National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

3e Technologies International
3e-525A-3 Access System

Report Number: CCEVS-VR-06-0045
Evaluation: VID 3031
Dated: 14 September 2006
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 6740
Fort George G. Meade, MD 20755-6740

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY 1
2 IDENTIFICATION 3
3 SECURITY POLICY 3
4 ASSUMPTIONS AND CLARIFICATION OF SCOPE 6
4.1 USAGE ASSUMPTIONS 6
4.2 ENVIRONMENTAL ASSUMPTIONS 6
5 ARCHITECTURAL INFORMATION 6
6 DOCUMENTATION 7
7 IT PRODUCT TESTING 8
7.1 DEVELOPER TESTING 8
7.2 EVALUATOR INDEPENDENT TESTING 9
7.3 STRENGTH OF FUNCTION 9
7.4 VULNERABILITY ANALYSIS 10
8 EVALUATED CONFIGURATION 10
9 RESULTS OF THE EVALUATION 10
10 VALIDATOR COMMENTS/RECOMMENDATIONS 11
11 SECURITY TARGET 12
12 GLOSSARY 13
13 BIBLIOGRAPHY 14

1 Executive Summary

This report documents the NIAP validator's assessment of the evaluation of the 3e Technologies International 3e-525A-3 Access System, a product of 3e Technologies International, Inc., 700 King Farm Boulevard, Suite 600, Rockville, MD 20850. It presents the evaluation results, their justifications, and the conformance results. This validation report 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 evaluation was performed by the CygnaCom Solutions Security Evaluation Laboratory (CCTL), and was completed during September 2006. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by CygnaCom Solutions. The evaluation determined that the product is both **Common Criteria Part 2 extended and Part 3 conformant**, and meets the assurance requirements of EAL 2 augmented with, ACM_SCP.1 (TOE CM Coverage), ALC_FLR.2 (Flaw Remediation), ACM_CAP.3 (Authorization Controls), and AVA_MSU.1 (Misuse – Examination of Guidance). The product is not conformant with any published Protection Profiles, but rather is targeted to satisfying specific organizational security policies while countering specific threats.

3e Technologies International 3e-525A-3 Access System (hereafter 3eTI Server System) is a secure wireless access system application designed to be used with another product for a wireless client that is the subject of a separate evaluation. The Target of Evaluation (TOE) was evaluated using the *Common Criteria for Information Technology Security Evaluation*, Version 2.3, August 2005 [CCV2.3], and the *Common Methodology for Information Technology Security Evaluation*, Version 2.3, Evaluation Methodology, August 2005 [CEMV2.3]. The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) best practices as described within CCEVS Publication #3 [CCEVS3] and Publication #4 [CCEVS4]. The Security Target (ST) for the 3eTI Server System is contained within the document 3e Technologies International 3e-525A-3 Access System Security Target, 22000201-701, Revision S, dated August 2006 [ST]. The ST has been shown to be compliant with the *Specification of Security Targets* requirements found within Annex B of Part 1 of [CCV2.3].

The Target of Evaluation (TOE) is a wireless LAN access system. The 3e-525A-3 Access System is a ruggedized access point intended for use in industrial and external environments. The TOE provides a secure, yet flexible, WLAN environment through the use of FIPS-validated components (evaluated separately by a FIPS certified laboratory) and support for industry standards:

- 3e WAP hardware device that accommodates 802.11a/b/g WLAN access and uses Power over Ethernet (PoE) access to the Ethernet WAN to eliminate the need for internal access point power supply units (AC-DC converters) and 110-220V cabling installations. The wireless LANs can include any mobile devices such as handheld Personal Data Assistants (PDAs), mobile web pads, and wireless laptops which support the 802.11a/b/g standards for wireless networking.

