National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Report Number: **CCEVS-VR-VID10409**

Dated: **August 19, 2011**

Version: **1.0 Final**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Mr. Deepak Somesula

CygnaCom Solutions

McLean, Virginia

Table of Contents

List of Figures

1 Executive Summary

This Validation Report (VR) documents the evaluation and validation of the product 3eTIAirguard™ Wireless Network Access System.

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

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 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

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.

The TOE provides the following security functionality: audit, cryptographic services, user data protection, identification and authentication, management, protection of the TSF, TOE access.

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed in July 2011. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 3.1 R3 [CC] Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.2 from the Common Methodology for Information Technology Security Evaluation, Version 3.1 R3, [CEM]. This Security Target claims demonstrable compliance to *US Government Wireless Local Area Network (WLAN), Access System for Basic Robustness Environments Protection Profile, July 25, 2007*.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap-ccevs.org. The Security Target (ST) is contained within the document *3eTI Wireless Network Access System Security Target*

2 Identification

Target of Evaluation:

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

Evaluated Software and Hardware:

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

Developer:	3e Technology International, Inc.
CCTL:	CygnaCom Solutions 7925 Jones Branch Dr, Suite 5400 McLean, VA 22102-3321
Evaluators:	Deepak Somesula
Validation Scheme:	National Information Assurance Partnership CCEVS
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1 R3, July 2009
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 3.1 R3, July 2009

3 Security Policy

The TOE's security policy is expressed in the security functional requirements identified in Section 6.1 of the ST. Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements.

The TOE provides the following security features:

3.1 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.

3.2 Cryptographic Services

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

3.3 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.

3.4 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.

3.5 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.

3.6 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.

3.7 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

3.8 Summary

3.8.1 SECURITY FUNCTIONAL REQUIREMENTS

A summary of the SFRs for the TOE follows. Note that _EXT in the SFR ID indicates extended requirements.

Table 3-1 : Summary of SFRs – Wireless Access Point

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)	FCS_BCM_(EXT).1 – Extended: Baseline Cryptographic Module	6
	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

Functional Class	Functional Components	#
	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
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

Table 3-2: Summary of SFRs – Security Server

Functional Class	Functional Components	#
Security Audit (FAU)	FAU_GEN.1 (SS) – Audit data generation (Security Server)	1
	FAU_GEN.2 (SS) – User identity association (Security Server)	2
	FAU_SAR.1 (SS) Audit review (Security Server)	3
	FAU_SAR.3 (SS) Selectable audit review (Security Server)	4
	FAU_SEL.1 (SS) – Selective Audit (Security Server)	5
Cryptographic Support (FCS)	FCS_BCM_(SS).1 – Extended: Security Server baseline cryptographic module	6
	FCS_CKM.1 (SS1) - Cryptographic key generation (for symmetric keys on Security Server)	7
	FCS_CKM.1 (SS2) - Cryptographic key generation (for asymmetric keys on Security Server)	8
	FCS_CKM.2 (SS) - Cryptographic key distribution (Security Server)	9
	FCS_CKM_(SS).2 - Cryptographic key handling and storage on Security Server)	10
	FCS_CKM.4 (SS) - Cryptographic key destruction (Security Server)	11
	FCS_COP.1 (SS1) – Cryptographic Operation (Data encryption/decryption on Security Server)	12
	FCS_COP.1 (SS2) – Cryptographic Operation (Digital Signature on Security Server)	13

