server)	No	Yes	13

Functional Class	Functional Components	Extended?	Refined?	#
	FCS_COP.1 (SS3) – Cryptographic Operation (Secure Hash on Security Server)	No	Yes	14
	FCS_COP.1 (SS4) - Cryptographic Operation (Key Agreement on Security Server)	No	Yes	15
	FCS_COP.1 (SS5) – Cryptographic Operation (HMAC on Security Server)	No	Yes	16
	FCS_COP_(SS).1 – Extended: Security Server random number generation	Yes	No	17
User Data Protection (FDP)	FDP_CPD_(SS).1 Extended: Certificate path development	Yes	No	18
	FDP_DAU_CPL_(SS).1 Extended: Certificate path initialisation – basic	Yes	No	19
	FDP_DAU_CPV_(SS).1 Extended: Intermediate certificate processing - Basic	Yes	No	20
	FDP_DAU_CPV_(SS).2 Extended: Certificate processing - basic	Yes	No	21
	FDP_DAU_CPV_(SS).1 Extended: Certificate path output - basic	Yes	No	22
	FDP_DAU_CRL_(SS).1 Extended: Basic CRL Checking	Yes	No	23
	FDP_DAU_OCS_(SS).1 Extended: Basic OCSP Client	Yes	No	24
	FDP_ITC_SIG_(SS).1 Extended: Import of PKI Signature	Yes	No	25
	FDP_RIP.1 (SS) – Subset Residual Information Protection (Security Server)	No	Yes	26
Identification and Authentication (FIA)	FIA_AFL.1 (SS) – Authentication failure handling (Security Server Administrator)	No	Yes	27
	FIA_ATD.1 (SS1) – Administrator attribute definition (Security Server)	No	Yes	28
	FIA_ATD.1 (SS2) – User attribute definition (Security Server)	No	Yes	29
	FIA_UAU.2 – User authentication before any action	No	Yes	30
	FIA_UAU.5 – Multiple authentication mechanisms	No	Yes	31
	FIA_UID.2 (SS) – User identification before any action (Security Server)	No	Yes	32
	FIA_USB.1 (SS) –User-subject binding (Security Server Administrator)	No	Yes	33
Security Management (FMT)	FMT_MOF.1 (SS) - Management of security functions behavior (Security Server)	No	Yes	34
	FMT_MSA.2 (SS) - Secure security attributes (Security Server)	No	Yes	35
	FMT_MTD.1 (SS) - Management of TSF Data (Security Server)	No	Yes	36
	FMT_SMF.1 (SS) - Specification of Management Functions (Security Server)	No	Yes	37
	FMT_SMR.1 (SS) - Security roles (Security Server)	No	Yes	38
Protection of TSF (FPT)	FPT_TST_(SS).1 - Extended Security Server testing	Yes	No	39
	FPT_TST.1 (SS) - TSF testing (Security Server Cryptography	No	Yes	40

Functional Class	Functional Components	Extended?	Refined?	#
	FPT_TST.2 (SS) - TSF testing (Security Server Key Generation Components)	No	Yes	41
TOE Access	FTA_SSL.3 (SS) TSF-initiated termination (Security Server)	No	Yes	42
	FTA_TAB.1 (SS) Default TOE access banners (Security Server)	No	Yes	43
Trusted Path/Channels (FTP)	FTP_ITC_(SS).1 – Extended Security Server trusted channel	Yes	No	44
	FTP_TRC.1 (SS) – Trusted Path (Security Server)	No	Yes	45

6.2.1 Security Audit (FAU) Requirements

6.2.1.1 FAU_GEN.1 (SS) Audit data generation (Security Server)

FAU_GEN.1.1 (SS) **Refinement:** The ***Security Server*** shall be able to generate an audit record of the following auditable events:

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

b) All auditable events for the minimum level of audit; and

c) **[All auditable events as shown in Table 6-6 below.]**

Table 6-6: Security Server Auditable Events

#	Requirement	Auditable Events	Additional Audit Record Contents
1	FAU_GEN.1 (SS)	None	None
2	FAU_GEN.2 (SS)	None	None
3	FAU_SAR.1 (SS)	None	None
4	FAU_SAR.3 (SS)	None	None
5	FAU_SEL.1 (SS)	All modifications to the audit configuration that occur while the audit collection is operating	None
6	FCS_BCM_(SS).1	None	None
7	FCS_CKM.1 (SS1)	Success and Failure of the cryptographic activity	The identity of the Administrator/Crypto-Officer performing the function
8	FCS_CKM.1 (SS2)	Success and Failure of the cryptographic activity	The identity of the Administrator/Crypto-Officer performing the function
9	FCS_CKM.2 (SS)	Success and failure of the cryptographic activity	The identity of the Administrator/Crypto-Officer performing the function

#	Requirement	Auditable Events	Additional Audit Record Contents
10	FCS_CKM_(SS).2	Error(s) detected during key transfer	If available – the authentication credentials of subjects with which the invalid key is shared
11	FCS_CKM.4 (SS)	Success and failure of the cryptographic activity	If available - the identity of the Administrator/Crypto-Officer performing the function
12	FCS_COP.1(SS1)	None	None
13	FCS_COP.1(SS2)	None	None
14	FCS_COP.1(SS3)	None	None
15	FCS_COP.1(SS4)	None	None
16	FCS_COP.1 (SS5)	None	None
17	FCS_COP_(SS).1	None	None
18	FDP_CPD_(SS).1	Success or failure to build path	For success, matching rules bypassed
19	FDP_DAU_CPI_(SS).1	None	None
20	FDP_DAU_CPV_(SS).1	Success or failure of certificate processing Bypass of revocation status checking	For failure, reason(s) for failure
21	FDP_DAU_CPV_(SS).2	Success or failure of certificate processing	For failure, reason(s) for failure
22	FDP_DAU_CPO_(SS).1	None	None
23	FDP_DAU_CRL_(SS).1	Rejection of CRL Override time checks	Reason for rejection
24	FDP_DAU_OCS_(SS).1	Rejection of OCSP response Override time checks	Reason for rejection
25	FDP_ITC_SIG_(SS).1	None	None
26	FDP_RIP.1 (SS)	None	None
27	FIA_AFL.1 (SS)	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g., disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal)	None
28	FIA_ATD.1 (SS1)	None	None
29	FIA_ATD.1 (SS2)	None	None
30	FIA_UAU.2	Use of the authentication mechanism (success or failure)	User identity. The TOE SHALL NOT record invalid passwords in the audit log
31	FIA_UAU_(SS).5	Final decision on authentication	None
32	FIA_UID.2 (SS)	None	None
33	FIA_USB.1 (SS)	Unsuccessful binding of user security attributes to a subject	None

#	Requirement	Auditable Events	Additional Audit Record Contents
34	FMT_MOF.1 (SS)	Changing the TOE encryption algorithm including the selection not to encrypt communications Start or Stop of audit record generation Changes to the TOE remote authentication settings; Changes to the threshold of failed authentication attempts; Changes to the session lock timeframe	Encryption algorithm selected The identity of the Administrator/Crypto-Officer performing the function
35	FMT_MSA.2 (SS)	All offered and rejected values for security attributes	None
36	FMT_MTD.1 (SS)	Changes to the set of rules used to pre-select audit events. Changes to the TOE authentication credentials	None – the TOE SHALL NOT record authentication credentials in the audit log.
37	FMT_SMF.1 (SS)	None	None
38	FMT_SMR.1 (SS)	Modifications to the group of users that are part of a role	This event is logged in the System Log only.
39	FPT_TST_SS).1	Execution of the self test	Success or Failure of test
40	FPT_TST.1 (SS1)	Execution of the self test	Success or Failure of test
41	FPT_TST.1 (SS2)	Execution of the self test	Success or Failure of test
42	FTA_SSL.3 (SS)	TSF Initiated Termination User inactivity causing Termination is logged in the APs	Termination of an interactive session by the session locking mechanism.
43	FTA_TAB.1 (SS)	None	None
44	FTP_ITC_(SS).1	Initiation/Closure of a trusted channel	Identification of the remote entity with which the channel was attempted/created; Success or failure of the event
45	FTP_TRP.1 (SS)	Initiation of a trusted channel	Identification of the remote entity with which the channel was attempted/created; Success or failure of the event

FAU_GEN.1.2 (SS) **Refinement:** The ***Security Server*** shall record within each audit record at least the following information:

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

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

6.2.1.2 FAU_GEN.2 (SS) User identity association (Security Server)

FAU_GEN.2.1 (SS) **Refinement:** For audit events resulting from actions of identified users, the ***Security Server*** shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.1.3 FAU_SAR.1 (SS) Audit review

FAU_SAR.1.1 (SS) **Refinement:** The ***Security Server*** shall provide **[the Security Officer**] with the capability to read **[all audit records]** from the audit records.

FAU_SAR.1.2 (SS) **Refinement:** The ***Security Server*** shall provide the audit records in a manner suitable for the user to interpret the information.

6.2.1.4 FAU_SAR.3 (SS) Selectable audit review (Security Server)

FAU_SAR.3.1 (SS) **Refinement:** The ***Security Server*** shall provide the ability to apply **[*selection*]** of audit data based on **[start time and end time.]**

6.2.1.5 FAU_SEL.1 (SS) Selective audit (Security Server)

FAU_SEL.1.1 (SS) **Refinement:** The ***Security Server*** shall be able to include or exclude auditable events from the set of audited events based on the following attributes: ***event type***.

6.2.2 Cryptographic Support (FCS) Requirements

6.2.2.1 FCS_BCM_(SS).1.1 Extended: Security Server Baseline Cryptographic Module

FCS_BCM_(SS).1.1 All FIPS-approved cryptographic functions implemented by the Security Server shall be implemented in a cryptomodule that is FIPS 140-2 validated, and perform the specified cryptographic functions in a FIPS-approved mode of operation. The FIPS 140-2 validation shall include an algorithm validation certificate for all FIPS-approved cryptographic functions implemented by the TOE.

FCS_BCM_(SS).1.2 All cryptographic modules implemented in the Security Server:

[

Entirely in software shall have a minimum overall rating of FIPS PUB 140-2, Level 1; also meet FIPS PUB 140-2, Level 3 for selections Roles, Services and Authentication; and Design Assurance. The logical interfaces used for the input and output of plaintext cryptographic key components, authentication data, and CSPs shall be logically separated from all other interfaces using a trusted path or AS02.16 must be satisfied; where "trusted path" is interpreted to include a communications channel established using a FIPS 140-2 Level 2 cryptographic module and the HTTPS protocol between the cryptomodule and the external IT entity.

].

6.2.2.2 FCS_CKM.1 (SS1) Cryptographic key generation (for symmetric key on Security Server)

FCS_CKM.1.1 (SS1) **Refinement:** The ***Security Server*** shall generate symmetric cryptographic keys using a FIPS-Approved Random Number Generator as specified in FCS_COP_(EXT).1, and provide integrity protection to generated symmetric keys in accordance with NIST SP 800-57 "Recommendation for Key Management" Section 6.1.

6.2.2.3 FCS_CKM.1 (SS2) Cryptographic key generation (for asymmetric keys on Security Server)

FCS_CKM.1.1 (SS2**) Refinement:** The ***Security Server*** shall generate asymmetric cryptographic keys in accordance with the mathematical specifications of the FIPS-approved or NIST-recommended standard **[FIPS 186-3],** using a domain parameter generator and a ***[FIPS-Approved Random Number Generator as specified in FCS_COP_(EXT).1]*** in a cryptographic key generation scheme that meets the following:

- The TSF shall provide integrity protection and assurance of domain parameter and public key validity to generated asymmetric keys in accordance with NIST SP 800-57 "Recommendation for Key Management" Section 6.1.
- Generated key strength shall be equivalent to, or greater than, a symmetric key strength of 128 bits using conservative estimates.

6.2.2.4 FCS_CKM.2 (SS) Cryptographic key distribution (Security Server)

FCS_CKM.2.1 (SS) **Refinement:** The ***Security Server*** shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method ***[Manual (Physical) Method and Automated (Electronic) Method]*** that meets the following:

- NIST Special Publication 800-57, "Recommendation for Key Management" Section 8.1.5
- NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"

6.2.2.5 FCS_CKM_(SS).2 Extended: Cryptographic Key Handling and Storage on Security Server

FCS_CKM_(SS).2.1 The Security Server shall perform a key error detection check on each transfer of key (internal, intermediate transfers). The TOE performs an odd parity check on every transfer of key material, both internal and intermediate key transfers.

FCS_CKM_(SS).2.2 The Security Server shall store persistent secret and private keys when not in use in encrypted form or using split knowledge procedures.

FCS_CKM_(SS).2.3 The Security Server shall destroy non-persistent cryptographic keys after a cryptographic administrator-defined period of time of inactivity.

Application Note: The cryptographic administrator must have the ability to set a threshold of inactivity after which non-persistent keys must be destroyed in accordance with FCS_CKM.4.

FCS_CKM_(SS).2.4 The Security Server shall prevent archiving of expired (private) signature keys.

6.2.2.6 FCS_CKM.4 (SS) Cryptographic key destruction (Security Server)

FCS_CKM.4.1 (SS) **Refinement:** The ***Security Server*** shall destroy cryptographic keys in accordance with a cryptographic key zeroization method that meets the following:

a) Key zeroization requirements of FIPS PUB 140-2, "Security Requirements for Cryptographic Modules"

b) Zeroization of all plaintext cryptographic keys and all other critical cryptographic security parameters shall be immediate and complete.

c) The TSF shall zeroize each intermediate storage area for plaintext key/critical cryptographic security parameter (i.e., any storage, such as memory buffers, that is included in the path of such data) upon the transfer of the key/critical cryptographic security parameter to another location.

d) For non-volatile memories other than EEPROM and Flash, the zeroization shall be executed by overwriting three or more times using a different alternating data pattern each time.

e) For volatile memory and non-volatile EEPROM and Flash memories, the zeroization shall be executed by a single direct overwrite consisting of a pseudo random pattern, followed by a read-verify.

6.2.2.7 FCS_COP.1 (SS1) Cryptographic Operation (Data encryption/decryption on Security Server)

FCS_COP.1.1 (SS1) **Refinement**: The ***Security Server*** cryptomodule shall perform encryption and decryption using the FIPS-approved security function AES algorithm operating in **[AES_CBC and AES_ECB Mode]** and cryptographic key size of ***[128 bits, 192 bits, and 256 bits].***

6.2.2.8 FCS_COP.1 (SS2) Cryptographic Operation (Digital Signature on Security Server)

FCS_COP.1.1 (SS2) **Refinement**: The ***Security Server*** shall perform cryptographic signature services using the FIPS-approved ***security functions and key size (modulus) as listed in Table 6-7 below*** that meets NIST Special Publication 800-57, "Recommendation for Key Management."

Table 6-7: Digital Signature Algorithms and Key Size (Modulus)

Digital Signature Algorithm	Key Size (Modulus)
RSA (rDSA)	2048 bits or higher
DSA	1024 bits or higher
ECDSA	160 bits or higher

6.2.2.9 FCS_COP.1 (SS3) Cryptographic Operation (Secure Hash on Security Server)

FCS_COP.1.1 (SS3) **Refinement:** The ***Security Server*** shall perform cryptographic hashing services using the FIPS-approved security function Secure Hash Algorithm and message digest size of ***[160 bits, 256 bits, 384 bits, and 512 bits].***

6.2.2.10 FCS_COP.1 (SS4) Cryptographic Operation (Key Agreement on Security Server))

FCS_COP.1.1 (SS4) **Refinement:** The ***Security Server*** shall perform cryptographic key agreement services using the FIPS-approved security function as specified in NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" ***[Finite Field-based key agreement algorithm and cryptographic key sizes (modulus) of 2048 bits]*** that meets NIST Special Publication 800-57, "Recommendation for Key Management."

6.2.2.11 FCS_COP.1 (SS5) Cryptographic Operation (HMAC on Security Server)

FCS_COP.1.1 (SS5) **Refinement:** The ***Security Server*** shall perform **[*hash-keyed message authentication]* i**n accordance with a specified cryptographic algorithm **[FIPS approved HMAC Algorithm]** and cryptographic key sizes **[160 bits]** that meet the following: **[FIPS 198]*.***

6.2.2.12 FCS_COP_(SS).1 Extended: Security Server Random Number Generation on Security Server

FCS_COP_(SS).1.1 The Security Server shall perform all random number generation (RNG) services in accordance with a FIPS-approved RNG **[Digital Signature Standard]** seeded by ***[one or more independent software-based entropy sources.]***

Application Note: The full FIPS 140-2 Reference from Annex C is as follows: "National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 27, 2000 with Change Notice – Appendix 3.2."

FCS_COP_(SS).1.2 The Security Server shall defend against tampering of the random number generation (RNG)/ pseudorandom number generation (PRNG) sources.

6.2.3 User Data Protection (FDP) Requirements

6.2.3.1 FDP_CPD_(SS).1 Certification path development

FDP_CPD_(SS).1.1 The Security Server shall develop a certification path from a trust anchor provided by ***[*** **[the Security Officer]** ***]*** to the subscriber using matching rules for the following subscriber certificate fields or extensions: ***[distinguished name, subject alternative names, subject key identifier, subject public key algorithm, certificate policies].***

FDP_CPD_(SS).1.2 The Security Server shall develop the certification path using the following additional matching rule: ***[none].***

FDP_CPD_(SS).1.3 The Security Server shall develop the certification path using the following additional matching rule ***[none].***

FDP_CPD_(SS).1.4 The Security Server shall bypass any matching rules except **[distinguished name]** if additional certification paths are required.