- The 3e-SS is a RADIUS-based server which provides EAP-TLS authentication of the clients connecting to the WLAN, ensuring only authorized connections are allowed. The Server is installed within the environment and connected to the 3e-WAP through the uplink port, allowing it to provide the authentication services for the mobile clients.
- The access system is a fully functional WLAN platform with augmented security functionality. While the system can provide standard 802.11a/b/g wireless access, the system can provide enhanced protection through a variety of cryptographic features, providing a high level of security for wireless environments. The 3e-WAP contains FIPS 140-2 Validated Level 2 secure encryption modules, with EAP-TLS provided by the 3e-SS software using the DKE Key exchange method when used in conjunction with 3e-010F clients. The 3e-WAP also includes 802.11i support. This product is expected to be used in conjunction with the LAN client comprised of either the 3e-010F-C-2 or 3e-010F-A-2 Crypto Client Software. The difference between the clients is in the drivers related to the supported hardware. The companion product is the subject of a separate evaluation.

Aspects of the following security functions are controlled / provided by the TOE in conjunction with the IT environment:

- Object access control
- Encryption Services and key management and exchange.
- Role-based user privileges
- Audit

The following are explicitly excluded from the TOE configuration, but are included in its environment:

- Client software (subject of a separate evaluation)
- Hardware platforms and Operating Systems for the Security Systems
- Network hardware and software (e.g., firewalls and routers)

The environment is assumed to counter the threats of unauthorized access to the physical components of the TOE. The TOE will properly authenticate users and protect crypto keys and information in transit between the LAN and the client.

All copyrights and trademarks are acknowledged.

2 Identification

TOE Identification: **3eTI 3e-525A-3 Access System**.
The TOE contains:
3e-525A-3 Hardware Version 1.0, Software Version 4.0.9.11.
3e-030-2 Software Version 3.0.7

Evaluation Assurance Level (EAL): Evaluation Assurance Level (EAL) 2 augmented with, ACM_SCP.1 (TOE CM Coverage), ALC_FLR.2 (Flaw Remediation), ACM_CAP.3 (Authorization Controls), and AVA_MSU.1 (Misuse – Examination of Guidance).

Strength of Function: SOF-Basic

Common Criteria Identification: Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005. International Standard – ISO/IEC 15408:2004.

CCTL: Cygnacom Solutions' Security Evaluation Laboratory
Suite 5200
4925 Jones Branch Drive
McLean, VA 22102-3305

Validation Team: William R. Simpson (Institute for Defense Analyses)

CC Identification: *Common Criteria for Information Technology Security Evaluation*, Version 2.3, August 2005 [CCV2.3].

CEM Identification: *Common Methodology for Information Technology Security Evaluation*, Version 2.3, Evaluation Methodology, August 2005 [CEMV2.3].

Interpretations: All NIAP and CCIMB interpretations as of the date of the Kick-off meeting held on 13 October 2005 were considered during the evaluation (all CCIMB interpretations issued prior to January 2004 had been incorporated into the version of the CC that was used). Specific interpretations identified as NIAP-0407, NIAP-0409, NIAP-0410, NIAP-0415 and NIAP-0425 had a direct impact on the work performed.

3 Security Policy

The 3eTI 3e-525A-3 Access System security policy is reflected in the security functional requirements for the TOE described in section 5 and 6 of the ST. A description of the principle security policies is as follows:

- **Audit.** The access system generates auditable events for actions on the 3e-WAP and the 3e-SS. These events can be viewed within the 3e-WAP Management Interface or they can be exported to audit systems within the IT environment. The 3e-WAP and the 3e-SS each generate separate records for their own actions, though each contain information

about the user/process associated with the event, result of the event and when the event occurred.

- **Encryption.** This access system includes cryptographic modules which have been evaluated against applicable Federal Information Processing Standard Publication (FIPS PUB) standards. The entire product has been evaluated against FIPS 140-2, which defines security requirements for cryptographic modules, while the 3DES and AES encryption algorithms have been evaluated against FIPS 46-3 and FIPS 197, respectively. All cryptographic operations of the access system use these evaluated modules/algorithms to ensure the security of all data passed through the 3e-WAP.

- **Identification and Authentication.** The access system requires that administrators be properly identified and authenticated prior to performing any administrative tasks on the system. Furthermore, multiple authentication mechanisms are provided for access to wireless services provided by the access system. The type of authentication mechanism invoked depends on the origin of the source (i.e., remote user from the wireless environment, remote administrative user or Crypto-Officer from the wired environment, or administrative user or Crypto-Officer from a local console) requesting the service. The authentication of a user or client computer will be based on a set of authentication credentials assigned to each user or client computer.