Functional Class	Functional Components	#
	FCS_COP.1 (SS3) – Cryptographic Operation (Secure Hash on Security Server)	14
	FCS_COP.1 (SS4) - Cryptographic Operation (Key Agreement on Security Server)	15
	FCS_COP.1 (SS5) – Cryptographic Operation (HMAC on Security Server)	16
	FCS_COP_(SS).1 – Extended: Security Server random number generation	17
User Data Protection (FDP)	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
	FDP_DAU_CRL_(SS).1 Extended: Basic CRL Checking	23
	FDP_DAU_OCS_(SS).1 Extended: Basic OCSP Client	24
	FDP_ITC_SIG_(SS).1 Extended: Import of PKI Signature	25
	FDP_RIP.1 (SS) – Subset Residual Information Protection (Security Server)	26
Identification and Authentication (FIA)	FIA_AFL.1 (SS) – Authentication failure handling (Security Server Administrator)	27
	FIA_ATD.1 (SS1) – Administrator attribute definition (Security Server)	28
	FIA_ATD.1 (SS2) – User attribute definition (Security Server)	29
	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
	FIA_USB.1 (SS) –User-subject binding (Security Server Administrator)	33
Security Management (FMT)	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
	FMT_SMF.1 (SS) - Specification of Management Functions (Security Server)	37
	FMT_SMR.1 (SS) - Security roles (Security Server)	38
Protection of TSF (FPT)	FPT_TST_(SS).1 - Extended Security Server testing	39
	FPT_TST.1 (SS) - TSF testing (Security Server Cryptography	40
	FPT_TST.2 (SS) - TSF testing (Security Server Key Generation Components)	41
TOE Access	FTA_SSL.3 (SS) TSF-initiated termination (Security Server)	42
	FTA_TAB.1 (SS) Default TOE access banners (Security Server)	43
Trusted Path/Channels (FTP)	FTP_ITC_(SS).1 – Extended Security Server trusted channel	44
	FTP_TRC.1 (SS) – Trusted Path (Security Server)	45

3.8.2 OPERATIONAL ENVIRONMENT OBJECTIVES

The TOE's operating environment must satisfy the following objectives.

1. The IT Environment will provide the capability to protect audit information and the authentication credentials.
2. The IT Environment will provide the capability to selectively view audit information.
3. 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. Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.
5. There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
6. The environment provides physical security commensurate with the value of the TOE and the data it contains.
7. 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. 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. 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. 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. The environment will provide mechanisms that support the TOE in providing a user's logical access to the TOE.
12. 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 Assumptions and Clarification of Scope

4.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL 4 assurance requirements.

- AGD_OPE.1
- AGD_PRE.1
- ALC_CMC.4
- ALC_CMS.4
- ALC_DEL.1

4.2 Assumptions

TOE Secure Usage Assumptions:

- Administrators are non-hostile, appropriately trained and follow all administrator guidance.
- There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- 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 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 4 in this case).
2. This evaluation only covers the specific version of the product identified in this document, and not any earlier or later versions released or in process.
3. The following are not included in the Evaluation Scope:

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 WAN as 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.

4. The Operational Environment needs to provide the following capabilities:

- 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.

5 Architectural Information

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 5-1 and Figure 5-2 below depict the two configurations of the TOE in their Operational Environments.

Figure 5-1 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 5-1: Wireless Access Point Only TOE Configuration