6.2.3.2 FDP_DAU_CPI_(SS).1 Certification path initialisation -- basic

FDP_DAU_CPI_(SS).1.1 The Security Server shall use the trust anchor provided by ***[*** **[the Security Officer]** ***]***.

FDP_DAU_CPI_(SS).1.2 The Security Server shall obtain the time of interest called "TOI' from a reliable source ***[local environment].***

FDP_DAU_CPI_(SS).1.3 The Security Server shall perform the following checks on the trust anchor ***[time validation and self signed signature].***

FDP_DAU_CPI_(SS).1.4 The Security Server shall derive from the trust anchor ***[subject DN, subject public key, subject public key algorithm object identifier, and subject public key parameters].***

6.2.3.3 FDP_DAU_CPV_(SS).1 Extended: Certificate processing - basic

FDP_DAU_CPV_(SS).1.1 The Security Server shall reject a certificate if any of the following checks fails:

a) Use parent-public-key, parent-public-key-algorithm-identifier, and parent-public-key-parameters to verify the signature on the certificate;

b) notBefore field in the certificate < = TOI;

c) notAfter field in the certificate > = TOI;

d) issuer field in the certificate = parent-DN; or

e) Security Server is able to process all extensions marked critical

FDP_DAU_CPV_(SS).1.3 The Security Server shall bypass the revocation check if the revocation information is not available.

FDP_DAU_CPV_(SS).1.4 The Security Server shall reject a certificate if the revocation status using ***[CRL, OCSP]*** demonstrates that the certificate is revoked.

FDP_DAU_CPV_(SS).1.5 The Security Server shall update the public key parameters state machine using the following rules:

a) Obtain the parameters from the subjectPublickeyInfo field of certificate if the parameters are present in the field; else

b) Retain the old parameters state if the subject public key algorithm of current certificate and parent public key algorithm of current certificate belong to the same family of algorithms, else

c) Set parameters = "null".

6.2.3.4 FDP_DAU_CPV_(SS).2 Intermediate certificate processing -- basic

FDP_DAU_CPV_(SS).2.1 The Security Server shall reject an intermediate certificate if any of the following additional checks fails:

a) basicConstraints field is present with cA = TRUE;

b) pathLenConstraint is not violated; or

c) if a critical keyUsage extension is present, keyCertSign bit is set

6.2.3.5 FDP_DAU_CPO_(SS).1) Certification path output -- basic

FDP_DAU_CPO_(SS).1.1 The Security Server shall output certification path validation failure if any certificate in the certification path is rejected.

FDP_DAU_CPO_(SS).1.2 The Security Server shall output the following variables from the end certificate: subject DN, subject public key algorithm identifier, subject public key, critical keyUsage extension.

FDP_DAU_CPO_(SS).1.3 The Security Server shall output the following additional variables from the end certificate ***[certificate, subject alternative names, extendedKeyUsage].***

FDP_DAU_CPO_(SS).1.4 The Security Server shall output the subject public key parameters from the certification path parameter state machine.

6.2.3.6 FDP_DAU_CRL_(SS).1 Extended: Basic CRL Checking

FDP_DAU_CRL_(SS).1.1 The Security Server shall obtain the CRL from ***[the local cache, repository].***

FDP_DAU_CRL_(SS).1.2 The Security Server shall obtain the trusted public key, algorithm, and public key parameters of the CRL issuer.

FDP_DAU_CRL_(SS).1.3 The Security Server shall invoke the cryptographic module to verify signature on the CRL using trusted public key, algorithm, and public key parameters of the CRL issuer.

FDP_DAU_CRL_(SS).1.4 The Security Server shall verify that if a critical keyUsage extension is present in CRL issuer certificate, cRLSign bit in the extension is set in the certificate.

FDP_DAU_CRL_(SS).1.5 The Security Server shall match the issuer field in the CRL with what it assumes to be the CRL issuer.

FDP_DAU_CRL_(SS).1.6 The Security Server shall reject the CRL if all of the following are true:

a) Time check are not overridden;

b) ***[TOI > thisUpdate + x where x=0]; and***

c) ***[TOI > nextUpdate + x if nextUpdate is present and where x=0].***

FDP_DAU_CRL_(SS).1.7 The Security Server shall permit ***[none]*** to override time checks.

FDP_DAU_CRL_(SS).1.8 The Security Server shall reject CRL if the CRL contains “critical” extension(s) that Security Server does not process.

FDP_DAU_CRL_(SS).1.9 The Security Server shall perform the following additional checks ***[none].***

6.2.3.7 FDP_DAU_OCS_(SS).1 Extended: Basic OCSP Client

FDP_DAU_OCS_(SS).1.1 The Security Server shall formulate the OCSP requests in accordance with PKIX RFC 2560.

FDP_DAU_OCS_(SS).1.2 The Security Server shall obtain the public key, algorithm, and public key parameters of the OCSP Responder from ***[the OCSP responder certificate].***
FDP_DAU_OCS_(SS).1.3 The Security Server shall invoke the cryptographic module to verify signature on the OCSP response using trusted public key, algorithm, and public key parameters of the OCSP responder.

FDP_DAU_OCS_(SS).1.4 The Security Server shall verify that if the OCSP responder certificate contains extendedKeyUsage extension, the extension contains the PKIX OID for ocsp-signing or the anyExtendedKeyUsage OID.

FDP_DAU_OCS_(SS).1.5 The Security Server shall match the responderID in the OCSP response with the corresponding information in the responder certificate

FDP_DAU_OCS_(SS).1.6 The Security Server shall match the certID in a request with certID in singleResponse.

FDP_DAU_OCS_(SS).1.7 The Security Server shall reject the OCSP response for an entry if all of the following are true:

a) time checks are not overridden;

b) ***[TOI > producedAt + x where x=0 =0;***

c) ***[TOI > thisUpdate for entry + x where =0]; and***

d) ***[TOI > nextUpdate for entry + x if nextUpdate is present and where x=0].].***

FDP_DAU_OCS_(SS).1.8 The Security Server shall reject OCSP response if the response contains “critical” extension(s) that Security Server does not process.

FDP_DAU_OCS_(SS).1.9 The Security Server shall perform the following additional checks ***[request nonce = response nonce].***

FDP_DAU_OCS_(SS).1.10 The Security Server shall permit ***[none]*** to override time checks.

FDP_DAU_OCS_(SS).1.11 The Security Server shall reject OCSP response if the response contains “critical” extension(s) that Security Server does not process.

6.2.3.8 FDP_ITC_SIG_(SS).1 Extended: Import of PKI Signature

FDP_ITC_SIG_(SS).1.1 The Security Server shall use the following information from the signed data **[*hashing algorithm, signature algorithm]*** during signature verification.

6.2.3.9 FDP_RIP.1 (SS) Subset Residual Information Protection (Security Server)

FDP_RIP.1.1 (SS) **Refinement:** The **Security Server** shall ensure that any previous information content of a resource is made unavailable upon the ***[allocation of the resource to]*** the following objects: network pack objects.

6.2.4 Identification and Authentication (FIA) Requirements

6.2.4.1 FIA_AFL.1 (SS) Administrator authentication failure handling (Security Server Administrator)

FIA_AFL.1.1 (SS) **Refinement:** The ***Security Server*** shall detect when ***3 consecutive*** unsuccessful authentication attempts occur related to remote administrators logging on to the Security Server.

FIA_AFL.1.2 (SS) **Refinement:** When the defined number of unsuccessful authentication attempts has been met or surpassed, the ***Security Server*** shall prevent the administrator from performing activities remotely that require authentication until an action is taken by a local Administrator.

6.2.4.2 FIA_ATD.1 (SS1) Administrator Attribute Definition (Security Server)

FIA_ATD.1.1 (SS1) **Refinement:** The ***Security Server*** shall maintain the following minimum list of security attributes belonging to individual administrators: password, ***[username, and role].***

6.2.4.3 FIA_ATD.1 (SS2) User Attribute Definition (Security Server)

FIA_ATD.1.1 (SS2) **Refinement**: The ***Security Server*** shall maintain the following minimum list of security attributes belonging to individual remotely authenticated users: ***[user ID, authentication credentials].***

6.2.4.4 FIA_UAU.2 Authentication before any action

FIA_UAU.2.1 **Refinement**: The ***Security Server*** shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.4.5 FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 **Refinement**: The ***Security Server*** shall provide:

a) [Administrator usernames and passwords

b) RADIUS Server authentication for remote users]

to support user authentication.

FIA_UAU.5.2 **Refinement**: The ***Security Server*** shall authenticate any user's claimed identify according to the **[following rules:**

a) Security officers shall login using a username and password.

b) Remote users shall be authenticated using a RADIUS Server that supports 802.1X authentication using Public Key X.509 certificates.]

6.2.4.6 FIA_UID.2 (SS) User identification before any action (Security Server)

FIA_UID.2.1 (SS**) Refinement**: The ***Security Server*** shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.4.7 FIA_USB.1 (SS) User-subject binding (Security Server Administrator)

FIA_USB.1.1 (SS) **Refinement**: The ***Security Server*** shall associate the following administrator user security attributes with subjects acting on the behalf of that user: ***[username, password, role].***

FIA_USB.1.2 (SS) **Refinement**: The ***Security Server*** shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: ***[upon successful authentication to the TOE].***

FIA_USB.1.3 (SS) **Refinement**: The ***Security Server*** shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: ***[administrators may change their own passwords].***

6.2.5 Security Management (FMT) Requirements

6.2.5.1 FMT_MOF.1 (SS) Management of security functions behavior (Security Server)

FMT_MOF.1.1 (SS) **Refinement**: The ***Security Server*** shall restrict the ability to ***[determine the behaviour of***] the functions **[listed in the first column of Table 6-8]** to **[the authorised roles identified in the third column of Table 6-8].**

Table 6-8: Management of Security Functions (Security Server)

Function	Management Capability	Authorized Role
Audit	Pre-selection of the events which trigger an audit record,	Security Officer
	Start and stop of the audit function	Security Officer
	Query audit	Security Officer
Cryptographic Services	Load a key	Security Officer
	Delete/zeroize a key	Security Officer
	Set a key lifetime	Security Officer
	Set the cryptographic algorithm	Security Officer
	Execute self tests of TOE and the cryptographic functions	Security Officer
	Change EAP-TLS cipher suite	Security Officer
Identification and Authentication (I&A)	Allow or disallow the use of an authentication server	Security Officer
Self Test	Execute tests of TOE cryptographic functions, and check integrity of cryptographic keys	Security Officer
	Enable/disable testing of TOE hardware, cryptographic functions, cryptographic keys	Security Officer
TOE Access	Set TOE Access Banner	Security Officer

6.2.5.2 FMT_MSA.2 (SS) Secure security attributes (Security Server)

FMT_MSA.2.1 (SS) **Refinement:** The ***Security Server*** shall ensure that only secure values are accepted for security attributes.

6.2.5.3 FMT_MTD.1 (SS) Management of TSF Data (Security Server)

FMT_MTD.1.1 (SS) **Refinement:** The ***Security Server*** shall restrict the ability to **[perform operations as listed in Table 6-9]** on the **[TSF data listed in Table 6-9]** to **[the authorised role specified in the last column of Table 6-9].**

Table 6-9: Management of TSF Data (Security Server)

Class	Operations	TSF Data	Authorized Role
FAU	Modify, query, clear, create the set of rules used to pre-select	Audit rules	Security Officer
FDP	Install and delete	Server Certificate, private key, and private key password	Security Officer
	Install, view, and delete	CA Certificates	Security Officer
	Add, view, and delete	Certificate Revocation Lists	Security Officer
	Configure	OCSP Responder	Security Officer

Class	Operations	TSF Data	Authorized Role
FIA	Add, modify, and delete AAA client information	Name, IP address, RADIUS shared secret, Authentication Key, Key Encryption Key	Security Officer
	Change	Their own authentication credentials	Security Officer

6.2.5.4 FMT_SMF.1 (1) Specification of Management Functions (Security Server)

FMT_SMF.1.1 (SS) **Refinement:** The ***Security Server*** shall be capable of performing the following management functions: **[as listed in Table 6-8 and Table 6-9].**

6.2.5.5 FMT_SMR.1 (SS) Security roles (Security Server)

FMT_SMR.1.1 (SS) **Refinement**: The ***Security Server*** shall maintain the roles:

a) Security Officer

b) Remote user

Application Note: The Security Officer is an authorized administrator.

FMT_SMR.1.2 (SS) **Refinement:** The ***Security Server*** shall be able to associate users with roles.

6.2.6 Protection of TSF (FPT) Requirements

6.2.6.1 FPT_TST_(SS).1 Extended: Security Server TSF Testing

FPT_TST_(SS).1.1The Security Server shall run a suite of self-tests during the initial start-up and also either periodically during normal operation, or at the request of an authorized administrator to demonstrate the correct operation of the TSF.

FPT_TST_(SS).1.2 The Security Server shall provide authorized administrators with the capability to verify the integrity of stored TSF executable code through the use of the TSF-provided cryptographic services.

6.2.6.2 FPT_TST.1 (SS1) TSF Testing (for Security Server cryptography)

FPT_TST.1.1 (SS1) **Refinement:** The ***Security Server*** shall run a suite of self tests in accordance with FIPS PUB 140-2 and Appendix C of this profile during initial start-up (on power on), at the request of the cryptographic administrator (on demand), under various conditions defined in section 4.9.1 of FIPS 140-2, and periodically (at least once a day) to demonstrate the correct operation of the following cryptographic functions:

a) Key error detection;

b) Cryptographic algorithms;

c) RNG/PRNG

FPT_TST.1.2 (SS1) **Refinement:** The ***Security Server*** shall provide authorized cryptographic administrator with the capability to verify the integrity of TSF data related to the cryptography by using TSF-provided cryptographic functions.

FPT_TST.1.3 (SS1) **Refinement:** The ***Security Server*** shall provide authorized cryptographic administrator with the capability to verify the integrity of stored TSF executable code related to the cryptography by using TSF-provided cryptographic functions.

6.2.6.3 FPT_TST.1 (SS2) TSF Testing (for key generation components on Security Server)

FPT_TST.1.1 (SS2) **Refinement**: The ***Security Server*** shall perform self tests immediately after generation of a key to demonstrate the correct operation of each key generation component. If any of these tests fails, that generated key shall not be used, the cryptographic module shall react as required by FIPS PUB 140-2 for failing a self-test, and this event will be audited.

FPT_TST.1.2 (SS2) **Refinement:** The ***Security Server*** shall provide authorized cryptographic administrators with the capability to verify the integrity of TSF data related to the key generation by using TSF-provided cryptographic functions.

FPT_TST.1.3 (SS2) **Refinement:** The ***Security Server*** shall provide authorized cryptographic administrators with the capability to verify the integrity of stored TSF executable code related to the key generation by using TSF-provided cryptographic functions.

6.2.7 TOE Access (FTA) Requirements

6.2.7.1 FTA_SSL.3 (SS) TSF-initiated termination (Security Server)

FTA_SSL.3.1 (SS) **Refinement:** The ***Security Server*** shall terminate a local interactive or remote user authentication session after ***constant*** time interval of user inactivity.

6.2.7.2 FTA_TAB.1 (SS) Default TOE access banners (Security Server)

FTA_TAB.1.1 (SS) **Refinement:** Before establishing a user session, the ***Security Server*** shall display an advisory warning message regarding unauthorized use of the TOE.

6.2.8 Trusted Path/Channels (FTP) Requirements

6.2.8.1 FTP_ITC_(SS).1 Extended: Security Server trusted channels

FTP_ITC_(SS).1.1 The Security Server shall provide an encrypted communication channel between itself, the Wireless Access Point, the Security Server management station and entities in the TOE IT operational Environment that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC_(SS).1.2 The Security Server shall permit the TSF, or the IT Environment entities to initiate communication via the trusted channel.

FTP_ITC_(SS).1.3 The Security Server shall initiate communication via the trusted channel for communication with the OCSP responder.

6.2.8.2 FTP_TRP.1 (SS) Trusted path (Security Server)

FTP_TRP.1.1 (SS) **Refinement:** The ***Security Server*** shall provide a communication path between itself and wireless users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification, replay or disclosure.

FTP_TRP.1.2 (SS) **Refinement:** The ***Security Server*** shall permit wireless client devices to initiate communication via the trusted path.

FTP_TRP.1.3 (SS) **Refinement:** The ***Security Server*** shall require the use of the trusted path for wireless user authentication and **[Security Officer authentication]**.

6.3 TOE Security Assurance Requirements

The security assurance requirements are evaluation assurance level 4 (EAL4) augmented with ALC_FLR.2. Table 6-10 lists the assurance components.