- **Management.** The access system provides a web-based interface to manage the configuration of the access point and an application interface to manage the cryptographic credentials stored in the Security Server. The management includes all security settings of the access point, controlling the types of communications which will be allowed to connect via the WLAN as well as the clients which will be allowed to connect.

- **Information Flow Control.** The access system enforces information flow by requiring the establishment of an encrypted communications channel between components of the system. The access system may further restrict potential information flows by granting or denying access to the network based upon authentication by a remote server. The 3e-WAP and 3e-SS require a secure communication channel.

- **Protection of the TSF.** The access system protects the TSF by ensuring that no access is granted to TOE functions without authorization. Internal testing of the TOE hardware and software ensures that all security functions are running and available before the access system will accept any communications.

The security functional requirements for the TOE and the IT environment are documented in section 7 of the ST. A combination of requirements drawn from part 2 of the CC [CCV2.3] as modified by NIAP Interpretations, with iteration and explicitly stated security requirements were necessary to define TOE functionality. A summary of the SFRs for the TOE and environment are included below.

TOE Security Functional Requirements

Functional Class	Functional Components
Security Audit (FAU)	FAU_GEN.1-NIAP-0410 - Audit data generation
	FAU_GEN.2-NIAP-0410 - User identity association
	FAU_SAR.1 Audit review
	FAU_SAR.2 Restricted audit review
	FAU_SAR.3 Selectable audit review
	FAU_SEL.1-NIAP-0407 - Selective audit
Cryptographic Support (FCS)	FCS_BCM_EXP.1 - Baseline Cryptographic Module
	FCS_CKM.1 - Cryptographic key generation
	FCS_CKM_EXP.2 - Cryptographic key establishment
	FCS_CKM.4 - Cryptographic key destruction
	FCS_COP_EXP.1 - Random Number Generation
	FCS_COP_EXP.2 - Cryptographic operation
User Data Protection (FDP)	FDP_IFC.1 (1) - Subset information flow control (Specified Users Policy)
	FDP_IFC.1 (2) - Subset information flow control (Wireless Encryption Policy)
	FDP_IFF.1-NIAP-0407 (1) - Simple security attributes (Specified Users SFP)
	FDP_IFF.1-NIAP-0407 (2) - Simple security attributes (Wireless Encryption SFP)
	FDP_ITT.1 Basic internal transfer protection
	FDP_RIP.1 (1) - Subset residual information protection
Identification and Authentication (FIA)	FIA_AFL.1-NIAP-0425 - Administrator Authentication failure handling
	FIA_ATD.1 - User attribute definition
	FIA_UAU.1 - Timing of authentication
	FIA_UID.1 - Timing of identification
	FIA_USB.1-NIAP-0415 - User-subject binding
Security Management (FMT)	FMT_MOF.1 (1) - Management of security functions behavior (Cryptographic Function)
	FMT_MOF.1 (2) - Management of security functions behavior (Audit Record Generation)
	FMT_MSA.1 - Management of security attributes
	FMT_MSA.2 - Secure security attributes
	FMT_MSA.3-NIAP-0409 - Static attribute initialization
	FMT_MTD.1 (1) - Management of TSF Data
	FMT_MTD.1 (2) - Management of TSF Data
	FMT_MTD.1 (3) - Management of TSF Data
	FMT_REV.1 - Revocation
	FMT_SMF.1 (1) - Specification of Management Functions (Cryptographic Function)
	FMT_SMF.1 (2) - Specification of Management Functions (TOE Audit Record Generation)
	FMT_SMF.1 (3) - Specification of Management Functions (Authorized WLAN User List)
	FMT_SMF.1 (4) - Specification of Management Functions (Cryptographic Key Data)
	FMT_SMR.1 (1) - Security roles
Protection of TSF (FPT)	FPT_RVM.1 - Non-bypassability of the TSP
	FPT_SEP.1 - TSF domain separation
	FPT_TST_EXP.1 - TSF testing
	FPT_TST_EXP.2 - TSF testing of Cryptographic Modules
TOE Access (FTA)	FTA_SSL.3 - TSF-initiated termination
	FTA_TAB.1 - Default TOE access banners

IT Environment Security Functional Requirements

Functional Class	Functional Components
Protection of TSF (FPT)	FPT_STM.1 - Reliable time stamps

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 EAL2 assurance requirements:

ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance

4.2 Environmental Assumptions

The environmental assumptions listed in the following table are required to ensure the security of the TOE.