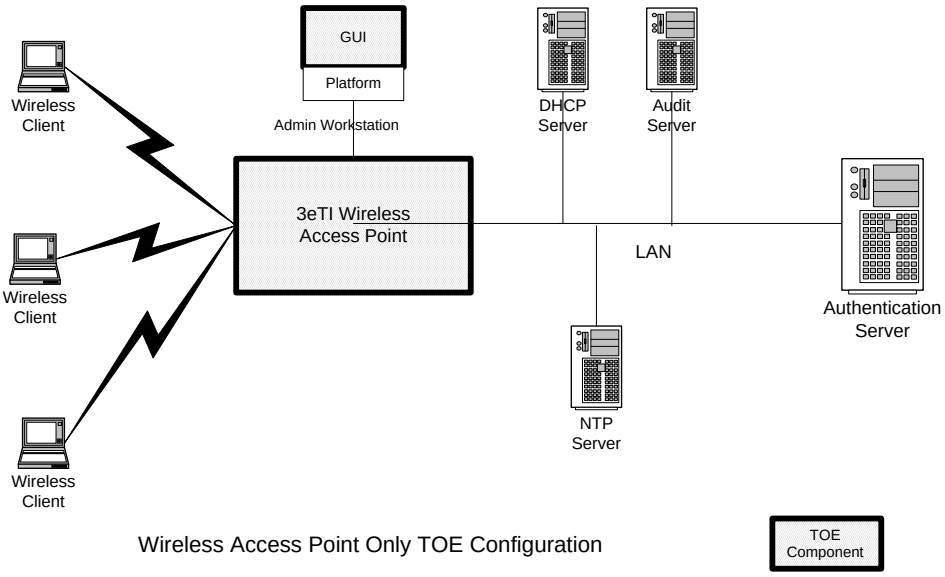
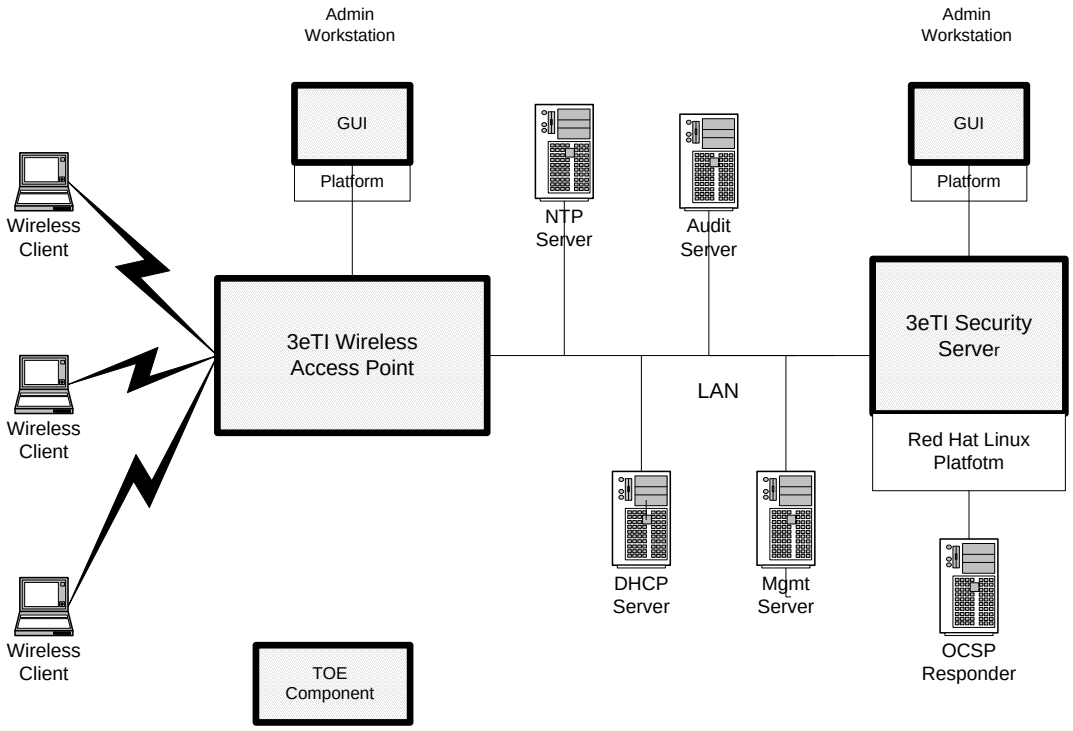


Figure 5-2 depicts a configuration of the TOE that includes the 3eTI Security Server. The 3eTI Security Server is installed on a Linux platform. The Security Server communicates with a Lightweight Directory Access Protocol (LDAP) Server to download CA certificates and Certificate Revocation Lists. If 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 5-2: TOE Configuration with 3eTI Security Server



TOE Configuration with 3eTI Security Server

The sections below describe the components of the TOE:

5.1.1 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

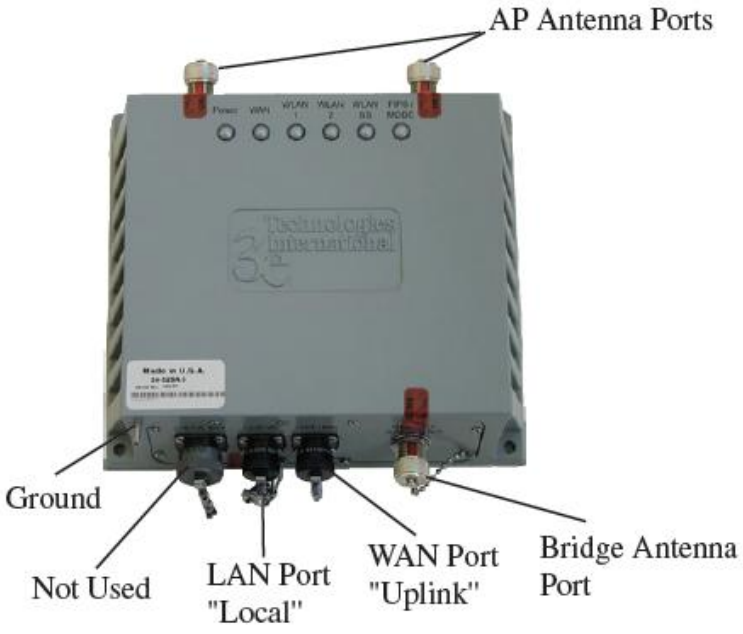
The AP software executes on the Intel XScale IPX425 network processor. On the 3e-525A3, 3e-525A-3MP, 3e-525A-3EP, 3e-525V-3, and 3e-525VE-4 AP models, the CPU is running at 533MHz mode. On the 3e-523-F2 and the 3e-523-3 appliance models, the same CPU runs at 266MHz. The platform includes an Intel IXP 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 5-3 below depicts the 3e-525A-3 Wireless Access Point as an example.

Figure 5-3: 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

5.1.1.1 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.

5.1.1.2 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.

5.1.1.3 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.

5.1.1.4 802.11 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.

5.1.1.5 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.

5.1.1.6 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

5.1.1.7 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.