Table 6-10: TOE Security Assurance Requirements

Assurance Class	Assurance Components
Development (ADV)	ADV_ARC.1 Architectural Design with domain separation and non-bypassability
	ADV_IMP.1 Implementation representation of the TSF
	ADV_FSP.4 Complete functional specification
	ADV_TDS.3 Basic modular design
Guidance Documents (AGD)	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative user guidance
Life cycle support (ALC)	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.2 Flaw reporting procedures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
Tests (ATE)	ATE_COV.2 Analysis of coverage
	ATE_FUN.1 Functional testing
	ATE_DPT.2 Testing: security enforcing modules
	ATE_IND.2 Independent testing – conformance
Vulnerability assessment (AVA)	AVA_VAN.3 Focused vulnerability analysis

6.4 Requirements Rationale

6.4.1 Rationale for Security Functional Requirements

Table 6-11 below shows that all security objectives for the TOE are addressed by security requirements. The table also provides the rationale that the security requirements are suitable to address the security objectives.

Table 6-11: TOE Security Functional Requirement to TOE Security Objectives Rationale

#	Security Objective (TOE)	Requirements Addressing the Objective	Security Functional Requirement Rationale
1	O.ADMIN _GUIDANCE	AGD_OPE.1 AGD_PRE.1 ALC_DEL.1	ALC_DEL.1 ensures that the administrator has the ability to begin their TOE installation with a clean (e.g., malicious code has not been inserted once it has left the developer's control) version of the TOE, which is necessary for secure management of the TOE The AGD_PRE.1 requirement ensures the administrator has the information necessary to install the TOE in the evaluated configuration. Often times a vendor's product contains software that is not part of the TOE and has not been evaluated. The Installation, Generation and Startup (IGS) documentation ensures that once the administrator has followed the installation and configuration guidance the result is a TOE in a secure configuration. The AGD_OPE.1 requirement mandates the developer provide the administrator with guidance on how to operate the TOE in a secure manner. This includes describing the interfaces the administrator uses in managing the TOE and any security parameters that are configurable by the administrator. The documentation also provides a description of how to set up and use the auditing features of the TOE. The AGD_OPE.1 requirement is also intended for non-administrative users. If the TOE provides facilities/interfaces for this type of user, this guidance will describe how to use those interfaces securely. This could include guidance on the setup of wireless clients for use with the TOE. If it is the case that the wireless clients may be configured by administrators that are not administrators of this TOE, then that guidance may be user guidance from the perspective of this TOE. AGD_OPE.1 AND AGD_PRE.1 analysis during evaluation will ensure that the guidance documentation can be followed unambiguously to ensure the TOE is not misconfigured in an insecure state due to confusing guidance.
2	O.AUDIT _GENERATION	FAU_GEN.1(1) FAU_GEN.2 (1) FAU_SAR.1 (1) FAU_SAR.3 (1) FAU_SEL.1 (1) FPT_STM_(EXT).1 FTP_ITC_(EXT).1	FAU_GEN.1(1) and FAU_GEN.1 (SS) define the set of events that the TOE must be capable of recording. This requirement ensures that the administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. There is a minimum of

#	Security Objective (TOE)	Requirements Addressing the Objective	Security Functional Requirement Rationale
		Additional SFRs when TOE includes Security Server: FAU_GEN.1(SS) FAU_GEN.2 (SS) FAU_SAR.1 (SS) FAU_SAR.3 (SS) FAU_SEL (SS) FPT_ITC_(SS).1	information that must be present in every audit record and this requirement defines that, as well as the additional information that must be recorded for each auditable event. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements an ST author adds to this PP. FAU_GEN.2 and FAU_GEN.2 (SS) ensure that the audit records associate a user identity with the auditable event. In the case of authorized users, the association is accomplished with the user ID. In all other cases, the association is based on the source network identifier, which is presumed to be the correct identity, but cannot be confirmed since these subjects are not authenticated. FAU_SAR.1 (1), FAU_SAR.3 (1), FAU_SAR.1 (SS), and FAU_SAR.3 (SS) specify that the TOE must be capable of reviewing audit records. FAU_SEL.1 (1) and FAU_SEL (SS) allow for the selection of events to be audited. This requires that the criteria used for the selection of auditable events to be defined. For example, the user identity can be used as selection criterion for the events to be audited. FPT_STM_(EXT).1 supports the audit functionality by ensuring that the TOE is capable of obtaining a time stamp for use in recording audit events. FTP_ITC_(EXT).1 and FPT_ITC_(SS).1 provide a trusted channel for services provided by the TOE Operational Environment (the audit server and the time server).
3	O.CONFIGURATION_IDENTIFICATION	ALC_CMC.4 ALC_CMS.4 ALC_FLR.2	ALC_CMC.4 contributes to this objective by requiring the developer have a configuration management plan that describes how changes to the TOE and its evaluation deliverables are managed. ALC_CMS.4 is necessary to define the items that must be under the control of the CM system. This requirement ensures that the TOE implementation representation, design documentation, test documentation (including the executable test suite), user and administrator guidance, and CM documentation are tracked by the CM system. ALC_FLR.2 plays a role in satisfying this objective by requiring the developer to have procedures that address flaws that have been discovered in the product, either through

#	Security Objective (TOE)	Requirements Addressing the Objective	Security Functional Requirement Rationale
			developer actions (e.g., developer testing) or discovery by others. The flaw remediation process used by the developer corrects any discovered flaws and performs an analysis to ensure new flaws are not created while fixing the discovered flaws.
4	O.CORRECT_TSF_OPERATION	FPT_TST_(EXT).1 FPT_TST.1(1) FPT_TST.1(2) Additional SFRs when TOE includes Security Server: FPT_TST_(SS).1 FPT_TST.1 (SS1) FPT_TST.1(SS2)	FPT_TST_(EXT).1 and FPT_TST_(SS).1 are necessary to ensure the correctness of the TSF software and TSF data. If TSF software is corrupted it is possible that the TSF would no longer be able to enforce the security policies. This also holds true for TSF data, if TSF data is corrupt the TOE may not correctly enforce its security policies. The FPT_TST.1 (1) and FPT_TST.1 (SS1) for crypto and FPT_TST.1 (2) and FPT_TST.1 (SS2) for key generation functional requirement have been included to address the critical nature and specific handling of the cryptographic related TSF data. Since the cryptographic TSF data has specific FIPS PUB requirements associated with them it is important to ensure that any fielded testing on the integrity of these data maintains the same level of scrutiny as specified in the FCS functional requirements.
5	O.CRYPTOGRAPHY	FCS_BCM_(EXT).1 FCS_CKM.1 (1) FCS_CKM.1 (2) FCS_CKM.2 (1) FCS_CKM.4 (1) FCS_CKM_(EXT).2 FCS_COP.1 (1) FCS_COP.1 (2) FCS_COP.1 (3) FCS_COP.1 (4) FCS_COP.1 (5) FCS_COP_(EXT).1 FTP_ITC_EXT.1 FTP_TRP.1 (1) Additional SFRs when TOE includes Security Server: FCS_BCM_(SS).1) FCS_CKM.1 (SS1) FCS_CKM.1 (SS2) FCS_CKM.2 (SS) FCS_CKM.4 (SS); FCS_CKM_(SS).2) FCS_COP,1 (SS1)	Baseline cryptographic services are provided in the TOE by FIPS PUB 140-2 compliant modules implemented in a hardware/software combination in Wireless Access Point (FCS_BCM_(EXT).1) and in software by the Security Server (FCS_BCM_(SS).1) These TOE services are based primarily upon functional security requirements in the areas of key management and cryptographic operations. In the area of key management there are functional requirements that address the generation of symmetric keys (FCS_CKM.1 (1) and FCS_CKM.1 (SS1), and the generation of asymmetric keys (FCS_CKM.1 (2) and FCS_CKM.1 (SS2); methods of manual and automated cryptographic key distribution (FCS_CKM.2 (1) and FCS_CKM.2 (SS)); cryptographic key destruction (FCS_CKM.4(1) and FCS_CKM.4(SS); and techniques cryptographic key handling and storage (FCS_CKM_(EXT).2 and FCS_CKM_(SS).2) . Specific functional requirements in the area of cryptographic operations address data encryption and decryption (FCS_COP.1 (1) and FCS_COP,1(SS1)); cryptographic signatures (FCS_COP.1 (2) and FCS_COP.1 (SS2);

#	Security Objective (TOE)	Requirements Addressing the Objective	Security Functional Requirement Rationale
		FCS_COP.1 (SS2) FCS_COP.1 (SS3) FCS_COP.1 (SS4) FCS_COP.1 (SS5) FCS_COP_(SS).1 FTP_ITC_(SS).1 FTP_TRP.1 (SS)	cryptographic hashing (FCS_COP.1 (3) and FCS_COP.1 (SS3)); cryptographic key agreement (FCS_COP.1 (4) and FCS_COP.1 (SS4); hash-keyed message authentication (FCS_COP.1 (5) and FCS_COP.1 (SS5); and improved random number generation (FCS_COP_(EXT).1 and FCS_COP_(SS).1) Cryptographic services are used to provide trusted channels for the TOE. (FTP_ITC_EXT.1 and FTP_TRP.1 (1)) Cryptographic services (TLS) are used to provide trusted path for the TOE administrator connecting to the TOE (FTP_ITC_SS).1 and FTP_TRP.1 (SS))
6	O.CRYPTOGRAPHY_ VALIDATED	FCS_BCM_(EXT).1 FCS_CKM.1 (1) FCS_CKM.1 (2) FCS_CKM.2 (1) FCS_CKM.4 (1) FCS_CKM_(EXT).2 FCS_COP.1 (1) FCS_COP.1 (2) FCS_COP.1 (3) FCS_COP.1 (4) FCS_COP.1 (5) FCS_COP_(EXT).1 Additional SFRs when TOE includes Security Server: FCS_BCM_(SS).1) FCS_CKM.1 (SS1) FCS_CKM.1 (SS2) FCS_CKM.2 (SS) FCS_CKM.4 (SS); FCS_CKM_(SS).2) FCS_COP,1 (SS1) FCS_COP.1 (SS2) FCS_COP.1 (SS3) FCS_COP.1 (SS4) FCS_COP.1 (SS5) FCS_COP_(SS).1	Baseline cryptographic services are provided in the TOE by FIPS PUB 140-2 compliant modules implemented in a hardware/software combination in Wireless Access Point (FCS_BCM_(EXT).1) and in software by the Security Server (FCS_BCM_(SS).1) These TOE services are based primarily upon functional security requirements in the areas of key management and cryptographic operations. In the area of key management there are functional requirements that address the generation of symmetric keys (FCS_CKM.1 (1) and FCS_CKM.1 (SS1), and the generation of asymmetric keys (FCS_CKM.1 (2) and FCS_CKM.1 (SS2); methods of manual and automated cryptographic key distribution (FCS_CKM.2 (1) and FCS_CKM.2 (SS)); cryptographic key destruction (FCS_CKM.4(1) and FCS_CKM.4(SS); and techniques cryptographic key handling and storage (FCS_CKM_(EXT).2 and FCS_CKM_(SS).2) . Specific functional requirements in the area of cryptographic operations address data encryption and decryption (FCS_COP.1 (1) and FCS_COP,1(SS1)); cryptographic signatures (FCS_COP.1 (2) and FCS_COP.1 (SS2); cryptographic hashing (FCS_COP.1 (3) and FCS_COP.1 (SS3)); cryptographic key agreement (FCS_COP.1 (4) and FCS_COP.1 (SS4); hash-keyed message authentication (FCS_COP.1 (5) and FCS_COP.1 (SS5); and improved random number generation (FCS_COP_(EXT).1 and FCS_COP_(SS).1)
7	O.DISPLAY_BANNER	FTA_TAB.1 (1) Additional SFR when TOE includes Security Server: FTA_TAB.1 (SS)	FTA_TAB.1 and FTA_TAB.1 (SS) meet this objective by requiring that the TOE display an administrator defined banner before a user can establish an authenticated session. This banner is under complete control of the administrator,

#	Security Objective (TOE)	Requirements Addressing the Objective	Security Functional Requirement Rationale
			who can specify any warnings regarding unauthorized use of the TOE and remove any product or version information if they desire. The only time that it is envisioned that an authenticated session would need to be established is for the performance of TOE administration. Bannering is not necessary prior to use of services that pass network traffic through the TOE.
8	O.DOCUMENTED _DESIGN	ADV_FSP.4 ADV_TDS.3	ADV_FSP.4 and ADV_TDS.3 support this objective by requiring that the TOE be developed using sound engineering principles. The use of a high level design and the functional specification ensure that developers responsible for TOE development understand the overall design of the TOE. This in turn decreases the likelihood of design flaws and increases the chance that accidental design errors will be discovered. ADV_TDS.3 and ADV_FSP.4 are also used to ensure that the TOE design is consistent across the Design and the Functional Specification.
9	O.MANAGE	FMT_MOF.1 (1) FMT_MSA.2 (1) FMT_MTD.1 (1) FMT_SMF.1 (1) FMT_SMR.1 (1) Additional SFRs when TOE includes Security Server: FMT_MOF.1 (SS) FMT_MSA.2 (SS) FMT_MTD.1 (SS) FMT_SMF.1 (SS) FMT_SMR.1 (SS)	FMT_MOF.1 (1), FMT_MSA.2 (1), FMT_MTD.1 (1), FMT_SMF.1 (1), FMT_MOF.1 (SS), FMT_MSA.2 (SS), FMT_MTD.1 (SS), FMT_SMF.1 (SS) are used to satisfy this management objective, as well as other objectives that specify the control of functionality. The requirements' rationale for this objective focuses on the administrator's capability to perform management functions in order to control the behavior of security functions. FMT_SMR.1 (1) and FMT_SMR.1 (SS) define the specific security roles to be supported. .
10	O.MEDIATE	FIA_UAU.1 FIA_UAU_(EXT).5, FIA_UID.2 (1) FIA_USB.1 (1) FDP_PUD_(EXT).1 Additional SFRs when TOE includes Security Server: FIA_UAU.2 FIA_UAU_(SS).5 FIA_UID.2 (SS) FIA_USB.1 (SS)	FIA_UAU.1, FIA_UAU.2, FIA_UAU_(EXT).5, FIA_UAU_(SS).5, FIA_UID.2(1) and FIA_UID.2(SS) ensure that the TOE has the ability to mediate packet flow based upon the authentication credentials of the wireless user. FIA_USB.1(1), FIA_USB,1 (2) and FIA_USB.1 (SS) bind the attributes of a user such as a user ID or PKI certificate with subjects executing on behalf of the user allowing access control decisions to be made on behalf of the user. FDP_PUD_(EXT).1 allows the administrator to control whether or not unencrypted data will be allowed to pass through the TOE.
11	O.PARTIAL _FUNCTIONAL _TESTING	ATE_FUN.1 ATE_COV.2 ATE_IND.2	ATE_FUN.1 requires the developer to provide the necessary test documentation to allow for an independent analysis of the developer's

#	Security Objective (TOE)	Requirements Addressing the Objective	Security Functional Requirement Rationale
			security functional test coverage. In addition, the developer must provide the test suite executables and source code, which the evaluator uses to independently verify the vendor test results and to support of the test coverage analysis activities. ATE_COV.2 requires the developer to provide a test coverage analysis that demonstrates the extent to which the TSFI are tested by the developer's test suite. This component also requires an independent confirmation of the extent of the test suite, which aids in ensuring that correct security relevant functionality of a TSFI is demonstrated through the testing effort. ATE_IND.2 requires an independent confirmation of the developer's test results by mandating that a subset of the test suite be run by an independent party. This component also requires an independent party to craft additional functional tests that address functional behavior that is not demonstrated in the developer's test suite. Upon successful completion of these requirements, the TOE's conformance to the specified security functional requirements will have been demonstrated.
12	O.RESIDUAL _INFORMATION	FDP_RIP.1 (1) FCS_CKM_(EXT).2 FCS_CKM.4 (1) Additional SFRs when TOE includes Security Server: FDP_RIP.1 (SS) FCS_CKM_(SS).2 FCS_CKM.4 (SS)	FDP_RIP.1 (1) and FDP_RIP.1 (SS) are used to ensure the contents of resources are not available once the resource is reallocated. For this TOE it is critical that the memory used to build network packets is either cleared or that some buffer management scheme be employed to prevent the contents of a packet being disclosed in a subsequent packet (e.g., if padding is used in the construction of a packet, it must not contain another user's data or TSF data). FCS_CKM_(EXT).2 and FCS_CKM_(SS).2 place requirements on how cryptographic keys are managed within the TOE. This requirement places restrictions in addition to FDP_RIP.1, in that when a cryptographic key is moved from one location to another (e.g., calculated in some scratch memory and moved to a permanent location) that the memory area is immediately cleared as opposed to waiting until the memory is reallocated to another subject. FCS_CKM.4 (1) and FCS_CKM.4 (SS) apply to the destruction of cryptographic keys used by the TSF. This requirement specifies how and when cryptographic keys must be destroyed. The proper destruction of these keys is critical in ensuring the content of these keys cannot

#	Security Objective (TOE)	Requirements Addressing the Objective	Security Functional Requirement Rationale
			possibly be disclosed when a resource is reallocated to a user.
13	O.SELF _PROTECTION	ADV_ARC.1	ADV_ARC.1 provides the security architecture description of the security domains maintained by the TSF that are consistent with the SFRs. Since self-protection is a property of the TSF that is achieved through the design of the TOE and TSF, and enforced by the correct implementation of that design, self-protection will be achieved by that design and implementation
14	O.TIME_STAMPS	FPT_STM_(EXT).1	FPT_STM_(EXT).1 (1) requires that the TOE be able to obtain reliable time stamps for its own use and therefore, partially satisfies this objective. Time stamps include date and time and are reliable in that they are always available to the TOE, and the clock must be monotonically increasing.
15	O.TOE_ACCESS	FIA_AFL.1 (1) FIA_ATD.1 (1) FIA_ATD.1 (2) FIA_UAU.2 FIA_UAU_(EXT).5 FIA_UID.2 (1) FTA_SSL.3 (1) FTA_TSE.1 FTP_ITC_(EXT).1 FTP_TRP.1 (1) Additional SFRs when TOE includes Security Server: FDP_CPD_(SS).1 FDP_DAU_CPL_(SS).1 FDP_DAU_CPV_(SS).1 FDP_DAU_CPV_(SS).2 FDP_DAU_CPO_(SS).1 FDP_DAU_CRL_(SS). FDP_DAU_OCS_(SS).1 FDP_ITC_SIG,1 FIA_AFL.1 (SS) FIA_ATD.1 (SS1) FIA_ATD.1 (SS2) FIA_UAU.2 FIA_UAU_(SS).5 FIA_UID.2 (SS) FTA_SSL.3 (SS) FTP_ITC_(SS).1 FTP_TRP.1 (SS)	FIA_UID.2 plays a role in satisfying this objective by ensuring that every user is identified before the TOE performs any mediated functions. In most cases, the identification cannot be authenticated (e.g., a user attempting to send a data packet through the TOE that does not require authentication. It is impractical to require authentication of all users that attempt to send data through the TOE, therefore, the requirements specified in the TOE require authentication where it is deemed necessary. This does impose some risk that a data packet was sent from an identity other than that specified in the data packet. FIA_UAU.1 and FIA_UAU_(EXT).5 contribute to this objective by ensuring that administrators and users are authenticated before they are provided access to the TOE or its services. In order to control logical access to the TOE an authentication mechanism is required. The local administrator authentication mechanism is necessary to ensure an administrator has the ability to login to the TOE regardless of network connectivity (e.g., it would be unacceptable if an administrator could not login to the TOE because the authentication server was down, or that the network path to the authentication server was unavailable). FIA_AFL.1 (1) and FIA_AFL (SS) ensure that the TOE can protect itself and its users from brute force attacks on their authentication credentials. FIA_ATD.1 (1), (2), (SS1), and (SS2) provide the ability to manage user security attributes.