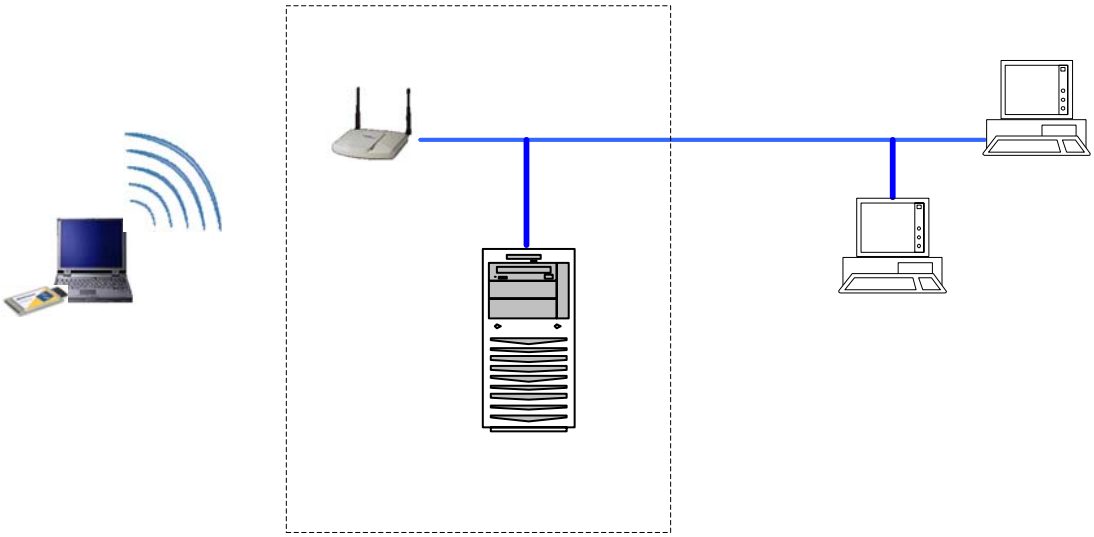
Environmental Assumptions

Name	Assumption Definition
A.NO_EVIL	Authorized Administrators, including Crypto-Officers, are non-hostile, appropriately trained, and shall follow and abide by the instructions provided by TOE guidance documentation.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment, in addition to the physical security provided by the enclosure of the TOE itself. The physical environment shall provide reliable power and air conditioning controls to insure reliable operation of the hardware.
A.HARDWARE	The software portion of TOE (3e-SS) shall be installed in a hardware system that is running Windows 2000 Server or Windows 2003 Server with a network interface card installed.

5 Architectural Information

The Target of Evaluation (TOE) is a wireless LAN access system. The 3e-525A-3 Access System is a ruggedized access point intended for use in industrial and external environments. The TOE provides a secure, yet flexible, WLAN environment comprised of two components: (a) the 3e-525A-3 Wireless Access Point (3e-WAP), and (b) the 3e-030-2 Security Server. (3e-SS). The figure below shows the concept of the TOE platform with Wireless Access Point and Security Server components.

TOE Platform



The 3e-WAP accommodates 802.11a/b/g WLAN access and uses Power over Ethernet (PoE) access to the Ethernet WAN to eliminate the need for internal access point power supply units (AC-DC converters) and 110-220V cabling installations. The wireless LANs can include any mobile devices such as handheld Personal Data Assistants (PDAs), mobile web pads, and wireless laptops which support the 802.11a/b/g standards for wireless networking.

The 3e-SS is a RADIUS-based server which provides EAP-TLS authentication of the clients connecting to the WLAN, ensuring only authorized connections are allowed. The Server is installed within the environment and connected to the 3e-WAP through the uplink port, allowing it to provide the authentication services for the mobile clients.

