National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

3eTI AirGuard Wireless Network Access System

Report Number: **CCEVS-VR-VID10689**
Dated: **October 13, 2015**
Version: **1.0**

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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Mr. Daniel Faigin

The Aerospace Corporation

Los Angeles, CA

Mr. Luke A Florer

The Aerospace Corporation

Chantilly, VA

Common Criteria Testing Laboratory

Ms. Nandini Pathmanathan

CygnaCom Solutions

McLean, Virginia

Much of the material in this report was extracted from evaluation material prepared by the CCTL. The CCTL team deserves credit for their hard work in developing that material. Many of the product descriptions in this report were extracted from the 3eTI-525/523 Series Wireless Network Access Points Security Target.

Table of Contents

List of Figures and Tables

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the 3eTI *3e-525* and *3e-523* Series Wireless Network Access System as defined in the 3-*e525/523 Series Wireless Network Access Points Security Target, v1.0* (ST). This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST. It presents the evaluation results, their justifications, and the conformance results.

The 3e-523/525 devices share the hardware platform and firmware. Differences between models are limited to enclosure, power options, and Wi-Fi radio interfaces. All models provide the same functionality of wireless endpoint access control.

The Target of Evaluation (TOE) is a Wireless Local Area Network (WLAN) Access Device as defined by the *U.S. Government Protection Profile for Wireless Local Area Network (WLAN) Access Systems, December 01, 2011*.

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed in September 2015. 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 R4 Part 2 extended and Part 3 conformant.
- Demonstrates exact compliance to *U.S. Government Protection Profile for Wireless Local Area Network (WLAN) Access Systems, December 01, 2011*as changed/clarified by *all applicable Technical Decisions*.

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.

2. Identification

Target of Evaluation: 3eTI AirGuard Wireless Network Access System.

The TOE consists of the following products:

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

ST Title: *3eTI AirGuard Wireless Network Access System Security Target, v1.0, Revision I*

Developer:	3e Technologies International
CCTL:	CygnaCom Solutions 7925 Jones Branch Dr, Suite 5400 McLean, VA 22102-3321
Evaluators:	Nandini Pathmanathan Herb Markle
Validation Scheme:	National Information Assurance Partnership CCEVS
Validators:	Daniel Faigin, Luke Florer
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1 R4, Sept 2012
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 3.1 R4, Sept 2012
PP Identification:	U.S. Government Protection Profile for Wireless Local Area Network (WLAN) Access Systems, December 01, 2011

3. Security Policy

The Target of Evaluation (TOE) enforces the following security policies as described in the ST:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Resource Utilization
- TOE Access
- Trusted Path/Channel

3.1. Security Audit

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

3.2. Cryptographic Support

The TOE uses certified cryptographic algorithms operating in the FIPS mode to perform all cryptographic operation. These cryptographic algorithms implements all cryptographic primitives as validated by the CAVP program. This includes DRBG random number generator seeded by the hardware-based noise source (#882), AES for encryption and decryption (#2060, 2078, 2105), RSA (#1072, 1278, 1491) and ECDSA signature generation and verification (#303, 415), SHA for hashing (#1801, 1807), HMAC for keyed-hash authentication (#1253, 1259). The TOE also uses its designed mechanism to zeroize Critical Security Parameters (CSPs) to mitigate the possibility of disclosure or modification. This cryptographic functionality is utilized by an RFC-compliant IPSec and TLS protocols, and as part of X.509 certificates.

3.3.User Data Protection

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

3.4.Identification and Authentication

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

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

3.5.Security Management

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

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

3.6.Protection of the TSF

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

The TOE runs a set of self-test on power-on to verify the correct operation of the TOE’s underlying hardware, TOE software and cryptographic modules. Additional

cryptographic tests are performed during normal operation. The security of network data is maintained by ensuring no residual information is included in network packets.

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

3.7. Resource Utilization

The TOE enforces maximum quotas for simultaneous wireless connections and simultaneous management connections.