#	Security Objective (TOE)	Requirements Addressing the Objective	Security Functional Requirement Rationale
			FTA_SSL.3 (1) and FTA_SSL.3 (SS) ensures that inactive user and administrative sessions are dropped. FTA_TSE.1 provides the capability to limit access based on MAC address. FTP_ITC_(EXT).1 and FTP_ITC_(SS). 1provides a trusted channel for services provided by the TOE Operational Environment (the remote authentication server) FTP_TRP.1 (1) and FTP_TRP.1 (SS) ensures that remote users have a trusted path in order to authenticate. The following SFRs specify requirements for certificate path processing: FDP_CPD_(SS).1, FDP_DAU_CPL_(SS).1, FDP_DAU_CPV_(SS).1, FDP_DAU_CPV_(SS).2, FDP_DAU_CPO_(SS).1, FDP_DAU_CRL_(SS), and FDP_DAU_OCS_(SS).1 FDP_ITC_SIG_(SS).1 specifies requirements for digital signature verification.
16	O.VULNERABILITY _ANALYSIS	AVA_VAN.3	The AVA_VAN.3 component provides the necessary level of confidence that vulnerabilities do not exist in the TOE that could cause the security policies to be violated. AVA_VAN.3 requires the evaluator may also identify areas of concern. These are specific portions of the TOE evidence that the evaluator has some reservation about, although the evidence meets the requirements for the activity with which the evidence is associated. For example, a particular interface specification looks particularly complex, and therefore may be prone to error either in the development of the TOE or in the operation of the TOE. There is no potential vulnerability apparent at this stage, further investigation is required. This is beyond the bounds of encountered, as further investigation is required. The focused approach to the identification of potential vulnerabilities is an analysis of the evidence with the aim of identifying any potential vulnerabilities evident through the contained information. It is an unstructured analysis, as the approach is not predetermined. For this TOE, the vulnerability analysis is specified for an attack potential of basic.
17	OSS.CERTIFICAT	Only applicable when	These SFRs specify requirements for certificate

#	Security Objective (TOE)	Requirements Addressing the Objective	Security Functional Requirement Rationale
	E _PATH _VALIDATION	Security Server is included in the TOE. FDP_CPD_(SS).1 FDP_DAU_CPI_(SS).1 FDP_DAU_CPV_(SS).1 FDP_DAU_CPV_(SS).2 FDP_DAU_CPO_(SS).1 FDP_DAU_CRL_(SS). FDP_DAU_OCS_(SS).1	path processing: FDP_CPD_(SS).1, FDP_DAU_CPI_(SS).1, FDP_DAU_CPV_(SS).1, FDP_DAU_CPV_(SS).2, FDP_DAU_CPO_(SS).1, FDP_DAU_CRL_(SS), and. FDP_DAU_OCS_(SS).1.
18	OSS.AUTHENTIC ATION _SERVER	Only applicable when Security Server is included in the TOE. FIA_ATD.1 (SS2) FIA_UAU.2 FIA_UAU_(SS).5 FIA_UID.2 (SS)	FIA_ATD.1 (SS2), FIA_UAU.2 (SS), FIA_UAU_(SS).5, and FIA_UID.2 (SS) specify requirements for authentication of remote users by a RADIUS authentication server.
19	OSS.SIGNATURE _VERIFICATION	Only applicable when Security Server is included in the TOE. FDP_ITC_SIG_(SS).1	FDP_ITC_SIG_(SS).1 specifies requirements for digital signature verification.

Table 6-12 below shows that all Security Functional Requirements for the TOE can be traced to objectives for the TOE for both TOE configurations, Access Point and Security Server, and Access Point only.

The first section of the matrix (Wireless Access Point SFRs) applies when the Security Server is not included in the configuration. It shows that all Wireless Access Point SFRs are mapped to TOE objectives without including the Security Server objectives and all objectives for the TOE are addressed by SFRs for the TOE.

Both the first and second sections of the matrix (Wireless Access Point SFRs and Security Server SFRs, respectively) apply to the TOE when the configuration includes the Security Server. It shows that all the TOE SFRs, including the Security Server SFRs, are mapped to all of TOE objectives, including the Security Server objectives. It also shows that all objectives for the TOE are addressed by SFRs for the TOE.

For completeness, the third section of the matrix (Applicable EAL4 SARs) includes the mapping from objectives to the Basic Robustness security assurance requirements from the Wireless LAN SS PP to show that all objectives are met. However, the TOE is claiming conformance to EAL4 augmented by ALC_FLR.2 and AVA_VAN.3.

Table 6-12: Wireless Access Point SFR to Objectives Matrix

	OBJECTIVES FOR THE TOE	O. ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.CRYPTOGRAPHY_VALIDATED	O.CONFIGURATION_ IDENTIFICATION	O.CORRECT_ TSF_OPERATION	O.CR Y PTOGRAPHY	O.DISPLAY_BANNER	O.DOCUMENTED_DESIGN	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_ TESTING	O.RESIDUAL_ INFORMATION	O.SELF_PROTECTION	O.TIME_STAMPS	O.TOE_ACCESS	O.VULNERABILITY_ANALYSIS	OSS.CERTIFICATE_PATH_PROCESSING	OSS.AUTHENTICATION_SERVER	OSS.SIGNATURE_VERIFCATION
Wireless Access Point SFRs																				
1	FAU_GEN.1 (1)		X																	
2	FAU_GEN.2 (1)		X																	
3	FAU_SAR.1 (1)		X																	
4	FAU_SAR.3 (1)		X																	
5	FAU_SEL.1 (1)		X																	
6	FCS_BCM_(EXT).1			X			X													
7	FCS_CKM.1 (1)			X			X													
8	FCS_CKM.1 (2)			X			X													
9	FCS_CKM.2 (1)			X			X													
10	FCS_CKM_(EXT).2			X			X						X							
11	FCS_CKM.4 (1)			X			X						X							
12	FCS_COP.1 (1)			X			X													
13	FCS_COP.1 (2)			X			X													
14	FCS_COP.1 (3)			X			X													
15	FCS_COP.1 (4)			X			X													
16	FCS_COP.1 (5)			X			X													
17	FCS_COP_(EXT).1			X			X													
18	FDP_PUD_(EXT).1										X									
19	FDP_RIP.1 (1)												X							
20	FIA_AFL.1 (1)															X				
21	FIA_ATD.1 (1)															X				
22	FIA_ATD.1 (2)															X				
23	FIA_UAU.1										X					X				
24	FIA_UAU_(EXT).5										X					X				
25	FIA_UID.2 (1)										X					X				
26	FIA_USB.1 (1)										X									
27	FIA_USB.1 (2)										X									
28	FMT_MOF.1 (1)									X										
29	FMT_MSA.2 (1)									X										
30	FMT_MTD.1 (1)									X										
31	FMT_SMF.1 (1)									X										
32	FMT_SMR.1 (1)									X										
33	FPT_STM_(EXT).1		X												X					

	OBJECTIVES FOR THE TOE	O. ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.CRYPTOGRAPHY_VALIDATED	O.CONFIGURATION_ IDENTIFICATION	O.CORRECT_ TSF_OPERATION	O.CR Y PTOGRAPHY	O.DISPLAY_BANNER	O.DOCUMENTED_DESIGN	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_ TESTING	O.RESIDUAL_ INFORMATION	O.SELF_PROTECTION	O.TIME_STAMPS	O.TOE_ACCESS	O.VULNERABILITY_ANALYSIS	OSS.CERTIFICATE_PATH_PROCESSING	OSS.AUTHENTICATION_SERVER	OSS.SIGNATURE_VERIFCATION
34	FPT_TST_(EXT).1					X														
35	FPT_TST.1 (1)					X														
36	FPT_TST.1 (2)					X														
37	FTA_SSL.3 (1)															X				
38	FTA_TAB.1 (1)							X												
39	FTA_TSE.1															X				
40	FTP_ITC_(EXT).1			X												X				
41	FTP_TRP.1 (1)			X												X				
Security Server SFRs																				
1	FAU_GEN.1 (SS)		X																	
2	FAU_GEN.2 (SS)		X																	
3	FAU_SAR.1 (SS)		X																	
4	FAU_SAR.3 (SS)		X																	
5	FAU_SEL.1 (SS)		X																	
6	FCS_BCM_(SS).1			X			X													
7	FCS_CKM.1 (SS1)			X			X													
8	FCS_CKM.1 (SS2)			X			X													
9	FCS_CKM.2 (SS)			X			X													
10	FCS_CKM_(SS).2			X			X						X							
11	FCS_CKM.4 (SS)			X			X						X							
12	FCS_COP.1 (SS1)			X			X													
13	FCS_COP.1 (SS2)			X			X													
14	FCS_COP.1 (SS3)			X			X													
15	FCS_COP.1 (SS4)			X			X													
16	FCS_COP.1 (SS5)			X			X													
17	FCS_COP_(SS).1			X			X													
18	FDP_CPD_(SS).1																	X		
19	FDP_DAU_CPL_(SS).1																	X		
20	FDP_DAU_CPV_(SS).1																	X		
21	FDP_DAU_CPV_(SS).2																	X		
22	FDP_DAU_CPO_(SS).1																	X		
23	FDP_DAU_CRL_(SS).																	X		
24	FDP_DAU_OCS_(SS).1																	X		
25	FDP_ITC_SIG_(SS).1																			X
26	FDP_RIP.1 (SS)																			
27	FIA_AFL.1 ((SS)																			

	OBJECTIVES FOR THE TOE	O. ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.CRYPTOGRAPHY_VALIDATED	O.CONFIGURATION_ IDENTIFICATION	O.CORRECT_ TSF_OPERATION	O.CR Y PTOGRAPHY	O.DISPLAY_BANNER	O.DOCUMENTED_DESIGN	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_ TESTING	O.RESIDUAL_ INFORMATION	O.SELF_PROTECTION	O.TIME_STAMPS	O.TOE_ACCESS	O.VULNERABILITY_ANALYSIS	OSS.CERTIFICATE_PATH_PROCESSING	OSS.AUTHENTICATION_SERVER	OSS.SIGNATURE_VERIFCATION
28	FIA_ATD.1 (SS1)																			
29	FIA_ATD.1 (SS2)																		X	
30	FIA_UAU.2										X								X	
31	FIA_UAU_(SS).5										X								X	
32	FIA_UID.2 (SS)										X								X	
33	FIA_USB.1 (SS)										X									
34	FMT_MOF.1 (SS)									X										
35	FMT_MSA.2 (SS)									X										
36	FMT_MTD.1 (SS)									X										
37	FMT_SMF.1 (SS)									X										
38	FMT_SMR.1 (SS)									X										
39	FPT_TST_(SS).1					X														
40	FPT_TST.1 (SS1)					X														
41	FPT_TST.1 (SS2)					X														
42	FTA_SSL.3 (SS)															X				
43	FTA_TAB.1 (SS)							X												
44	FTP_ITC_(SS).1			X												X				
45	FTP_TRP.1 (SS)			X												X				
Applicable EAL4 SARs																				
1	ADV_ARC.1													X						
2	ADV_FSP.4								X											
3	ADV_TDS.3								X											
4	AGD_OPE.1	X																		
5	AGD_PRE.1	X																		
6	ALC_CMC.4				X															
7	ALC_CMS.4				X															
8	ALC_DEL.1	X																		
9	ALC_FLR.2				X															
10	ATE_COV.2											X								
11	ATE_FUN.1											X								
12	ATE_IND.2											X								
13	AVA_VAN.3																X			

6.4.2 Requirements Dependencies Rationale

Table 6-13 and Table 6-14 below show that all TOE SFR dependencies have been addressed.

Table 6-13: Wireless Access Point SFR Dependencies

#	Functional Requirements	Dependencies from CC or PP	Met By SFR	Row Ref
1	FAU_GEN.1 (1) - Audit data generation	FPT_STM.1	FPT_STM.1 (1)	33
2	FAU_GEN.2 (1) - User identity association	FAU_GEN.1	FAU_GEN.1 (1)	1
		FIA_UID.1	FIA_UID.2 (1)	
3	FAU_SAR.1 (1) – Audit review	FAU_GEN.1	FAU_GEN.1 (1)	1
4	FAU_SAR.3 (1) – Selectable audit review	FAU_SAR.1	FAU_SAR. (1)	3
5	FAU_SEL.1 (1) - Selective audit	FAU_GEN.1	FAU_GEN.1 (1)	1
		FMT_MTD.1	FMT_MTD.1 (1)	30
6	FCS_BCM_(EXT).1 – Extended: Baseline Cryptographic Module	None	N/A	-
7	FCS_CKM.1 (1) - Cryptographic key generation (for symmetric keys)	FCS_COP.1 (1)	FCS_COP.1 (1)	12
		FCS_CKM.4	FCS_CKM.4 (1)	11
		FMT_MSA.2	FMT_MSA.2 (1)	29
8	FCS_CKM.1 (2) - Cryptographic key generation (for asymmetric keys)	FCS_COP.1 (2)	FCS_COP.1(1)	12
		FCS_CKM.4	FCS_CKM.4 (1)	11
		FMT_MSA.2	FMT_MSA.2 (1)	29
9	FCS_CKM.2 (1) - Cryptographic key distribution	FCS_CKM.1 (1)	FCS_CKM.1 (1)	7
		FCS_CKM.1 (2)	FCS_CKM.1 (2)	8
		FMT_MSA.2	FMT_MSA.2 (1)	29
10	FCS_CKM_(EXT).2 - Cryptographic key handling and storage	FCS_CKM.1 (1)	FCS_CKM.1 (1)	7
		FCS_CKM.1 (2)	FCS_CKM.1 (2)	8
		FMT_MSA.2	FMT_MSA.2 (1)	29
11	FCS_CKM.4 (1) - Cryptographic key destruction	FCS_CKM.1 (1)	FCS_CKM.1 (1)	7
		FCS_CKM.1 (2)	FCS_CKM.1 (2)	8
		FMT_MSA.2	FMT_MSA.2 (1)	29
12	FCS_COP.1 (1) – Cryptographic Operation (Data encryption/decryption)	FCS_CKM.1 (1)	FCS_CKM.1 (1)	7
		FCS_CKM.4	FCS_CKM.4 (1)	11
		FMT_MSA.2	FMT_MSA.2 (1)	29
13	FCS_COP.1 (2) – Cryptographic Operation (Digital Signature)	FCS_CKM.1 (2)	FCS_CKM.1 (2)	8
		FCS_CKM.4	FCS_CKM.4 (1)	11
		FMT_MSA.2	FMT_MSA.2 (1)	29
14	FCS_COP.1 (3) – Cryptographic Operation (Hashing)	None	Not applicable. SHA Algorithm does not use keys.	-
15	FCS_COP.1 (4) – Cryptographic Operation (Key agreement)	FCS_CKM.1 (2)	FCS_CKM.1 (2)	8
		FCS_CKM.4	FCS_CKM.4 (1)	11
		FMT_MSA.2	FMT_MSA.2 (1)	29
16	FCS_COP.1 (5) – Cryptographic Operation (HMAC)	FCS_CKM.1 (1)	FCS_CKM.1 (2)	7
		FCS_CKM.4	FCS_CKM.4 (1)	11
		FMT_MSA.2	FMT_MSA.2 (1)	29
17	FCS_COP_(EXT).1 – Extended: Random Number Generation	None	N/A	-
18	FDP_PUD_(EXT).1 Protection of User Data	None	N/A	-