5.1.1.8 Ethernet Driver

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

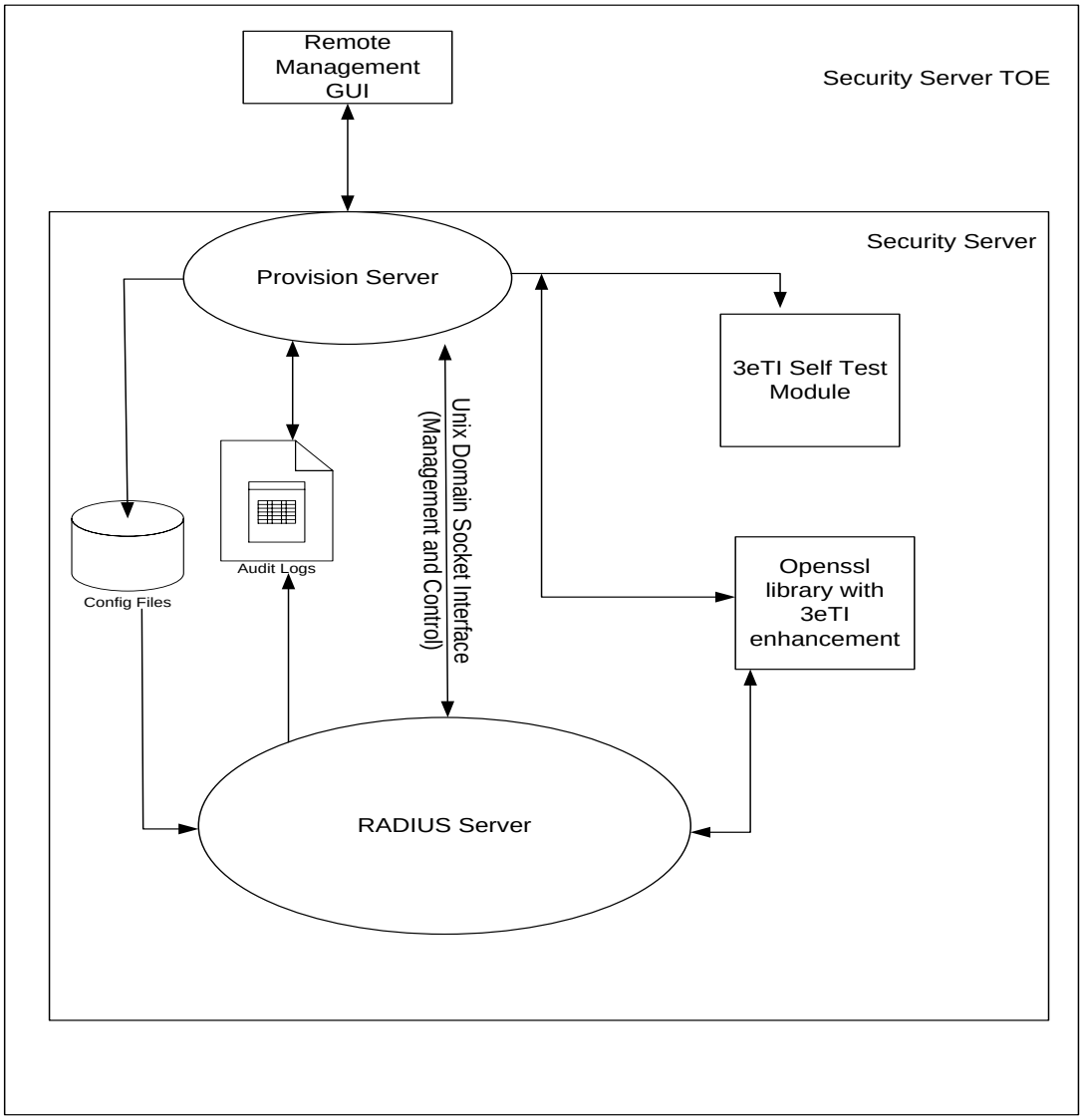
5.1.2 SECURITY SERVER TOE COMPONENT

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 5-4 below depicts the major sub-components of the Security Server.

Figure 5-4: 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

5.1.2.1 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.

5.1.2.2 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.

5.1.2.3 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

5.1.2.4 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.

5.1.2.5 Self-Test Module

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

5.1.2.6 Audit Log Files

The Audit Log Files store the CC required auditable events.

5.1.2.7 Configuration Files

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

6 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation and methodology for delivery of the evaluated configuration. In these tables, the following conventions are used:

Documentation that is delivered to the customer is shown with **bold** titles.

Documentation that was used as evidence but is not delivered is shown in a normal typeface.

The TOE is physically delivered to the End-User. The guidance is part of the TOE and is delivered in printed form and as PDFs on the installation media.

6.1 Guidance Documentation

The following documents are developed and maintained by 3eTI and delivered to the end user of the TOE:

[1] **3eTI 3e-030-2 Security Server Version 4.0 User's Guide December 2010**

[2] **3eTI AirGuard™ 3e–523–3 / 3e-523S-1 / 3e-523-F2 Wireless Data Point User's Guide**

[3] **3eTI AirGuard™ 3e–525A-3 / 3e-525A-3MP / 3e-525A-3EP / 3e-525V-3 / 3e-525Ve-4 Wireless Access Point User's Guide**

[4] **Common Criteria Supplement For 3eTI 525&523 Family Access Point**

[5] **Security Server Common Criteria Supplement**

6.2 Security Target (ST)

Security Target (ST)

[1] 3eTI Wireless Network Access System Security Target Version 2.0.

6.3 Evaluation Technical Report (ETR)

[1] Evaluation Technical Report For a Target of Evaluation, Volume 1: Evaluation of the ST, 3e Technologies International, Wireless Network Access System, Version 1.0, 2011-July-19.

7 IT Product Testing

At EAL 4, the overall purpose of the testing activity is “independently testing a subset of the TSF, whether the TOE behaves as specified in the design documentation, and to gain confidence in the developer's test results by performing a sample of the developer's tests” (ATE_IND.2, 14.6.2.1 [CEM])

At EAL 4, the developer’s test evidence must “show the correspondence between the tests provided as evaluation evidence and the functional specification. This section describes the testing efforts of the vendor and the evaluation team.

The objective of the evaluator’s independent testing sub-activity is “to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests” (ATE_IND.2, Independent testing – sample [CC]).

7.1 Developer Testing

The developer testing effort that is described in detail in the Developer Test Plan involved executing the test sets in the test configurations described in the Test Procedures documents.

7.1.1 OVERALL TEST APPROACH AND RESULTS:

3eTI testing consisted of the following types of tests:

Manual Tests:

All the developer tests were performed manually. All expected results are mentioned as part of the Developer’s test procedure description and all actual results are observations to ensure that expected results match actual results.

7.1.2 DEPTH AND COVERAGE

All developer test cases test TOE security functions by stimulating an external interface.

Although the developer tests are performed using the User Interface, the evaluator determined that the test cases as described in the test documentation adequately exercise the internal interfaces.