3.8. TOE Access

The TOE provides the following TOE Access functionality:

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

3.9. Trusted Path/Channels

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

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

4. Assumptions and Clarification of Scope

4.1. Secure Usage Assumptions

The ST identifies the following assumptions about the use of the product:

1. It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
2. Information cannot flow between the wireless client and the internal network without passing through the TOE.
3. Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment. It is assumed the TOE hardware and software critical to security policy enforcement will be adequately protected from unauthorized physical modification.
4. TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4.2. Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

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

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:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Protection Profile for Wireless Local Area Network (WLAN) Access Systems, December 01, 2011, to which this evaluation claimed exact compliance.
- Consistent with the expectations of the Protection Profiles, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed ST. Any additional security related functional capabilities included in the product were not covered by this evaluation.
- Specifically, the evaluation excluded following functionality:
    - IEEE 802.11s mesh networking (AP to AP communication service);
    - Tampering protection, as it is covered by assumptions;
    - Serial Port and Modbus functionality, since it requires optional hardware add-on (Section 2.6.4 Serial Communication, Figure 64: Services Settings – Serial Communication – Raw Socket of the user's guide detail on how to disable this port). In the evaluated configuration, the TOE does not implement local serial interface therefore this functionality was not tested.

The evaluated configuration of the TOE includes the 3eTI *3e-525* and *3e-523* Series Wireless Network Access System, with firmware version 5.1, that is comprised of one or more of the product models. The TOE includes all the code that enforces the policies identified.

The Non-FIPS 140-2 mode of operation is excluded from the evaluation. This mode will be disabled by configuration. The exclusion of this functionality does not affect compliance to the Protection Profile for Wireless Local Area Network (WLAN) Access Systems.

5. Architectural Information

5.1. TOE Components

The TOE provides the connection point between wireless client hosts and the wired network. Once installed as trusted node on the wired infrastructure, the TOEs provide the encryption service on the wireless network between itself and the wireless clients.

The TOE is an appliance and consists of hardware and firmware.