#	Functional Requirements	Dependencies from CC or PP	Met By SFR	Row Ref
19	FDP_RIP.1 (1) - Subset residual information protection	None	N/A	-
20	FIA_AFL.1 (1) - Administrator Authentication failure handling	FIA_UAU.1	FIA_UAU.1	23
21	FIA_ATD.1 (1) - Administrator attribute definition	None	N/A	-
22	FIA_ATD.1 (2) - User attribute definition	None	N/A	-
23	FIA_UAU.1 - Timing of local authentication	FIA_UID.1	FIA_UID.2 (1)	25
24	FIA_UAU_(EXT).5 – Multiple authentication mechanisms	None	N/A	-
25	FIA_UID.2 (1) - User identification before any action	None	N/A	-
26	FIA_USB.1 (1) - User-subject binding (Administrators)	FIA_ATD.1 (1)	FIA_ATD.1 (1)	21
27	FIA_USB.1 (2) - User-subject binding (Wireless user)	FIA_ATD.1 (2)	FIA_ATD.1 (2)	22
28	FMT_MOF.1 (1) - Management of security functions behavior (Cryptographic Function)	FMT_SMF.1 (1)	FMT_SMF.1 (1)	31
		FMT_SMR.1	FMT_SMR.1 (1)	32
29	FMT_MSA.2 (1) - Secure security attributes	FDP_IFC.1	FDP_PUD_(EXT).1	18
		FMT_MSA.1	FMT_MTD.1 (1)	30
		FMT_SMR.1	FMT_SMR.1 (1)	32
30	FMT_MTD.1 (1) - Management of Audit Data	FMT_SMF.1	FMT_SMF.1 (1)	31
		FMT_SMR.1	FMT_SMR.1 (1)	32
31	FMT_SMF.1 (1) - Specification of Management Functions (Cryptographic Functions)	None	N/A	-
32	FMT_SMR.1 (1) - Security roles	FIA_UID.1	FIA_UID.2 (1)	25
33	FPT_STM_(EXT).1 – Reliable time stamps	None	None	-
34	FPT_TST_(EXT).1 - TSF testing	None	None	-
35	FPT_TST.1 (1) - TSF testing (for cryptography)	None	None	-
36	FPT_TST.1 (2) - TSF testing (for key generation components)	None	None	-
37	FTA_SSL.3 (1) - TSF-initiated termination	None	None	-
38	FTA_TAB.1 (1) - Default TOE access banners	None	None	-
39	FTA_TSE.1 – TOE Session Establishment	None	None	-
40	FTP_ITC_(EXT).1 – Inter-TSF trusted channel	None	None	-
41	FTP_TRP.1 (1) – Trusted Path	None	None	-

Table 6-14: Security System SFR Dependencies

#	Functional Requirements	Dependencies from CC or PP	Met By	Row Ref #
1	FAU_GEN.1 (SS) - Audit data generation	FPT_STM.1	N/A Reliable time is provided by the environment	-
2	FAU_GEN.2 (SS) - User identity association	FAU_GEN.1	FAU_GEN.1 (SS)	1
		FIA_UID.1	FIA_UID.2 (SS)	32
3	FAU_SAR.1 (SS) – Audit review	FAU_GEN.1	FAU_GEN.1 (SS)	1
4	FAU_SAR.3 (SS) – Selectable audit review	FAU_SAR.1	FAU_SAR.1 (SS)	3
5	FAU_SEL.1 (SS) - Selective audit	FAU_GEN.1	FAU_GEN.1 (SS)	1
		FMT_MTD.1	FMT_MTD.1 (SS)	36
6	FCS_BCM_(SS).1 – Extended: Baseline Cryptographic Module	None	N/A	
7	FCS_CKM.1 (SS1) - Cryptographic key generation (for symmetric keys)	FCS_COP.1	FCS_COP.1 (SS1)	12
		FCS_CKM.4	FCS_CKM.4 (SS)	11
		FMT_MSA.2	FMT_MSA.2 (SS)	35
8	FCS_CKM.1 (SS2) - Cryptographic key generation (for asymmetric keys)	FCS_COP.1	FCS_COP.1 (SS2)	13
		FCS_CKM.4	FCS_CKM.4 (SS)	11
		FMT_MSA.2	FMT_MSA.2 (SS)	35
9	FCS_CKM.2 (SS) - Cryptographic key distribution	FCS_CKM.1	FCS_CKM.1 (SS1) FCS_CKM.1 (SS2)	7 8
		FMT_MSA.2	FMT_MSA.2 (SS)	35
10	FCS_CKM_(SS).2 - Cryptographic key handling and storage	FCS_CKM.1	FCS_CKM.1 (SS1) FCS_CKM.1(SS2)	7 8
		FMT_MSA.2	FMT_MSA.2 (SS)	35
11	FCS_CKM.4 (SS) - Cryptographic key destruction	FCS_CKM.1	FCS_CKM.1(SS1) FCS_CKM.1 (SS2)	7 8
		FMT_MSA.2	FMT_MSA.2 (SS)	35
12	FCS_COP.1 (SS1) – Cryptographic Operation (Data encryption/decryption)	FCS_CKM.1 (1)	FCS_CKM.1 (SS1)	7
		FCS_CKM.4	FCS_CKM.4 (SS)	11
		FMT_MSA.2	FMT_MSA.2 (SS)	35
13	FCS_COP.1 (SS2) – Cryptographic Operation (Digital Signature)	FCS_CKM.1(2)	FCS_CKM. (SS2)	8
		FCS_CKM.4	FCS_CKM.4 (SS)	11
		FMT_MSA.2	FMT_MSA.2 (SS)	35
14	FCS_COP.1 (SS3) – Cryptographic Operation (Hashing)	None	N/A SHA Algorithm does not use keys.	-
15	FCS_COP.1 (SS4) – Cryptographic Operation (Key agreement)	FCS_CKM.1	FCS_CKM.1 (SS1)	7
		FCS_CKM.4	FCS_CKM.4 (SS)	11
		FMT_MSA.2	FMT_MSA.2 (SS)	35
16	FCS_COP.1 (SS5) – Cryptographic Operation (HMAC)	FCS_CKM.1	N/A Key is entered manually	-
		FCS_CKM.4		
		FMT_MSA.2	FMT_MSA.2 (SS)	35
17	FCS_COP_(SS).1 – Extended: Random Number Generation	None	N/A	-
18	FDP_CPD_(SS).1 Extended: Certificate path development	None	N/A	-
19	FDP_DAU_CPI_(SS).1 Extended: Certificate path initialisation – basic	FCS_COP.1	FCS_COP.1 (SS2)	13
		FPT_STM.1	FPT_STM.1 (SS)	39

#	Functional Requirements	Dependencies from CC or PP	Met By	Row Ref #
20	FDP_DAU_CPV_(SS).1 Extended: Intermediate certificate processing - Basic	FCS_COP.!	FCS_COP.1 (SS2)	13
		FPT_STM.1	N/A Reliable time is provided by the environment	-
		[FDP_DAU_OCS_(EXT).1 or	FDP_DAU_OCS_(SS).1	24
		FDP_DAU_CRL_EXT).1]	FDP_DAU_CRL_(SS).1	23
21	FDP_DAU_CPV_(SS).2 Extended: Certificate processing - basic	FDP_DAU_CPV_(EXT).1	FDP_DAU_CPV_(SS).1	20
22	FDP_DAU_CPO_(SS).1 Extended: Certificate path output - basic	FDP_DAU_CPV_(EXT).1	FDP_DAU_CPV_(SS).1	20
23	FDP_DAU_CRL_(SS).1 Extended: Basic CRL Checking	FCS_BCM_(SS).1	FCS_BCM_(SS).1	6
		FPT_STM.1	N/A Reliable time is provided by the environment	-
24	FDP_DAU_OCS_(SS).1 Extended: Basic OCSP Client	FCS_BCM_(SS).1	FCS_BCM_(SS).1	6
		FPT_STM.1	N/A Reliable time is provided by the environment	-
25	FDP_ITC_SIG_(SS).1 Extended: Import of PKI Signature	FDP_DAU_CPO_(EXT).1	FDP_DAU_CPO_(SS).1	22
26	FDP_RIP.1 (SS) – Subset Residual Information Protection (Security Server)	None	N/A	-
27	FIA_AFL.1 (SS) - Administrator Authentication failure handling	FIA_UAU.1	FIA_UAU.2	30
28	FIA_ATD.1 (SS1) - Administrator attribute definition	None	N/A	-
29	FIA_ATD.1 (SS2) - User attribute definition	None	N/A	-
30	FIA_UAU.2 – User Authentication before any action	FIA_UID.1	FIA_UID.2 (SS)	32
31	FIA_UAU_(SS).5 – Multiple authentication mechanisms	None	N/A	-
32	FIA_UID.2 (SS) - User identification before any action	None	N/A	-
33	FIA_USB.1 (SS) - User-subject binding (Administrators)	FIA_ATD.1	FIA_ATD.1 (SS)	28
34	FMT_MOF.1 (SS) - Management of security functions behavior (Security Server)	FMT_SMF.1	FMT_SMF.1 (SS)	37
		FMT_SMR.1	FMT_SMR.1 (SS)	38
35	FMT_MSA.2 (SS) - Secure security attributes (Security Server)	FDP_ACC.1 or FDP_IFC.1	FDP_DAU_CPV_(SS).1 FIA_UAU_(SS).5	20 31
		FMT_MSA.1	FMT_MTD.1 (SS)	36
		FMT_SMR.1	FMT_SMR.1 (SS)	38
36	FMT_MTD.1 (SS) - Management of Audit Data	FMT_SMF.1	FMT_SMF.1 (SS)	37
		FMT_SMR.1	FMT_SMR.1 (SS)	38

#	Functional Requirements	Dependencies from CC or PP	Met By	Row Ref #
37	FMT_SMF.1 (SS) - Specification of Management Functions (Cryptographic Functions)	None	N/A	-
38	FMT_SMR.1 (SS) - Security roles	FIA_UID.1	FIA_UID.2 (SS)	32
39	FPT_TST_(SS).1 - TSF testing	None	N/A	-
40	FPT_TST.1 (SS1) - TSF testing (for cryptography)	None	N/A	-
41	FPT_TST.1 (SS2) - TSF testing (for key generation components)	None	N/A	-
42	FTA_SSL.3 (SS) - TSF-initiated termination	None	N/A	-
43	FTA_TAB.1 (SS)- Default TOE access banners	None	N/A	-
44	FTP_ITC_(SS).1 – Inter-TSF trusted channel	None	N/A	-
45	FTP_TRP.1 (SS) – Trusted Path	None	N/A	-

6.4.3 Rationale for Assurance Requirements

The Evaluation Assurance Level (EAL) 4 augmented by ALC_FLR.2 Flaw reporting procedures was chosen to meet customer requirements.

7 TOE Summary Specification

This chapter identifies and describes the security functions implemented by the TOE and the assurance measures applied to ensure their correct implementation.

7.1 Access Point IT Security Functions

Each of the security function descriptions is organized by the security requirements corresponding to the security function. Therefore, the description of each function emphasizes how the function specifically satisfies each of its related requirements. This serves to both describe the security functions and provide a rationale that the security functions are suitable to satisfy the necessary requirements.

Table 7-1: TOE Security Functions

Security Function		Functional Components	#
Audit (AU)	AU-1 Audit Generation	FAU_GEN.1 (1) - Audit data generation (Wireless Access Point)	1
	AU-2 Audit Identity Association	FAU_GEN.2 (1) - User identity association (Wireless Access Point)	2
	AU-3 Audit Review	FAU_SAR.1 (1) – Audit review (Wireless Access Point)	3
		FAU_SAR.3 (1) – Selectable audit review (Wireless Access Point)	4
	AU-4 Audit Selection	FAU_SEL.1 (1) - Selective audit (Wireless Access Point)	5
Cryptographic Support (FCS)	CS-1 Baseline Cryptographic Module	FCS_BCM_(EXT).1 – Extended: Baseline Cryptographic Module	6
	CS-2 Cryptographic Symmetric Key Generation	FCS_CKM.1 (1) - Cryptographic key generation (for symmetric keys on Wireless Access Point)	7
	CS-3 Cryptographic Asymmetric Key Generation	FCS_CKM.1 (2) - Cryptographic key generation (for asymmetric keys on Wireless Access Point)	8
	CS-4 Cryptographic Key Distribution	FCS_CKM.2 (1) - Cryptographic key distribution (Wireless Access Point)	9
	CS-5 Cryptographic Key Handling and Storage	FCS_CKM_(EXT).2 - Extended: Cryptographic key handling and storage	10
	CS-6 Cryptographic Key Destruction	FCS_CKM.4 - Cryptographic key destruction (Wireless Access Point)	11
	CS-7 Cryptographic Operation (Data encryption/decryption)	FCS_COP.1 (1) – Cryptographic Operation (Data encryption/decryption on Wireless Access Point)	12
	CS-8 Cryptographic Operation (Digital Signature)	FCS_COP.1 (2) – Cryptographic Operation (Digital Signature on Wireless Access Point)	13
	CS-9 Cryptographic Operation (Hashing)	FCS_COP.1(3) – Cryptographic Operation (Hashing on Wireless Access Point)	14
	CS-10 Cryptographic Operation (Key agreement)	FCS_COP.1 (4) – Cryptographic Operation (Key agreement on Wireless Access Point)	15
	CS-11 Keyed-Hash Message Authentication (HMAC)	FCS_COP.1 (5) – Cryptographic Operation (HMAC on Wireless Access Point)	16
	CS-12 Random Number Generation	FCS_COP_(EXT).1 – Extended: Random Number Generation	17

Security Function		Functional Components	#
User Data Protection (FDP)	DP-1 Protection of User Data	FDP_PUD_(EXT).1 – Extended: Protection of User Data	18
	DP-2 Residual Information Protection	FDP_RIP.1 (1) - Subset residual information protection (Wireless Access Point)	19
Identification and Authentication (FIA)	IA-1 Authentication Failure Handling	FIA_AFL.1 (1) - Administrator authentication failure handling (Wireless Access Point)	20
	IA-2 Attribute Definition	FIA_ATD.1 (1) - Administrator attribute definition (Wireless Access Point)	21
		FIA_ATD.1 (2) - User attribute definition (Wireless Access Point)	22
	IA-3 Identification and Authentication	FIA_UAU.1 – Timing of local authentication	23
		FIA_UAU_(EXT).5 – Extended: Multiple authentication mechanisms	24
		FIA_UID.2 (1) - User identification before any action (Wireless Access Point)	25
	IA-4 User-Subject Binding	FIA_USB.1 (1) - User-subject binding (Administrator on Wireless Access Point)	26
		FIA_USB.1 (2) - User-subject binding (Wireless User on Wireless Access Point)	27
Security Management (FMT)	SM-1 Management of TSF Functions and Data	FMT_MOF.1 (1) - Management of security functions behavior (Wireless Access Point)	28
		FMT_MSA.2 (1) - Secure security attributes (Wireless Access Point)	29
		FMT_MTD.1 (1) - Management of TSF Data (Wireless Access Point)	30
		FMT_SMF.1 (1) - Specification of Management Functions (Wireless Access Point)	31
	SM-2 Security Roles	FMT_SMR.1 (1) - Security roles (Wireless Access Point)	32
Protection of the TSF (FPT)	PT-1: Time Stamps	FPT_STM_(EXT).1 – Extended: Reliable time stamps	33
	PT-2: TSF Testing	FPT_TST_(EXT).1 - Extended: TSF testing	34
	PT-3: TSF Cryptographic Testing	FPT_TST.1 (1)- TSF testing (for cryptography on Wireless Access Point)	35
		FPT_TST.1 (2) - TSF testing (for key generation components on Wireless Access Point)	36
TOE Access (FTA)	TA-1: TSF-Initiated Termination	FTA_SSL.3 (1) - TSF-initiated termination (Wireless Access Point)	37
	TA-2: Default TOE Access banners	FTA_TAB.1 (1) - Default TOE access banners (Wireless Access Point)	38
	TA-3 MAC Address Filtering	FTA_TSE.1 – TOE Session Establishment	39
Trusted Path/Channels (FTP)	TC-1: Inter-TSF Trusted Channel	FTP_ITC_(EXT).1 Extended: Inter-TSF trusted channel	40
	TC-2: Trusted Path	FTP_TRP.1 (1) Trusted Path (Wireless Access Point)	41

7.1.1 Audit Functions

7.1.1.1 AU-1 Audit Generation

FAU_GEN.1 (1)

The TOE collects audit data for the events listed in Table 6-2: Auditable Events. 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).