6 Documentation

The following is a list of the end-user documentation that was used to support this evaluation:

- [User Guide AP] Manual, 3e-525A-3 User's Guide, Version 4.0.9.11, 29000167-001, Revision D, July 27 2006
- [User Guide SS] Manual, 3e-030-2 Security Server User's Guide, Version 3.0.7 29000166-001, Revision A, July 25 2006
- [User Guide Erratta Sheet] Errata Sheet, 3e-525A-3 User's Guide, 29000167-100, Revision A
- Errata Sheet, 3e-030-2 Security Server User's Guide, 29000187-100 Revision A
- [CI] 3e-525A-3 Access System Common Criteria Configuration Items List, 22000201-700, August, 2006, Revision D

Wireless Client

- [CM-DC] Product-Related Document Control Procedure, 0000121-001 Revision A, SOP-121 Product-Related Document Control Procedure
- [DEL] Product Delivery Procedure, 00000310-001, Revision A, July, 2006
- [FLR] Defect Management System Procedure, 00000106-001, Revision A, August, 2006

7 IT Product Testing

7.1 Developer Testing

The vendor testing covered all of the security functions identified in Section 7 of the ST. These security functions were: Security Audit, Managed User Access, and Security Management. At EAL2, vendor testing must demonstrate correspondence between the tests and the functional specification. However complete testing is not required; "coverage analysis need not demonstrate that all security functions have been tested, or that all external interfaces to the TOE Security Function (TSF) have been tested."[1]

The testing was focused on demonstrating that the SFRs worked as claimed in the ST. The test procedures consisted mainly of automated scripts, with a few manual tests to test administrator operations entered through the Administrator component. For the automated scripts, the output from the script was stored in a file and then compared with the expected results file. For the manual tests, a screen shot showing the results was saved.

The testing showed that the proper audit records were generated accurately and unambiguously and contained the required information that authorized administrators could access the audit records, and that unauthorized users could not. It also tested both authorized and unauthorized accesses to the stored content.

The evaluator determined that the vendor tested (at a high level) all of the security-relevant aspects of the product that were claimed in the ST. The evaluator determined that the developer's tests were sound in their approach. The test document provided the configuration of the test hardware and software, the objective for each of the tests, and test procedures. The information provided was adequate to be able to reproduce the tests. The evaluators determined that the developer's approach to testing the TSFs was appropriate for this EAL2 augmented evaluation.

The vendor tests were conducted in conjunction with the companion client product (cryptographic WLAN client comprised of either the 3e-010F-C-2 or 3e-010F-A-2 Crypto Client Software (evaluated separately by a FIPS certified laboratory and by the evaluator under Common Criteria)). The lab repeated the entire vendor test set which covered audit features, Identification and Authentication features, potential misuse and data protection. It also covered, to a limited extent the flow control by testing expired certificates, access to logs, and other events that should restrict information flow. The lab was able to verify the results of the vendor testing of the product.

[1] CEM, V2.3, paragraph 6.8.2.2 (application note for EAL2:ATE_COV.1)

7.2 Evaluator Independent Testing

At EAL 2, the stated purpose of the evaluator's independent testing activity "is to determine, by independently testing a subset of the TSF, whether the TOE behaves as specified, and to gain confidence in the developer's test results by performing a sample of the developer's tests." ([CEM V2.3] 12.8.4.1). The CEM further instructs the evaluator to consider a number of factors including: the "Rigour of developer testing of the security functions. Some security functions identified in the functional specification may have had little or no developer test evidence attributed to them." (([CEM V2.3] 12.8.4.4 paragraph 816) As a result, the testing at EAL 2 may not be systematic and the end-users should not assume that all claims in the ST have been explicitly verified by either the developer or the evaluators.

The testing was performed in a dedicated laboratory at the 3eTi building in Rockville, MD. All machines in the laboratory are used solely for Common Criteria Testing of 3eTi's products. The lab is kept locked when not in use for functional and independent Common Criteria testing. The evaluation team installed the TOE as specified in the secure installation procedures. The same test equipment that was used for developer testing was used for the independent testing.
The evaluator reran all of the developer tests. All of the results duplicated those of the developer. The evaluator also devised twelve tests, each of which covered multiple security functionalities. Tests were devised to establish various types of encryption with valid and revoked certificates. Both positive and negative tests were devised. A coverage analysis was provided to insure that each of the security functions was exercised. Each of these tests produced the expected results.