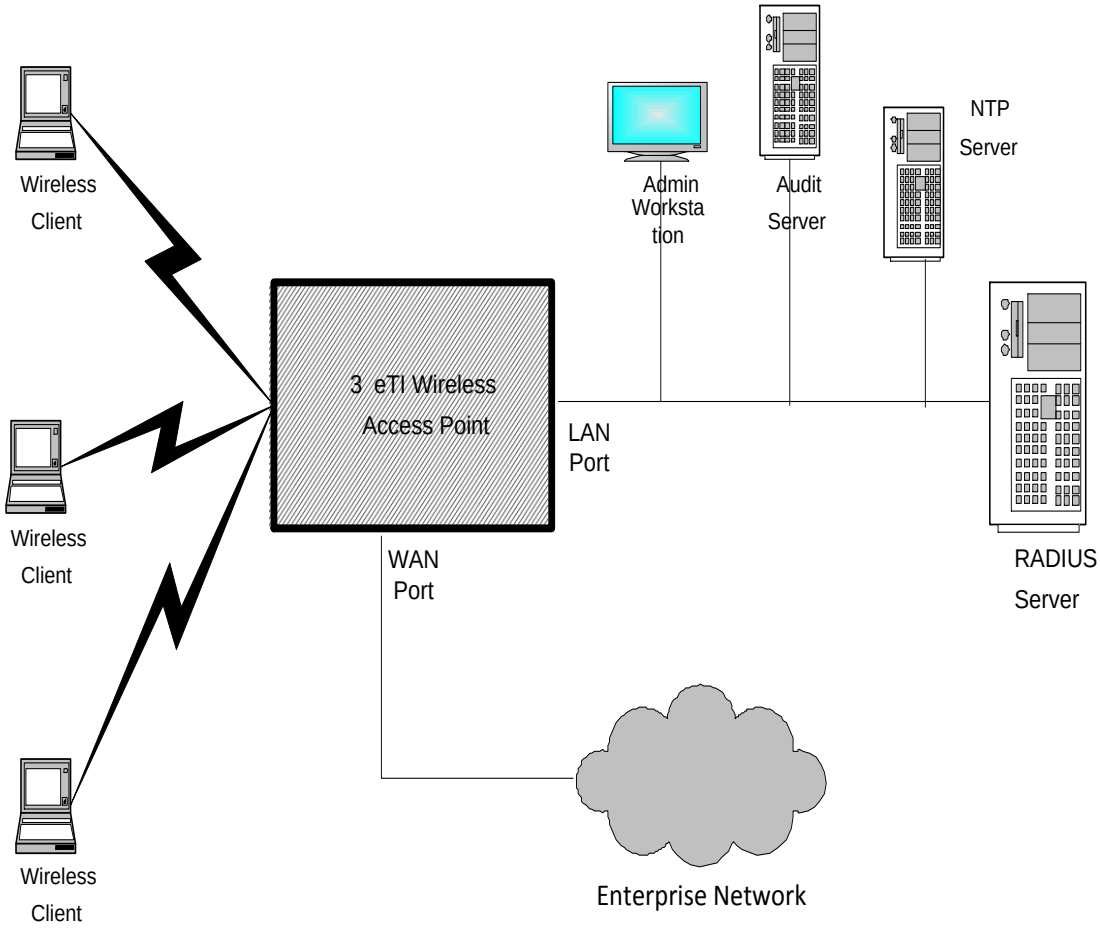
Wireless communication between clients and the TOE is carried out using the IEEE 802.11 protocol standard. The 802.11 standard governs communication transmission for wireless devices. In the evaluated configuration, the TOE supports 802.11a, 802.11b, 802.11g, and 802.11n wireless protocols. The TOE utilizes WPA2 wireless security protocol, which is the Wi-Fi Alliance interoperable specification based on IEEE 802.11i security standard.

Each TOE model has one or more radio frequency (RF) interfaces and one or more Ethernet interfaces. All these interfaces are controlled by the software executing on the TOE.

The TOE maintains a security domain containing all hardware, firmware, and software. This security domain is maintained by controlling the actions that can occur at the interfaces described above and providing the hardware resources that carry out the execution of tasks. The TOE ensures isolation of different wireless clients that have sessions with the WLAN, which includes maintaining critical security parameters (CSP) necessary to support secure sessions with wireless devices.

The TOE controls the actions and the manner in which external users may interact with its interfaces. This way the TOE can ensure the enforcement of the security functionality when interfacing with the external users. The figure below shows the TOE and its operational environment. The trusted path between TOE and Administration Station is TLS/HTTPS and the trusted path between TOE and NTP, Log Server and RADIUS server is IPsec.

Figure 1-1: TOE Operational Environment



Wireless Access Point Operational Enviroment

5.2. Physical Scope of the TOE

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

The TOE implements the following physical interfaces.

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

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

- External audit storage (Syslog) server
- Reliable time stamps from a Network Time Protocol (NTP) server
- Centralized Authentication, Authorization, and Accounting management (RADIUS) server

6. Documentation

The following documents were available for the evaluation. These documents are developed and maintained by 3eTI and delivered to the end user of the TOE:

6.1. User Documentation

Reference Title
3eTI AirGuard User's Guide, Revision G, 29010012-001, 21 September 2015

7. Product Testing

This section describes the testing efforts of the Evaluation Team. The information is derived from the *Evaluator Test Report for 3e-TI AirGuard Wireless Network Access System*. The purpose of this activity was to confirm that the TOE behaves in accordance with security functional requirements specified in the ST.

7.1. Developer Testing

WLANPP evaluations do not require developer testing evidence for assurance activities.

7.2. Evaluator Independent Testing

A test plan was developed in accordance with the Testing Assurance Activities specified in the WLAN PP.