The TOE exports audit data over HTTPS using AES-CBC-128 bit encryption.

7.1.1.2 AU-2 Audit Identity Association

FAU_GEN.2 (1)

All actions performed by the TOE are associated with users or with the unique MAC address of a client. User associated events are those performed through the Remote Management GUI, such as an administrator changing the TOE configuration settings. MAC address associated events are those that deal with traffic sent by clients of the TOE, such as successful shared secret authentication.

Since all actions performed by the TOE are associated with a unique identifier, this information is maintained in the audit record, allowing the events stored there to be traced directly to the user or system for which they were performed.

7.1.1.3 AU-3 Audit Review

FAU_SAR.1 (1), FAU_SAR.3 (1)

The Remote Management GUI provides an interface for Administrators and Crypto Officers to review audit records.

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

7.1.1.4 AU-4 Audit Selection

FAU_SEL.1 (1)

The TSF is able to select auditable events based on the following: user identity, event type, device interface, and wireless client identity. The administrator selects auditable events using the Web Management Application.

7.1.2 Cryptographic Support Functions

The cryptographic module for the APs is a combination of hardware and software.

The TOE provides both the user space cryptographic functionality using OpenSSL and kernel space cryptographic functionality using the Kernel Crypto Library.

OpenSSL provides the following cryptographic algorithms in FIPS mode:

- AES
- RSA
- HMAC
- SHA

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

- AES
- HMAC
- SHA1

7.1.2.1 CS-1 Baseline Cryptographic Module

FCS_BCM_(EXT).1

The 3eTI Access Points are undergoing FIPS 140 validation for an overall level 2, with level 3 for the sub-categories shown in Table 7-2 below.

The FIPS 140 certificate number for the 3e-523-F2 and 3e-523-3 Access Points is 1541.

The FIPS 140 certificate number for the 3e-525A-3, 3e-525V-3, and 3e-525VE-4 Access Points is 1476.

Table 7-2: Access Point FIPS-140 Levels

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	2
Cryptographic Key Management	3 (2)
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A
Operational Environment	N/A

*(2) 3e-523-F2 and 3e-523-3 meet level 2 for Cryptographic Key Management

The Security Policy for the 3e-523 Access Points is entitled:

> *"3e Technologies International, Inc., FIPS 140-2 Non-Proprietary Security Policy Level 2 Validation; 3e-523-F2 & 3e-523-3 Secure Multi-function Wireless Data Points; HW Versions 1.0, 1.1, 1.2, 2.0; FW Versions 4.4" "*

The Security Policy for the 3e-525 Access Points is entitled:

> *"3e Technologies International, Inc., FIPS 140-2 Non-Proprietary Security Policy Level 2 Validation; 3e-525A-3, 3e-525V-3, and 3e-525E-4 Secure Multi-function Wireless Data Points; HW Versions 2.0(A); FW Versions 4.4" "*

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

Table 7-3: Access Point FIPS-140 Tested Algorithms

Algorithm	Cert No.
RNG	583
OpenSSL	
AES	1022
TDES	783
SHS	976
HMAC	571
RSA	490
TDES	783
CryptoLib (Kernel)	
AES	1021
HMAC	570
SHS	975
TDES	782
CrytoCore (Intel XScale CPU)	
AES	1023

7.1.2.2 CS-2 Cryptographic Symmetric Key Generation

FCS_CKM.1 (1)

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

The symmetric key for communications between the TOE and the wireless client is generated during the 802.11i defined 4-way handshake process using random numbers generated by a FIPS-Approved Random Number Generator. The random numbers are exchanged and the key is then derived following NIST SP 800-56A.

The symmetric key for communications between the TOE and the administrator is generated using the Random Number Generator within the Extensible Authentication Protocol (EAP-TLS) during TLS session establishment using RSA keys for key wrapping and key establishment.

Table 7-4 below lists all the AES keys are used and managed in the Access Point.

Table 7-4: Access Point AES Key Use and Management

AES Key	Mode / Size	Input	Storage	Zeroization	Purpose
system config AES key (256 bit)	AES key (HEX string)	Hardcoded in FLASH	Plaintext in FLASH	Zeroized when firmware is upgraded	Used to encrypt the configuration file
AP / Client Static key	AES ECB (e/d; 128,192,256)	Input encrypted (using TLS session key)	Ciphertext in flash, Encrypted with “system config AES key”	N/A	Used to encrypt unicast, and broadcast/multitcast traffic in support of static mode

AES Key	Mode / Size	Input	Storage	Zeroization	Purpose
PTK	AES (key derivation; 256)	Not input (derived from PMK)	Plaintext in RAM	When 802.11i session ends	802.11i PTK
KEK	AES ECB(e/d; 128)	Not input (derived from PTK)	Plaintext in RAM	When 802.11i session ends	802.11i KEK
TK	AES CCM (e/d; 128)	Not input (derived from PTK)	Plaintext in RAM	When 802.11i session ends	802.11i TK
TK (copy in driver)	AES CCM (e/d; 128)	Not input (derived from PTK)	Plaintext in RAM	When 802.11i session ends.	802.11i TK
GMK	AES (key derivation; 256)	Not input (RNG)	Plaintext in RAM	Zeroized when local Antennae mode changed or when re-key period expires	802.11I
Backend key	AES ECB key (d;128)	Input encrypted (using TLS session key)	Ciphertext in flash, encrypted with “system config AES key”	N/A	Decrypt TLS master secret returned to session key) with “system config AES key” module by Security Server after successful user authentication in support of 802.11i EAPTLS
Bridging static key	AES ECB (e/d 128,192,256)	Input encrypted (using TLS session key)	Ciphertext in flash, encrypted with “system config AES key”	N/A	Used to encrypt bridged traffic between two modules

7.1.2.3 CS-3 Cryptographic Asymmetric Key Generation

FCS_CKM.1 (2)

Asymmetric RSA public/private keys are generated by a Certificate Authority. The certificates are installed into the TSF during the manufacturing process under a controlled process.

7.1.2.4 CS-4 Cryptographic Key Distribution

FCS_CKM.2

The TSF’s key material, such as the Pair-wise Master Key (PMK) for Wireless Protected Access (WPA2) in Pre-shared Key (PSK) mode, can be distributed manually over HTTPS secured channel by a remote authorized administrator.

7.1.2.5 CS-5 Cryptographic key handling and storage

FCS_CKM_EXT.2

Persistent keys and secrets are stored in flash in the encrypted form. These persistent keys and secrets include the RADIUS server password, RADIUS server Key Encryption Key, Pre-Shared Key (PSK), user-name, and password.

The master key used to read those secrets/keys are kept in split knowledge procedures, by using a secret stored at a known location on flash, together with the MAC address stored in EE Prom and hashed with a constant length string to produce a 128-bit key.

Active keys are stored in SDRAM.

The internal key transfer between TSF modules always uses an extra key integrity field so that key corruption can be detected.

7.1.2.6 CS-6 Cryptographic Key Destruction

FCS_CKM.4 (1)

During the association of a wireless client with an AP, the AP maintains keys that are used during the wireless client session with the TOE. If the wireless client session with an AP is terminated, then the keys associated with that wireless client on the AP are destroyed. A reboot of the AP will also destroy all keys resident on the AP.

The administrator can command the AP to delete keys and can also set when the APs should destroy keys after a given idle time. All keys in the TOE are overwritten with zeroes when they are deleted.

7.1.2.7 CS-7 Cryptographic Operation (Data encryption/decryption)

FCS_COP.1 (1)

The OpenSSL Library in user space and the Kernel Crypto Library in kernel space both provide AES for symmetric encryption/decryption.

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

AES_CCM mode is employed for wireless data traffic between an AP and a wireless client, while AES_ECB mode is used for wireless bridge inter-AP data payload encryption.

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.

The key used for communication between APs is manually input to the TOE through a secured channel (HTTPS) together with key error detection guard (CRC). The size of the key is 256 bits for static AES-ECB mode and 128 bits for AES-CCM mode.

The interface between the Access Point and the RADIUS server is the RADIUS protocol. All incoming and outgoing RADIUS messages have an integrity check using SHA1. This integrity field is encapsulated as one of the RADIUS attribute fields. The RADIUS-ACCEPT message

sent by the RADIUS server to the TOE contains the PMK attribute, this PMK attribute is encrypted using AES-Key-Wrap protocol RFC 3394. The Key wrap key size is 128 bits.

For TOE's AP interface to wireless client, AES_CCM with 128 bits key is used. For TOE's AP-AP bridge interface, AES_CCM with 128 bits key, or AES_ECB with 128, 192, 256 bits can be used by administrator's configuration. For TOE's TLS interface, AES_CBC with 128 or 256 bits key.

7.1.2.8 CS-8 Cryptographic Operation (Digital Signature)

FCS_COP.1 (2)

The OpenSSL Library provides the RSA Digital Signature Algorithm (DSA) to the HTTPS Daemon for the TLS session. The HTTPS Daemon enforces a 2048 bit RSA key length for use with the RSA DSA.

7.1.2.9 CS-9 Cryptographic Operation (Hashing)

FCS_COP.1 (3)

The TSF provides SHA with key sizes of 256, 384, or 512 for secure hashing.

7.1.2.10 CS-10 Cryptographic Operation (Key agreement)

FCS_COP.1 (4)

The TSF implements two cryptographic key agreement algorithms as follows:

- Establishment of wireless transient key between the TOE and the wireless client.
- Establishment of TLS session symmetric key between the TOE and the Administrator

Both key agreement operations are implemented in the OpenSSL Library sub-component.

Wireless Client

End-to-end wireless encryption between the TOE and the wireless client is implemented using WPA2-PSK.

The PMK is generated by the RADIUS Server in coordination with the wireless client, encrypted with the AES key wrap protocol, and passed to the AP. If the RADIUS Server is not available (WPA2/PSK mode), the PMK is entered manually.

The AP uses the PMK and the 802.11i four-way handshake to generate the Pairwise Transient Key (PTK) and the GTK (Group Temporal Key).

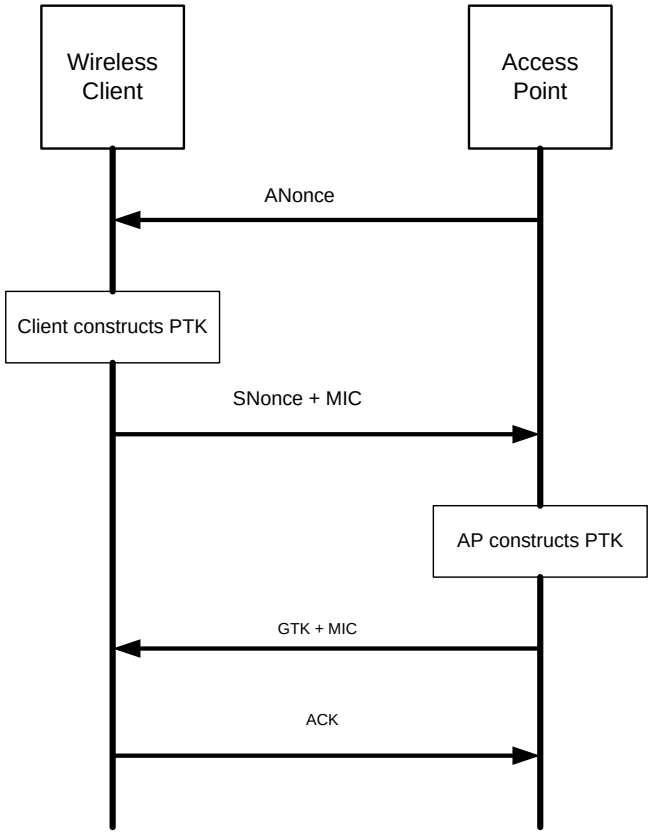
The PTK is generated by concatenating the following attributes: PMK, AP nonce (ANonce), the client (station) nonce (SNonce), AP MAC address, and client MAC address. The product is then put through a cryptographic hash function. The four steps are as follows:

1. The AP sends a nonce-value to the client (ANonce). The client now has all the attributes to construct the PTK.
2. The client sends its own nonce-value (SNonce) to the AP together with a MIC, including authentication, which is really a Message Authentication and Integrity Code: (MAIC).

3. The AP sends the GTK and a sequence number together with another MIC. This sequence number will be used in the next multicast or broadcast frame, so that the receiving STA can perform basic replay detection.
4. The client sends an acknowledgement to the AP.

The messages exchanged during the handshake are depicted in Figure 7-1 below.

Figure 7-1: 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 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.

VLAN

Each VLAN is essentially one virtual wireless access user domain. The wireless client has to be successfully authenticated to the TOE, though each VLAN uses its own

authentication setting. Each VLAN which maps to one unique SSID on the Wireless AP interface enforces its own wireless user data encryption. Within each VLAN, the wireless user undergoes the same key establishment procedure as described above for wireless user which is defined by IEEE 802.11i.

Administrator

Key establishment between the TOE and the Administrator occurs during TLS session establishment using public/private key pairs. The TLS session is setup between the administrator and TOE with mutual authentication, the TOE's server certificate contains 2048 bits or higher public key. The TOE's server side implementation will choose the cipher list that uses the finite field based key agreement such as TLS_DHE_DSS_WITH_AES_128_CBC_SHA or TLS_DHE_DSS_WITH_AES_256_CBC_SHA.

Wireless Bridge (Mesh)

Keys are manually input to the TOE for wireless Bridge/mesh network interface. By possessing the same key, the Access Point can successfully setup the wireless bridge and mesh network.

7.1.2.11 CS-11 Keyed-Hash Message Authentication (HMAC)

FCS_COP.1 (5)

The TOE's OpenSSL Library and the Kernel Crypto Library both implement an HMAC algorithm in FIPS-approved mode. Table 7-5 below describes how the HMAC algorithm is used and how the HMAC keys are input or derived, stored and zeroized.

Table 7-5: HMAC Algorithm Use and Key Management

HMAC Use	Key	Key Source	Key Storage	Key Destruction
Authenticate downloaded configuration file message	Configuration file pass phrase (ASCII string)	Input by Crypto Officer. Encrypted using TLS session key.	Plaintext in RAM.	Zeroized after use
Authenticate firmware load message	Firmware load key (ASCII string)	Embedded in firmware at compile time. Firmware upgrade is encrypted using TLS session key	Plaintext in flash	Zeroized when firmware is upgraded.
Authenticate SNMP message	SNMP packet auth keys (ASCII string)	Input, Encrypted using TLS session key	Ciphertext in flash, encrypted with "system config AES key"	Zeroized when reset to factory settings.
802.11i KCK	KCK	128 bits derived from PTK	Plaintext in RAM	When 802.11i session ends.
Authenticate module to Security Server	Security Server password (ASCII string)	Input, Encrypted using TLS session key	Ciphertext in flash, Encrypted with "system config AES key"	N/A
Authenticate messages between module and security server	Backend password (ASCII string)	Input, Encrypted using TLS session key	Ciphertext in flash, Encrypted with "system config AES key"	N/A

7.1.2.12 CS-12 Random Number Generation

FCS_COP_(EXT).1

The Random Number Generator is implemented using the FIPS 140-2 Digital Signature Standard (DSS) algorithm.

For the FIPS 140-2 Approved RNG implemented in the TOE, the seed and the seed key are generated through the following mechanism: XSEED is always zero. The seed key is generated using the OpenSSL RNG algorithm. The OpenSSL RNG algorithm is exclusively used as an input to the FIPS 186-3 approved RNG. It is the output of the FIPS 186-2 procedure that is used in the TOE as the random number for use.

The entropy sources for the RNG are system hardware interrupts counts. Those hardware interrupts counts are accumulated into a large file.

7.1.3 User Data Protection Functions

7.1.3.1 DP-1 User Data Protection

FDP_PUD_(EXT).1

Wireless Client

The administrator can control whether or not unencrypted data is allowed to pass through the TOE by using Access Control List (MAC address filtering). The allowed wireless client will be able to pass unencrypted authentication data through the TOE This encryption policy decides whether the AP will encrypt and decrypt communications with wireless clients.

After a wireless client has successfully authenticated to the TOE the wireless client can communicate with other wireless clients that have successfully authenticated through the TOE and with other wired clients that operate on the wired network controlled by the TOE. If the administrator has enabled encryption, the TOE will encrypt user data transmitted to a wireless client from the radio interface of the wireless access system and decrypt user data received from a wireless client by the radio interface of the wireless access system. This ensures that the TOE supports end-to-end wireless encryption.

Wireless Bridge

The data sent through the Wireless Bridge RF interface is always encrypted to safeguard the data privacy and integrity for data transmitted between APs.

VLAN

Each VLAN is essentially one virtual wireless access user domain. The wireless client has to be successfully authenticated to the TOE, though each VLAN uses its own authentication setting. Each VLAN which maps to one unique SSID on the Wireless AP interface enforces its own wireless user data encryption.

7.1.3.2 DP-2 Residual Information Protection

FDP_RIP.1

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

7.1.4 Identification and Authentication Functions

7.1.4.1 IA-1 Authentication failure handling

FIA_AFL.1

The Web Management Application will authenticate the administrator when the administrator logs in through the remote web browser over the HTTPS connection. The user name and password will be check against the local hashed value. If the failure count reaches the configured threshold, the HTTPS session will be terminated by the HTTPS server.