Test results, which are contained in proprietary reports, were satisfactory to both the Evaluation Team and the Validation Team.

The independent tests were conducted in conjunction with the companion client product (cryptographic WLAN client comprised of either the 3e-010F-C-2 or 3e-010F-A-2 Crypto Client Software (evaluated separately by a FIPS certified laboratory and by the evaluator under Common Criteria)). The lab tested the product functionality which covered the administrative and user guidance for safe configuration, audit features, Identification and Authentication features, cryptographic transmission to the extent that data were observed by sniffer and found to be "not transmitted in the clear" (the actual algorithm was certified by FIPS-140 testing and was not part of this evaluation). The testing covered misuse and data protection through a combination of the user interface and attempts to escalate privilege. Multiple users were logged on and various combinations of log off and user identifications were used to test for separation of data and session integrity. It did not cover the flow control in exhaustive testing, but did cover the basic functionality of the TSF by exercising both valid user requests and invalid user requests. The coverage analysis relates the independent testing to ST claimed functionality and, although not required by EAL2, the coverage of all functions at the interface level was incorporated in the independent testing.

7.3 Strength of Function

The TOE was demonstrated to meet SOF basic.

7.4 Vulnerability Analysis

The vendor searched for publicly known vulnerabilities specifically related to the TOE using key words related to the product type, as well as publicly known vulnerabilities in the third-party products that are incorporated in the TOE. Potential product vulnerabilities in the developer's vulnerability analysis for the product were reviewed and justifications examined, with several added to the labs penetration test development. No publicly-known vulnerabilities specific to the evaluated version of 3eTi Server System were found. The developer examined the known vulnerabilities in the supporting third party products (MS Windows) using the National Vulnerability Database (nvd.nist.gov), the Common Vulnerability and Exposure list (www.cve.mitre.org), and SecureFocus (www.securityfocus.com); an explanation was given why these are not exploitable in the intended environment. These data bases covered primarily the environments and contained the standard 802.11 and other wireless vulnerabilities which were reviewed for exploitability and incorporated in the vulnerability testing where appropriate.

The evaluator devised penetration tests using the developer's analysis, including some of the developer's tests. NESSUS (www.nessus.org) was used for port analysis. No exploitable obvious vulnerabilities were found. The following tools were used in the vulnerability testing:

- Nessus version 3.0.3 (beta) for Windows
- nmap and WinPcap for Windows.
- The wireless sniffer tool AiroPeek NX, from WildPackets, software version is 2.0.5 and it is used without any modification

At EAL 2 vulnerability testing is only a requirement for obvious vulnerabilities.

8 Evaluated Configuration

The evaluated configuration was 3e-525A-3 Hardware Version 1.0, Software Version 4.0.9.11., and 3e-030-2 Software Version 3.0.7, both operating under Windows 2000 operating system. The hardware version has a bridge mode for extended the wireless range. This bridge mode was not in the evaluated configuration

9 Results of the 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 CC, Version 2.3; CEM, Version 2.3, and all applicable NIAP CCEVS and International Interpretations in effect on 13 October 2005.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 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 evaluation determined that the product is both **Common Criteria Part 2 extended and Part 3 conformant**, and meets the assurance requirements of EAL 2 augmented. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom Solutions. The security assurance requirements are displayed in the following table.

TOE Security Assurance Requirements (EAL 2 Augmented)

Augmentation shown in Italics

Assurance Class	Assurance Components
Configuration Management (ACM*)*	***ACM_CAP.3 Authorization controls***
	ACM_SCP.1 TOE CM coverage
Delivery and Operation (ADO)	**ADO_DEL.1 Delivery procedures**
	ADO_IGS.1 Installation, generation, and start-up procedures
Development (ADV)	**ADV_FSP.1 Informal functional specification**
	ADV_HLD.1 Security enforcing high-level design
	ADV_RCR.1 Informal correspondence demonstration
Guidance Documents (AGD)	**AGD_ADM.1 Administrator guidance**
	AGD_USR.1 User guidance
Life cycle support (ALC)	***ALC_FLR.2 Flaw reporting procedures***
Tests (ATE)	**ATE_COV.1 Analysis of Coverage**
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability assessment (AVA)	***AVA_MSU.1 Examination of guidance***
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