TOE testing directly tests external TSF interfaces. The behavior of the TSF is realized at its interfaces. Hostile intent will be expressed at the Network Asset Interface.

The evaluator ensured that the test sample included the tests such that:

- All Security Functions are tested
- All External interfaces are exercised

- All Internal interfaces are exercised
- All Security Functional Requirements are tested.
- All relevant security relevant features mentioned in the Administration/User Guides are covered in testing.

7.1.3 RESULTS

The evaluator checked the test procedures and the Test Evidence and found that the expected test results are consistent with the actual test results provided. For each test case examined, the evaluator checked the expected results in the test procedures with the actual results provided in the Test Evidence and found that the actual results were consistent with the expected results. The evaluator checked all of the test procedures.

.

7.2 Evaluator Independent Testing

The evaluator performed the following activities during independent testing:

- Execution the Developer's Functional Tests (ATE_IND.2)
- Team-Defined Functional Testing (ATE_IND.2)
- Vulnerability/Penetration Testing (AVA_VAN.3)

7.2.1 EXECUTION THE DEVELOPER'S FUNCTIONAL TESTS

The evaluator selected to rerun 40% of the developer's tests:

- as a means of ensuring the coverage of the security features,
- as a means to gain confidence in the developer's test results, and
- a quick means of ensuring TOE is in a properly configured state

The developer's test cases were executed only after the TOE was installed in the evaluated configuration that is consistent with the Security Target (Section 1). The evaluator confirmed that the test configuration was consistent with the evaluated configuration in the Security Target.

The test configurations used by the evaluator were the same as that used by the developer.

The test results and screenshots for the test cases were recorded during the Evaluator testing. Overall success of the testing was measured by 100% of the retests being consistent with expected results. Anomalies were documented along with suggested / required solutions.

All of the Developer's Functional Tests rerun by the Evaluator received a 'Pass' verdict.

7.2.2 TEAM-DEFINED FUNCTIONAL TESTING

The Evaluator selected individual test procedures from the set of Developer Functional Tests, and modified the input parameters to ensure fuller coverage of security functions and correctness of developer reported results (ensuring that the results were not canned).

Additional tests were developed for the purpose of verifying that the product operates in accordance with Vendor claims, i.e. that a bug is fixed or a capability operates as described in the product documentation.

The test results and screenshots for the test cases were recorded during the Evaluator testing. Overall success of the testing was measured by 100% of the tests being consistent with expected results. Anomalies were documented along with suggested / required solutions.

The Evaluator developed additional tests listed in the Evaluator Test Plan & Report.

All of the Team-Defined Tests received a ‘Pass’ verdict.

8 Results of Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon version 3.1 R3 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL.

Below lists the assurance requirements the TOE was required meet to be evaluated and pass at Evaluation Assurance Level 4 augmented with ALC_FLR.2. The following components are taken from CC part 3. The components in the following section have no dependencies unless otherwise noted.

- ADV_ARC.1 Security architecture description
- ADV_FSP.4 Complete functional specification
- ADV_IMP.1 Implementation Representation of the TSF
- ADV_TDS.3 Basic modular design
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- 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_LCD.1 Developer defined life-cycle model
- ALC_TAT.1 Well-defined development tools
- ALC_FLR.2 Flaw reporting procedures
- ASE_CCL.1 Conformance claims
- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST Introduction
- ASE_OBJ.2 Security objectives
- ASE_REQ.2 Derived security requirements

- ASE_SPD.1 Security problem definition
- ASE_TSS.1 TOE summary specification
- ATE_COV.2 Analysis of coverage
- ATE_FUN.1 Functional testing
- ATE_IND.2 Independent testing – sample
- AVA_VAN.3 Focused Vulnerability analysis

The evaluators concluded that the overall evaluation result for the target of evaluation is Pass. The evaluation team reached PASS verdicts for all applicable evaluator action elements and consequently all applicable assurance components.

- The TOE is CC Part 2 Extended
- The TOE is CC Part 3 Conformant.
- The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.

9 Validators Comments/Recommendations

The validators have no comments or specific recommendations.

10 Security Target

3eTI Wireless Network Access System Security Target is compliant with the Specification of Security Targets requirements found within Annex B of Part 1 of the CC.