7.1.4.2 IA-2 Attribute definition

FIA_ATD.1 (1), FIA_ATD.1 (2)

User accounts associated with wireless clients have the following attributes: username, host MAC address, and authentication credentials. In the evaluated configuration, the authentication credentials may be either a certificate used for EAP-TLS or a pre-shared key used WPA-PSK. The client must present the authentication credentials prior to gaining general access to the WLAN resources.

Administrators have the following attributes: user name, password, and role. The role is either Crypto-officer or Administrator.

7.1.4.3 IA-3 Identification and Authentication

FIA_UAU.1, FIA_UAU_(EXT).5, FIA_UID.2

The TOE provides identification and authentication of wireless client users and administrators.

Wireless Client Authentication

The Access Point implements WiFi certified WPA2 security that also includes IEEE 802.1X port access control to provide for the authentication of wireless clients and to restrict unauthorized access into the TOE.

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

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

Once the wireless client and the AP have negotiated the required security methods, the authentication phase of the process is initiated. The Access Point provides both remote EAP-TLS and local WPA2-PSK pre-shared key authentication as described in the sections below. Local authentication of wireless clients is used when the RADIUS server is not available. During this 802.1x authentication state, the AP denies all packets sent by the client that are not 802.1x EAP packets.

After successful authentication of a wireless client, an IP address is also associated with the client. The IP address may be obtained from a DHCP server on the wired network, or if the client is not using DHCP, then the IP address already configured into the client will be used as an additional identifier for the client along with the MAC address.

Wireless Client Remote EAP-TLS Authentication

If remote EAP-TLS authentication is used, the AP encapsulates the 802.1X EAPOL authentication packets received from the wireless client using the RADIUS protocol and forwards them to the authentication server. The authentication server may be either the 3eTI Security Server included in the TOE or a third party authentication server in the IT environment. The 802.1x protocol allows for different EAP authentication methods.. The Access Point has been WPA2 WiFi certified for the following EAP variants: EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, and EAP-FAST.

However, since only EAP-TLS is available in FIPS mode, EAP-TLS must be used in the evaluated configuration. When EAP-TLS is configured, mutual authentication is performed between the supplicant (wireless user) and the authentication server.

Wireless Client Local WPA2-PSK Authentication

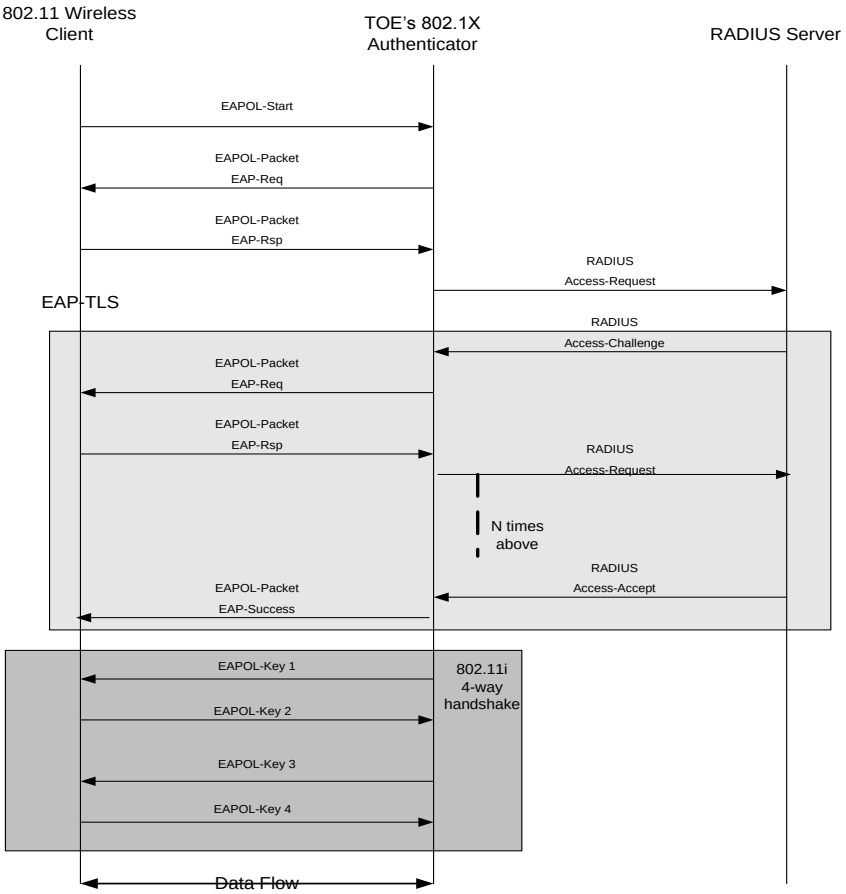
Wireless User local authentication mode is necessary if the RADIUS server is not available in the Operational Environment. To make the local authentication possible, the AP Driver will allow the EAPOL message from un-authenticated client to go to 802.11 Authenticator Module the Access Point). The Access Point uses the fact that the wireless client user possesses the Pre-Shared Key (PSK) to perform authentication.

The TOE is able to implement FIPS 140-2 validated WPA2 using a pre-share key (WPA2-PSK). Using WPA2-PSK does not require the use of an authentication server. When using WPA2-PSK, authentication is done between the supplicant (wireless client) and the authenticator (the Access Point). The PSK acts as a type of authentication credential when WPA2-PSK is used. The PSK is a pass phrase that is set by the administrator of the TOE through the HTTPS management interface.

EAP Packet Flow

Figure 7-2 below depicts the flow of EAP packets between the wireless client, the AP, and the RADIUS Server during a successful 802.1X authentication session.

Figure 7-2: EAP Packet Flow



The upper third of Figure 7-2 shows the packet flow during the initial association between the wireless client and the AP using EAPOL-Start. The AP responds with an EAP Response packet., and the wireless client sends an EAP Access-Request packet.

The middle third of Figure 7-2 shows the communication between the AP and the RADIUS Server over EAP-TLS, when the RADIUS Server is available.

Finally, the lower third depicts the 4-way handshake used to generate the Pairwise-Transient Key (PTK) and the Group Transient Key (GTK) for AES communications as described in Section 7.1.2.10CS-10 Cryptographic Operation (Key agreement).

Wireless User Authentication in VLAN

Each VLAN is essentially a virtual wireless access user domain. Each VLAN has separate authentication setting which can be either remote authentication via EAP-TLS or local WPA2-PSK. When a wireless user access the TOE through one SSID, it's automatically assigned to that VLAN (one-to-one mapping between VLAN and SSID) and that VLAN's authentication mechanism will be enforce by the TOE to authenticate the wireless user.

Wireless Bridge Authentication

For wireless bridge authentication between two Access Points, the possession of the same AES key is used to authenticate the remote Access Point. Only after successful authentication, will the user data packets be allowed to pass through the Access Point

Administrator

An administrator provides a username and password through the HTTPS client. In the evaluated configuration, HTTPS is used for web interface communication. HTTP is disabled and is not used in the evaluated configuration. The TOE then authenticates and authorizes the administrator's access into TOE.

Audit of Authentication Attempts

All authentication successful and unsuccessful authentication attempts are audited by the Access Point including remote and local authentication of wireless clients and local authentication for the management user.

7.1.4.4 IA-4 User-subject binding

FIA_USB.1 (1), FIA_USB.1 (2)

All actions within the TOE are tied to the wireless users/clients accessing the TOE resources through unique bindings. This allows each action or process to be uniquely identified with a specific user or client connected to the TOE. The primary mechanism of this binding is the authentication credentials of the wireless client (or user), with a secondary binding (that never conflicts) being the MAC address or the username.

The Session Set ID (SSID) maps to the VLAN tag ID of the client. The TOE supports up to 8 extended SSIDs.

The administrator first authenticates to the Web Management Application using a user name and password. Then the authorized administrator is bound with its defined role, either Crypto-Officer or Administrator.

7.1.5 Security Management Functions

The Web Management Application provides capabilities for the authorized administrator to manage cryptographic, audit, and authentication functions and data.

7.1.5.1 SM-1 Management of TOE Functions and Data

FMT_MOF.1(1), FMT_MSA.2, FMT_SMF.1(1), FMT_SMF.1(3)

The TOE provides the Crypto-Officer with the ability to configure the cryptographic settings of the WLAN environment.

The Crypto-Officer can perform the following cryptographic operations:

- Load a key
- Delete/zeroize a key
- Set a key lifetime
- Set the cryptographic algorithm
- Set the TOE to encrypt or not to encrypt wireless transmissions

- Execute self tests of TOE hardware and the cryptographic functions

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

The TOE provides the Crypto-Officer with the ability to manage the audit settings of the TOE. The Crypto-Officer can perform the following audit functions:.

- Pre-selection of the events that trigger an audit record,
- Start and stop of the audit function

Authorized administrators are able to configure the users/clients that can access the TOE. The types of credentials which can be modified are pre-shared keys (such as those used in WPA2) and certificates (for EAP-TLS).

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

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

- Enable or disable the use of an authentication server
- Set the number of authentication failures that may occur before the TOE takes action to disallow future logins

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

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

7.1.5.2 SM-2 Security Roles

FMT_SMR.1 (1)

The TOE provides three roles: Crypto-Officer, Administrator, and user.

The Crypto-Officer and Administrator are both authorized administrators.

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

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

All other management functions in the TOE can be performed by the Administrator as well as the Crypto-Officer. Any authorized administrator can create client user accounts with certificates,although only the Crypto-Officer can establish this mechanism for authentication. An

authorized administrator has the ability to modify, delete, clear, and create security relevant data.

The user role is the implicit role for anyone accessing the system as a wireless client through the WLAN. The user role has no administrative ability on the TOE, only the ability to access the WLAN resources.

7.1.6 Protection of the TSF Functions

7.1.6.1 PT-1 Time Stamps

FPT_STM_(EXT).1

The Access Point has a running NTP daemon to synchronize the local time with an external NTP server.. In the absence of an NTP server in the Operational Environment, the authorized administrator has the capability to set the time locally.

7.1.6.2 PT-2 TSF Testing

FPT_TST_(EXT).1

The TSF performs a firmware integrity check and a configuration file integrity check on system start up, periodically in maintenance mode, and at administrator request.

7.1.6.3 PT-3 TSF Cryptographic Testing

FPT_TST.1 (1), FPT_TST.1 (2)

The self-test module can execute at power-on initialization time, on a request from the management application initiated by authorized administrator, and at a configurable time interval. During the TSF cryptographic testing, the RNG/PRNG, algorithms and key error detection are tested. A software integrity check, key and security parameters integrity checks, and cryptographic tests including RSA sign, RSA verify, AES_CCM and SHA1 tests, are also performed during TSF cryptographic testing.

The TOE performs the following power-up and conditional self-tests:

Power-up self-tests with known answer tests (KAT):

- AES ECB - encrypt/decrypt KAT
- AES CCM KAT
- SHA-1 KAT
- HMAC-SHA-1 KAT
- FIPS 186-2 (Appendix 3.1, 3.3) RNG KAT
- SHA-1 Integrity Test for firmware

Conditional self-tests:

- CRNGT for Approved PRNG
- CRNGT for non-Approved PRNG (Open SSL based RNG)

Bypass Tests

- Firmware Load Test using HMAC-SHA-1

The TOE also performs an odd parity check on all internal and intermediate key transfers. This serves as a key error detection check.

The administrator and Security Officer can request self-tests to be executed or set the time period for periodic testing through HTTPS Web Management interface.

If any of these tests fail, an audit record is generated.

7.1.7 TOE Access Functions

7.1.7.1 TA-1 TSF-Initiated Termination

FTA_SSL.3 (1)

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

The AP Driver implements a wireless user inactivity watch timer to drop a wireless client user, if the defined time interval is reached without any user data activity.

Both time intervals are configurable by the authorized administrator.

7.1.7.2 TA-2 TOE Access Banners

FTA_TAB.1 (1)

The Remote Management GUI displays a TOE access banner to the remote administrative user before the user can log into the system.

7.1.7.3 TA-3 MAC Address Filtering

FTA_TSE.1

The TOE can be configured to filter connections by MAC address

7.1.8 Trusted Path/Channels Functions

7.1.8.1 TC-1 Inter-TSF Trusted Channel

FTP_ITC_(EXT).1

The Access Point provides an encrypted communication channel between the TOE and the authentication server. The Access Point initially uses a password to authenticate its RADIUS messages to the authentication server in support of EAP-TLS authentication. The Access Point then uses a Backend AES key to decrypt the wrapped PMK returned to the TOE by the authentication server after successful authentication.

Messages passed between the TOE and the Audit servers in the Operational Environment are encrypted using HTTPS.

7.1.8.2 TC-2 Trusted Path

FTP_TRP.1 (1)

The TOE's implementation of IEEE 802.11 fully supports WPA and WPA2, which protects initial authentication data between the wireless client and the access point. The TOE is managed through a remote session with HTTPS that provides a trusted path.

7.2 Security Server IT Security Functions

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

Table 7-6: Security Server IT Security Functions

Security Function		Functional Components	#
Audit (AU)	AU-SS1 Audit Generation	FAU_GEN.1 (SS) – Audit data generation (Security Server)	1
	AU-SS2 Audit Identity Association	FAU_GEN.2 (SS) – User identity association (Security Server)	2
	AU-SS3 Audit Review	FAU_SAR.1 (SS) Audit review (Security Server)	3
		FAU_SAR.3 (SS) Selectable audit review (Security Server)	4
	AU-SS4 Audit Selection	FAU_SEL.1 (SS) – Selective Audit (Security Server)	5
Cryptographic Support (FCS)	CS-SS1 Baseline Cryptographic Module	FCS_BCM_(SS).1 – Extended: Security Server baseline cryptographic module	6
	CS-SS2 Cryptographic Symmetric Key Generation	FCS_CKM.1 (SS1) - Cryptographic key generation (for symmetric keys on Security Server)	7
	CS-SS3 Cryptographic Asymmetric Key Generation	FCS_CKM.1 (SS2) - Cryptographic key generation (for asymmetric keys on Security Server)	8
	CS-SS4 Cryptographic Key Distribution	FCS_CKM.2 (SS) - Cryptographic key distribution (Security Server)	9
	CS-SS5 Cryptographic Key Handling and Storage	FCS_CKM_(SS).2 - Cryptographic key handling and storage on Security Server	10
	CS-SS6 Cryptographic Key Destruction	FCS_CKM.4 (SS) - Cryptographic key destruction (Security Server)	11
	CS-SS7 Cryptographic Operation (Data encryption/decryption)	FCS_COP.1 (SS1) – Cryptographic Operation (Data encryption/decryption on Security Server)	12
	CS-SS8 Cryptographic Operation (Digital Signature)	FCS_COP.1 (SS2) – Cryptographic Operation (Digital Signature on Security Server)	13
	CS-SS9 Cryptographic Operation (Hashing)	FCS_COP.1 (SS3) – Cryptographic Operation (Secure Hash on Security Server)	14

Security Function		Functional Components	#
	CS-SS10 Cryptographic Operation (Key agreement)	FCS_COP.1 (SS4) - Cryptographic Operation (Key Agreement on Security Server)	15
	CS-SS11 Keyed-Hash Message Authentication (HMAC)	FCS_COP.1 (SS5) – Cryptographic Operation (HMAC on Security Server)	16
	CS- SS12 Random Number Generation	FCS_COP_(SS),1 – Extended: Security Server random number generation	17
User Data Protection (FDP)	DP-SS1 Certificate Path Validation	FDP_CPD_(SS).1 Extended: Certificate path development	18
		FDP_DAU_CPL_(SS).1 Extended: Certificate path initialisation – basic	19
		FDP_DAU_CPV_(SS).1 Extended: Intermediate certificate processing - Basic	20
		FDP_DAU_CPV_(SS).2 Extended: Certificate processing - basic	21
		FDP_DAU_CPV_(SS).1 Extended: Certificate path output - basic	22
	DP-SS2 CRL Checking	FDP_DAU_CRL_(SS).1 Extended: Basic CRL Checking	23
	DP-SS3 OCSP Client	FDP_DAU_OCS_(SS).1 Extended: Basic OCSP Client	24
	DP-SS4 PKI Signature Verification	FDP_ITC_SIG_(SS).1 Extended: Import of PKI Signature	25
	DP-SS5 Residual Information Protection	FDP_RIP.1 (SS) – Subset Residual Information Protection (Security Server)	26
Identification and Authentication (FIA)	IA-SS1 Authentication Failure Handling	FIA_AFL.1 (SS) – Authentication failure handling (Security Server Administrator)	27
	IA-SS2 Attribute Definition	FIA_ATD.1 (SS1) – Administrator attribute definition (Security Server)	28
		FIA_ATD.1 (SS2) – User attribute definition (Security Server)	29
	IA-SS3 RADIUS Server Identification and Authentication	FIA_UAU.2 – User authentication before any action	30
		FIA_UAU.5 – Multiple authentication mechanisms	31
		FIA_UID.2 (SS) – User identification before any action (Security Server)	32
	IA-SS4 Security Officer Identification and Authentication	FIA_UAU.2 – User authentication before any action	30
		FIA_UAU.5 – Multiple authentication mechanisms	31
		FIA_UID.2 (SS) – User identification before any action (Security Server)	32
	IA-SS5 User-Subject Binding	FIA_USB.1 (SS) - User-subject binding (Security Server Administrator)	33
Security Management (FMT)	SM-SS1: Management of the Security Server	FMT_MOF.1 (SS) - Management of security functions behavior (Security Server)	34
		FMT_MSA.2 (SS) - Secure security attributes (Security Server)	35
		FMT_MTD.1 (SS) - Management of TSF Data (Security Server)	36

Security Function		Functional Components	#
		FMT_SMF.1 (SS) - Specification of Management Functions (Security Server)	37
	SM-SS2 Security Roles	FMT_SMR.1 (SS) - Security roles (Security Server)	38
Protection of the TSF (FPT)	PT-SS1: Security Server Testing	FPT_TST_(SS).1 - Extended Security Server testing	39
		FPT_TST.1 (SS1) - TSF testing (Security Server Cryptography	40
		FPT_TST.1 (SS2) - TSF testing (Security Server Key Generation Components)	41
TOE Access (FTA)	TA-SS1 TSF Initiated Termination	FTA_SSL.3 (SS) TSF-initiated termination (Security Server)	42
	TA-SS2 TOE Access Banners	FTA_TAB.1 (SS) Default TOE access banners (Security Server)	43
Trusted Path/Channels (FTP)	TC-SS1: Security Server Trusted Channels	FTP_ITC_(SS).1 – Extended Security Server trusted channel	44
	TC-SS2 Trusted Path	FTP_TRC.1 (SS) – Trusted Path (Security Server)	45

7.2.1 Audit Functions

7.2.1.1 AU-SS1 Audit Generation

FAU_GEN.1 (SS)

The Security Server collects audit data for the events listed in Table 6-2: Auditable Events. 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).