10 Validator Comments/Recommendations

The Validator agrees with the conclusion of the CygnaCom Solutions Evaluation Team, and recommends to CCEVS Management that an EAL2 augmented certificate rating be issued for 3eTI 3e-525A-3 Access System. Testing was more than would be expected at EAL2 in that the vendor test suite was completely duplicated by the laboratory and all security functions were independently tested though not exhaustively. Neither of these are required at the EAL2 level. Vulnerability testing was not exhaustive, but is not required at all at this level where a review of the vendor's vulnerability analysis is sufficient and a testing for obvious vulnerabilities is required.

The evaluators have looked at the design of the Access System, tested its functionality, and looked for obvious vulnerabilities; they found that the TOE satisfies the functional claims made in the ST and the validator concurs. Note that no evaluation verifies that there are no flaws, only that the evaluator could not find any.

The cryptography used in this product has been FIPS certified. The common criteria does not evaluate cryptologic algorithms. The use of FIPS certified algorithms, the mandatory access control and certificate administration scheme, are sufficient to provide the TOE and the client adequate mitigation against a moderate threat for confidentiality and integrity.

This is not true for availability. The TOE does not protect the connection between itself and the Client interface; an unauthorized party could potentially observe or disrupt this connection. However, encrypted communication will be more difficult to interpret. The wireless connection is subject to disruption and denial of service through jamming the wireless link. The bridging function available in the hardware for extending the range of the system is not included in the evaluated product. These factors were not tested and no claims were made that the TOE provided such protections.

The vendor chose to exclude the bridging capability of the server system. The bridging is used to extend the range of the wireless link by passing communication from one wireless access point to another. The vendor cited increased evaluation costs and time as the issues for not including this capability. Users should be advised that use of the bridging function places the system outside of the evaluated configuration.

The limited storage available for audit records may be extended by regularly archiving the logs to a network point as described in the administrator's manual.

11 Security Target

The Security Target for 3eTI 3e-525A-3 Access System is contained within the document 3e Technologies International 3e-525A-3 Access System Security Target, 22000201-701, Revision S, dated August 2006 [ST]. The ST is compliant with the *Specification of Security Targets* requirements found within Annex B of Part 1 of the CC [CCV2.3]. The ST is an accurate representation of the product and its functionality and is coherent. Excluded from the ST was the bridging function available in the product and is discussed in section 10. The ST adequately describes the TOE, the physical and logical boundaries and, to the extent tested, the interfaces present in the TOE (no additional interfaces have been discovered).

12 Glossary

The following table is a glossary of terms used within this validation report.

Acronym	Expansion
CC	*Common Criteria for Information Technology Security Evaluation*. [Note: Within this Validation Report, CC always means Version 2.3, dated August 2005.]
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CCIMB	Common Criteria Interpretations Management Board
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
I&A	Identification and Authentication
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
PP	Protection Profile
SFR	Security Function Requirement
SOF	Strength of Function
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

13 Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): http://niap.nist.gov/cc-scheme/
- Cygnacom Solutions: http://www.cygnacom.com/
- 3e Technologies International, Inc., http://www.3eti.com/
- Nessus vulnerability scanner, http://www.nessus.org/

CCEVS Documents

[CCV2.2] *Common Criteria for Information Technology Security Evaluation*, Version 2.2, January 2004.

[CCV2.3] *Common Criteria for Information Technology Security Evaluation*, Version 2.3, August 2005.

[CEMV2.2] *Common Methodology for Information Technology Security Evaluation*, Version 2.2, Part 2: Evaluation Methodology, January 2004.

[CEMV2.3] *Common Methodology for Information Technology Security Evaluation*, Version 2.3, Part 2: Evaluation Methodology, August 2005.

[CCEVS3] *Guidance to Validators of IT Security Evaluations*, Version 1.0, February 2000.

[CCEVS4] *Guidance to Common Criteria Testing Laboratories*, Draft, Version 1.0, March 2000.

Other Documents

[ST] 3e Technologies International 3e-525A-3 Access System Security Target, 22000201-701, Revision S, dated August 2006.