Testing was conducted Testing was conducted July 6th-9th, 2015 at the 9715 Key West Avenue, Suite 500, Rockville, Maryland, USA, 20850.

The Evaluator successfully performed the following activities during independent testing:

- Placed TOE into evaluated configuration by executing the preparative procedures
- Successfully executed the WLAN PP Assurance-defined tests including the optional TLS tests
- Planned and executed a series of vulnerability/penetration tests

It was determined after examining the Test Report and full set of test results provided by the evaluators the testing requirements for WLAN PP are fulfilled.

8. Results of Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*.

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 R4 of the CC and the CEM. Additionally the evaluators performed the assurance activities specified in the *Wireless Local Area Network (WLAN) Access System Protection Profile, Version 1.0,* dated December 1, 2011.

The evaluation determined the TOE meets the SARs contained the PP.

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

Below lists the assurance requirements the TOE was required to be evaluated against. All assurance activities and work units received a passing verdict. The following components are taken from CC part 3:

- ADV_FSP.1 Basic functional specification
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ALC_CMC.1 Labelling of the TOE
- ALC_CMS.1 TOE CM coverage
- ASE_CCL.1 Conformance claims
- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST Introduction
- ASE_OBJ.1 Security objectives
- ASE_REQ.1 Derived security requirements
- ASE_TSS.1 TOE summary specification
- ATE_IND.1 Independent testing – conformance
- AVA_VAN.1 Vulnerability survey

The evaluators concluded that the overall evaluation result for the target of evaluation is PASS. 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

Please note that Wi-Fi compliance was not explicitly tested. Instead, the vendor affirmation of standards-based implementation supported by Wi-Fi Alliance certification was accepted.

As was noted in the Clarification of Scope section of this report, the devices provide more functionality than was covered by the evaluation. Only the functionality claimed in the SFR's in the Security Target was evaluated. All other functionality provided by the devices needs to be assessed separately and no further conclusions should be drawn as to their effectiveness, nor can any claims be made relative to their security based upon this evaluation.

10. Glossary

10.1. Acronyms

The following are product specific and CC specific acronyms. Not all of these acronyms are used in this document.

BGP	Border Gateway Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	HyperText Transmission Protocol
HTTPS	HyperText Transmission Protocol, Secure
IP	Internet Protocol
IPS	Intrusion Protection System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OSPFv2	Open Shortest Path First
PDF	Portable Document Format
RADIUS	Remote Authentication Dial-In User Service
RIP	Routing Information Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer,
ST	Security Target
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security,
UDP	User Datagram Protocol
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network

11. Bibliography

URLs

[1] Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).

[2] CygnaCom Solutions CCTL (http://www.cygnacom.com).

CCEVS Documents

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, July 2009 Version 3.1 Revision 4 Final, CCMB-2012-09-001.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, July 2009 Version 3.1 Revision 4 Final, CCMB-2012-09-002.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, July 2009, Version 3.1 Revision 4 Final, CCMB-2012-09-003.

[4] Common Methodology for Information Technology Security Evaluation - Evaluation methodology, July 2009, Version 3.1 Revision 4 Final, CCMB-2012-09-004.

Lab Documents

[1] Assurance Activity Report for 3eTI AirGuard Wireless Network Access System conforming to the Protection Profile for Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 8 October 2015.

[2] Evaluation Technical Report for 3eTI AirGuard Wireless Network Access System Volume 1: Evaluation of the ST, Version 1.1, 8 October 2015.

[3] Evaluation Technical Report for 3eTI AirGuard Wireless Network Access System Volume 2: Evaluation of the TOE, Version 1.1, 8 October 2015.

Vendor Documents

[1] 3eTI AirGuard Wireless Network Access System Security Target, Revision I, 8 October 2015.

[2] 3eTI AirGuard User's Guide, Revision G, 29010012-001, 21 September 2015.