The Security Server relies on the Operational Environment to provide reliable time. The Security Server platform has a running NTP daemon to synchronize the local time with an external NTP server. In the absence of an NTP server in the Operational Environment, the Security Officer has the capability to set the time locally.

7.2.1.2 AU-SS2 Audit Identity Association

FAU_GEN.2 (SS)

All actions performed by the Security Server are associated with users or with the unique MAC address of a client. User associated events are those performed through the Remote Management GUI interface, such as an administrator changing the TOE configuration settings. MAC address associated events are those that deal with traffic sent by clients of the TOE, such as successful shared secret authentication.

Since all actions performed by the TOE are associated with a unique identifier, this information is maintained in the audit record, allowing the events stored there to be traced directly to the user or system for which they were performed.

7.2.1.3 AU-SS3 Audit Review

FAU_SAR.1 (SS)
FAU_SAR.3 (SS)

The Remote Management GUI provides an interface for Security Officer to review audit records.

Audit records can be selected on the basis of start time and end time.

7.2.1.4 AU-SS4 Audit Selection

FAU_SEL.1 (SS)

The Security Server is able to select auditable events based on the following: user identity, event type, device interface, and wireless client identity. The administrator selects auditable events using the Web Management Application.

7.2.2 Cryptographic Support Functions

Cryptographic functionality is provided by the OpenSSL Library sub-component of the Security Server.

All cryptographic operations performed by the Security Server in FIPS mode use only FIPS-approved algorithms. The corresponding FIPS 140-2 approved algorithms are all CAVP validated by 3eTI as listed in Table 7-7 below.

Table 7-7: Security Server FIPS-140 Tested Algorithms and Their Purpose

Algorithm	Purpose	FIPS 140 Cert #
AES-128 (CBC)	EAP-TLS	CAVP certificate # 1546
AES-256 (CBC)	EAP-TLS	CAVP certificate # 1546
AES-128 (ECB)	FIPS AES Key Wrap	CAVP certificate # 1546
SHA-1	RADIUS FIPS Authentication EAP-TLS	CAVP certificate #1371
SHA-256	EAP-TLS	CAVP certificate #1371
SHA-384	EAP-TLS	CAVP certificate #1371
HMAC-SHA-1	RADIUS FIPS Authentication EAP-TLS	CAVP certificate #879
RSA	EAP-TLS	CAVP certificate # 749
DSA	EAP-TLS	(CAVP certificate # 478
ECDSA	EAP-TLS	CAVP certificate # 191
RNG	EAP-TLS	CAVP certificate #834

The TOE provides additional cryptographic algorithms, but the CC evaluated configuration operates in FIPS mode.

7.2.2.1 CS-SS1 Baseline Cryptographic Module

FCS_BCM_(SS).1

The 3eTI Security Server Cryptographic Core is undergoing a FIPS 140-2 certification. The FIPS 140 certificate number is 1563.

This 3eTI Security Server Cryptographic Core module meets the overall requirements to Level 1 security of FIPS 140-2. Table 7-8 below summarizes the subcategory specifications:

Table 7-8: Security Server FIPS-140 Levels

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	3
Finite State Model	1
Physical Security	N/A
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	N/A
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

The Security Policy is entitled:

> *"3e Technologies International, Inc., FIPS 140-2 Non-Proprietary Security Policy; 3e-030-2 Security Server Cryptographic Core (Version 4.0)"*

When the TOE is operated in FIPS-mode, all cryptographic operations performed by the TOE are FIPS-compliant, using only FIPS-approved algorithms.

7.2.2.2 CS-SS2 Symmetric Key Generation

FCS_CKM.1 (SS1)

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

The symmetric key for communications between the Security Server and the administrator is generated using the Random Number Generator within the Extensible Authentication Protocol (EAP-TLS) during TLS session establishment using RSA keys.

AES keys are also used for key wrapping and key establishment.

7.2.2.3 CS-SS3 Asymmetric Key Generation

FCS_CKM.1 (SS2)

Asymmetric public/private key pairs for the DSA, rDSA, and ecDSA digital signature algorithms are generated externally by a Certificate Authority off-line and imported into the Security Server.

7.2.2.4 CS-SS4 Cryptographic Key Distribution

FCS_CKM.2 (SS)

The Pair-wise Master Key (PMK) sent from the Security Server to the Access Point is AES key-wrapped with the AES Key Encryption Key (KEK).

7.2.2.5 CS-SS5 Cryptographic key handling and storage

FCS_CKM_(SS).2

All plaintext keys are stored in volatile RAM only. Plaintext keys are promptly destroyed after their usage. Persistent keys stored in files or on hard disk are encrypted all the time. The master key used to encrypt and decrypt the persistent keys is stored with split knowledge procedures.

7.2.2.6 CS-SS6 Cryptographic Key Destruction

FCS_CKM.4 (SS)

All keys except public security parameters such as public keys are zeroized and freed once no longer needed.

The Security Officer can also delete keys. All keys in the TOE are overwritten with zeroes when they are deleted.

7.2.2.7 CS-SS7 Cryptographic Operation (Data encryption/decryption)

FCS_COP.1 (SS1)

The OpenSSL Library provides AES for symmetric encryption/decryption.

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

AES_CCM mode is employed for wireless data traffic between AP and wireless client, while AES_ECB mode is used for wireless bridge inter-AP data payload encryption.

The Cipher Block Chaining Message Authentication Code (CBC-MAC) component of CCMP provides data integrity. The CBC-MAC allows for the detection of a modified packet. If a CBC-MAC indicates a packet has been modified the packet is dropped.

7.2.2.8 CS-SS8 Cryptographic Operation (Digital Signature)

FCS_COP.1 (SS2)

The Security Server implements the rDSA, DSA, and ecDSA digital signature algorithms using its OpenSSL Library. The key sizes are 2048 bits or higher for rDSA, 1024 bits or higher for DSA, and 160 bits for or higher for ecDSA.

The OpenSSL Library provides the RSA Digital Signature Algorithm (DSA) to the HTTPS Daemon for the TLS session . The HTTPS Daemon enforces a 2048 bit RSA key length for use with the RSA DSA.

The Security Server trust anchor is a self-signed ecDSA public key certificate.

The Security Server also imports CA public key certificates to support certificate path validation.

7.2.2.9 CS-SS9 Cryptographic Operation (Hashing)

FCS_COP.1 (SS3)

The Security Server provides SHA with key sizes of 160, 256, 384, or 512 bits for secure hashing.

7.2.2.10 CS-SS10 Cryptographic Operation (Key agreement)

FCS_COP.1 (SS4)

The Security Server implements two cryptographic key agreement algorithms. Both key agreement operations are implemented in the OpenSSL Library sub-component.

The RADIUS Server sub-component uses EAP-TLS to establish the Pairwise Master Key (PMK). A description of this process is provided in Section 7.1.4.3 IA-3 Identification and Authentication.

Key establishment between the Remote Management GUI and the Security Officer occurs during TLS session establishment using RSA public/private key pairs.

7.2.2.11 CS-SS11 Keyed-Hash Message Authentication (HMAC)

FCS_COP.1 (SS5)

The Security Server's OpenSSL Library implements an HMAC algorithm in FIPS-approved mode.

HMAC is used by the Security Server for authentication of the Access Point and to unwrap the PMK generated as part of the EAP-TLS RADIUS authentication process.

7.2.2.12 CS-SS12 Random Number Generation

FCS_COP_(SS).1

The Random Number Generator is implemented using the FIPS 140-2 Digital Signature Standard (DSS) algorithm.

For the FIPS 140-2 Approved RNG implemented in the TOE, the seed and the seed key are generated through the following mechanism: XSEED is always zero. The seed key is generated using the OpenSSL RNG algorithm. The OpenSSL RNG algorithm is exclusively used as an input to the FIPS 186-3 approved RNG. It is the output of the FIPS 186-3 procedure that is used in the TOE as the random number for use.

The entropy sources for the RNG are system hardware interrupts counts. Those hardware interrupts counts are accumulated into a large file.

7.2.3 User Data Protection Functions

7.2.3.1 DP-SS1 Certificate Path Validation

FDP_CPD_(SS).1, FDP_DAU_CPL_(SS).1, FDP_DAU_CPV_(SS).1, FDP_DAU_CPV_(SS).2,

FDP_DAU_CPV_(SS).1,

The RADIUS Server sub-component of the Security Server provides Certificate Path Validation functionality.

The trusted anchor is a self-signed ECDSA certificate. The public/private key pair is generated externally and imported into the TOE.

CA Certificates are also generated externally and imported into the TOE.

7.2.3.2 DP-SS2 CRL Checking

FDP_DAU_CRL_(SS).1

The Security Server checks locally stored certificate revocation lists to ensure that certificates provided by users and intermediate certificates have not been revoked.

The Security Officer imports CRL lists into the TOE from an LDAP server.

7.2.3.3 DP-SS2 OCSP Client

FDP_DAU_OCS_(SS).1

The Security Server provides an Online Certificate Status Protocol (OCSP) client that can check with an OCSP responder to determine the status of a specific X.509 certificate.

7.2.3.4 DP-SS4 Digital Signature Verification

FDP_ITC_SIG_(SS).1

The digital signature verification function is provided by the OpenSSL Library.

7.2.3.5 DP-SS5 Residual Information Protection

FDP_RIP.1 (SS)

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

7.2.4 Identification and Authentication Functions

7.2.4.1 IA-SS1 Authentication failure handling

FIA_AFL.1 (SS)

The Web Management Application will authenticate the Security Officer when they log in through a remote web browser over the HTTPS connection. The user name and password will be checked against the local hashed value. If the consecutive failure count reaches 3 consecutive unsuccessful attempts, the HTTPS session will be terminated by the HTTPS server.

7.2.4.2 IA-SS2 Attribute definition

FIA_ATD.1 (SS1), FIA_ATD.1 (SS2)

The Security Officer is the trusted administrator for the Security Server and has the following attributes: user name, password, and role.

The Security Server also stores attributes for remote users that are authenticated by the RADIUS Server sub-component. In the evaluated configuration, the remote user authentication credentials are Public Key certificates.

7.2.4.3 IA-SS3 RADIUS Server Identification and Authentication

FIA_UAU.2 (SS), FIA_UAU_(SS).5, FIA_UID.2 (SS)

The Security Server provides identification and authentication of remote users using the RADIUS Server sub-component.

The 3eTI Security Server performs the Authentication Server (AS) function identified by IEEE 802.1x. During authentication, the AP translates wireless frames from the client into EAP-TLS messages encapsulated in RADIUS messages to be sent to the authentication server (AS). The authentication request is sent as a RADIUS "Access-Request." The RADIUS Server responds with either a "Access-Accept", "Access-Reject", or "Access-Challenge" message.

A detailed description of the EAP-TLS RADIUS authentication process is provided in Section 7.1.4.3 IA-3 Identification and Authentication.

7.2.4.4 IA-SS4 Security Officer Identification and Authentication

FIA_UAU.2 (SS), FIA_UAU_(SS).5, FIA_UID.2 (SS)

The Security Officer provides a username and password through the HTTPS client. HTTPS is the configured option for web interface communication in the evaluated configuration. HTTP is disabled and is not used in the evaluated configuration. The Security Server then authenticates and authorizes the administrator's access into TOE.

7.2.4.5 IA-SS5 User-subject binding

FIA_USB.1 (SS)

A Security Officer first authenticates to the Web Management Application using a user name and password. The Security Officer is bound to the Security Officer role.

7.2.5 Security Management Functions

7.2.5.1 SM-SS1 Management of Security Server

FMT_MOF.1 (SS), FMT_MSA.2 (SS), FMT_MTD.1 (SS), and FMT_SMF.1 (SS)

The Security Officer can perform the following audit-related operations:

- Pre-selection of the events which trigger an audit record,
- Start and stop of the audit function

The Security Officer can perform the following cryptographic-related operations:

- Load a key
- Delete/zeroize a key
- Set a key lifetime
- Set the cryptographic algorithm
- Execute self tests of TOE hardware and the cryptographic functions

The Security Officer is able to perform the following certificate related operations:

- Install and delete the Security Server certificate and its associated private key and password
- Install and delete CA certificates
- Install and delete Certificate Revocation Lists
- Configure the OCSP client

The Security Officer is able to perform the following TOE Access-related operations

- Set the number of authentication failures that must occur before the Security Server takes action to disallow future logins
- Set the length of time a session may remain inactive before it is terminated
- Set TOE Access Banner

7.2.5.2 SM-SS2 Security Roles

FMT_SMR.1 (SS)

The Security Server provides two roles: Security Officer and remote user.

All the management functions in the TOE are performed by the Security Officer.

The remote user does not access the Security Server directly, but is authenticated by the RADIUS server.

7.2.6 Protection of the TSF Functions

7.2.6.1 PT-SS1 TSF Testing

FPT_TST_(SS).1, FPT_TST.1 (SS1), FPT_TST.1 (SS2)

The Security Server performs TSF testing upon initialization and at the request of the Security Officer

The Security Server implements an integrity test for the module software by verifying its 384 bit ECDSA signature. The software integrity test passes if and only if the signature verifies successfully using the ECDSA public key. Upon software updates, during which the security server is re-initialized, this integrity check is always performed as well.

The power-on self test consists of a software integrity test and known answer tests for the cryptographic algorithm implementations.

The TOE performs the following testing of cryptographic functionality

- AES ECB - encrypt/decrypt KAT
- AES CBC -encrypt/decrypt KAT
- AES Key Wrap KAT
- SHA-1 KAT
- SHA-2 KAT
- HMAC-SHA-1 KAT

- PRNG FIPS 186-2 (Appendix 3.1, 3.3) KAT
- RSA Sign/Verify, Encrypt/Decrypt KAT
- DSA Sign/Verify, Encrypt/Decrypt KAT
- ECDSA Sign/Verify, Encrypt/Decrypt KAT
- Software Integrity Test
- CRNGT for Approved PRNG
- DH pair wise consistency test (power-up)

If any of the above tests fail, an audit record is generated.

7.2.7 TOE Access Functions

7.2.7.1 TA-SS1 TSF-Initiated Termination

FTA_SSL.3 (SS)

The Web Management Application will close the remote session, if it detects inactivity longer than the predefined time period. The remote session will be closed by the Web Management Application together with the HTTPS session.

7.2.7.2 TA-SS2 TOE Access Banners

FTA_TAB.1 (SS)

The Web Management Application displays a TOE access banner to the remote user before the user can log into the system.

7.2.8 Trusted Path/Channels Functions

7.2.8.1 TC-SS1 TSF Trusted Channel

FTP_ITC_(SS).1

The TOE provides an encrypted communication channel between the Security Server and the Access Point. The Access Point initially uses a password to authenticate the RADIUS messages sent to the RADIUS Server sub-component in support of EAP-TLS authentication. The Security Server sends the Pair-wise Master Key that is a result of EAP-TLS to the Access Point wrapped in an AES Key Encryption Key (KEK).

All incoming and outgoing RADIUS messages have an integrity check using SHA1. This integrity field is encapsulated as one of the RADIUS attribute field. The RADIUS-ACCEPT message sent by the RADIUS server to the TOE contains the PMK attribute, this PMK attribute is encrypted using AES-Key-Wrap protocol RFC 3394. The Key wrap key size is 128 bits.

The connections between the Security Server and the Audit Servers in the Operational Environment are made using HTTPS.

7.2.8.2 TC-SS2 Trusted Path

FTP_TRP.1 (SS)

The Security Server uses HTTPS (HTTP over TLS) for communication between the trusted administrator (Security Officer) and the Security Server.