National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

For

Carrier Access Broadmore 500, 1700, and 1750

Release 4.1.1

Report Number: CCEVS-VR-06-0032

Dated: July 18, 2006

Version: 2.6

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

Validator

Nicole Carlson
Stuart Schaeffer, Senior Validator
The Aerospace Corporation
El Segundo, California

Common Criteria Testing Laboratory

Michelle Ruppel
Mark Plascencia
Sherie Kim
Ken Kolstad
InfoGard Laboratories
San Luis Obispo, California

Table of Contents

1 EXECUTIVE SUMMARY

This report documents assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Carrier Access Broadmore (the TOE). It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the InfoGard Common Criteria Testing Laboratory (CCTL) in San Luis Obispo, California, United States of America, and was completed in June 2006. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, produced by InfoGard. The evaluation determined that the product is both Common Criteria Part 2 and Part 3 Conformant, and meets the assurance requirements of EAL 3. The product does not claim conformance with any published Protection Profiles. All security functional requirements are derived from Part 2 of the Common Criteria or expressed in the form of Common Criteria Part 2 requirements.

During this evaluation, the validators monitored the activities of the InfoGard evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., work units of the Common Evaluation Methodology (CEM)), and reviewed successive versions of the Evaluation Technical Report (ETR) and test reports. The validator determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the validator concludes that the InfoGard findings are accurate, the conclusions justified, and the conformance claims correct.

2 INTRODUCTION[1]

The Broadmore is an Asynchronous Transfer Mode (ATM) service multiplexer enabling broadband and other non-ATM technologies to be transported across an ATM network. It is designed as an ATM network service access node that supports the transport of existing broadband services (voice, video, and data) over ATM networks. The Broadmore accepts signals from non-ATM-ready equipment, converts the signals to standard ATM cells, and multiplexes the cells onto a single ATM User Network Interface (UNI) port. Typically, the Broadmore is deployed at the edge of an ATM network as the ATM node element closest to the customer. Both Permanent Virtual Circuit (PVC) and Switched Virtual Circuit (SVC) service are available based upon user-defined module configuration. The Broadmore is designed as a modular system that can be configured to meet the service access and network interface requirements of the user. This is done by the use of different configuration of data-plane cards (that provide end-user traffic handling but do not involve any management or security services) and management cards that provide the management capabilities in a secure manner.

3 IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 3-1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

[1] Description of the TOE drawn from [7]

Table 3-1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation[2]	Carrier Access Broadmore 500 Release 4.1.1 P/N: 7665-500DC-CD, consisting of chassis 7665-05DC, CPU 7660-007, CPU I/O 7660-411 and Software Version 4.1.1 Carrier Access Broadmore 1700 Release 4.1.1 P/N: 7665-1700-CD, consisting of chassis 7665-17C, CPU 7660-007, CPU I/O 7660-411 and Software Version 4.1.1 Carrier Access Broadmore 1750 Release 4.1.1 P/N: 7665-1750-CD, consisting of chassis 7665-17B, CPU 7660-007, CPU I/O 7660-411 and Software Version 4.1.1
Protection Profile	None
Security Target	*Security Target for Carrier Access Broadmore 500, 1700, 1750 Release 4.1.1*, version 2.0, June 15 2006
Evaluation Technical Report	*Evaluation Technical Report for Carrier Access Broadmore 500, 1700, 1750 Release 4.1.1*, version 1.0, June 16 2006
Conformance Result	Common Criteria Version 2.2 (ISO/IEC 15408:1999) Part 2 and Part 3 Conformant; EAL 3
Sponsor	Carrier Access Corporation
Developer	Carrier Access Corporation
Evaluators	InfoGard Laboratories
Validator	The Aerospace Corporation

While the fully qualified name of the TOE is found in Table 1 above, in the interest of conciseness it may be referred to as *Carrier Access Broadmore 500, 1700, and 1750 release 4.1.1*.

[2] Carrier Access Corporation has indicated that it identifies refurbished units with the suffix "-REF" appended to the part number (e.g. 7665-500DC-CD-REF for a refurbished Carrier Access Broadmore 500 Release 4.1.1 unit). As they are functionally identical to new units, they are part of this evaluation.

4 SECURITY POLICY

No organizational security policies apply.

5 ASSUMPTIONS [3]

5.1 Usage Assumptions

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

5.2 Environmental Assumptions

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

A.PHYSEC The TOE hardware and software critical to the TOE will be protected from unauthorized physical modification.

It is assumed that the IT environment provides support commensurate with the expectations of the TOE. This is achieved by using evaluated products (or products in evaluation at the time of the writing of this VR) in the environment. The expectations of the TOE with respect to the security provided by the IT environment are captured in the ST in the environmental objectives, but *were not* verified by the evaluation.

[3] Information drawn from [8]

6 ARCHITECTURAL INFORMATION[4]

The Broadmore 500, 1700, and 1750 Release 4.1.1 devices are ATM service multiplexers: Asynchronous Transfer Mode multiplexers. They are designed to receive as input raw broadband data (e.g. voice, video) and convert the data to ATM cells for transport over an ATM network. Only the security management features of these devices are included in this evaluation.

Figure 6.1 presents an example of the Broadmore device in its environment. In this example, two Broadmore devices are used to connect two non-ATM based devices. Non-ATM device 1 sends transmissions using the services it supports to the Broadmore, which converts the communications to an ATM format and sends them over the ATM service to another Broadmore. The second Broadmore converts the ATM format to the non-ATM format used by the second non-ATM device.

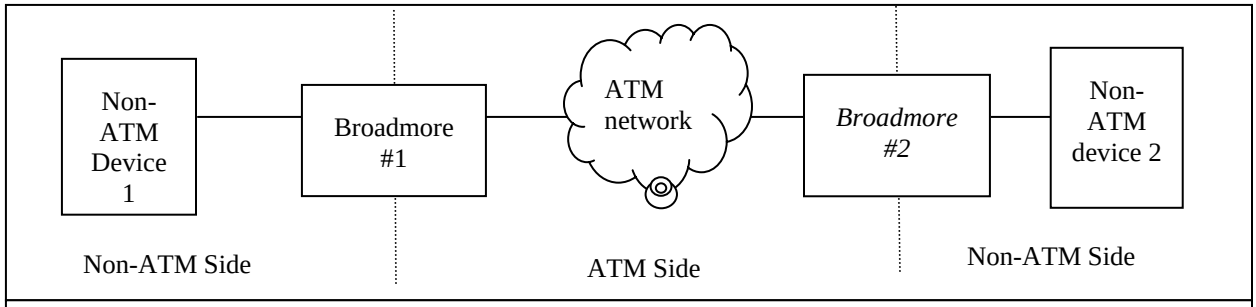

Figure 6-1: The Broadmore in a Sample Environment

Figure 6-1: The Broadmore architecture, presents a generic view of the components of the Broadmore appliance and its environment. Elements of the diagram are described in the following paragraphs. This sample architecture shows a Broadmore 1700 model configured with redundant NIM and CPU, and with a remote workstation connected via an Ethernet port to the CPU board. Note that this is one possible configuration for the model 1700.

[4] Information and figures drawn from [8]

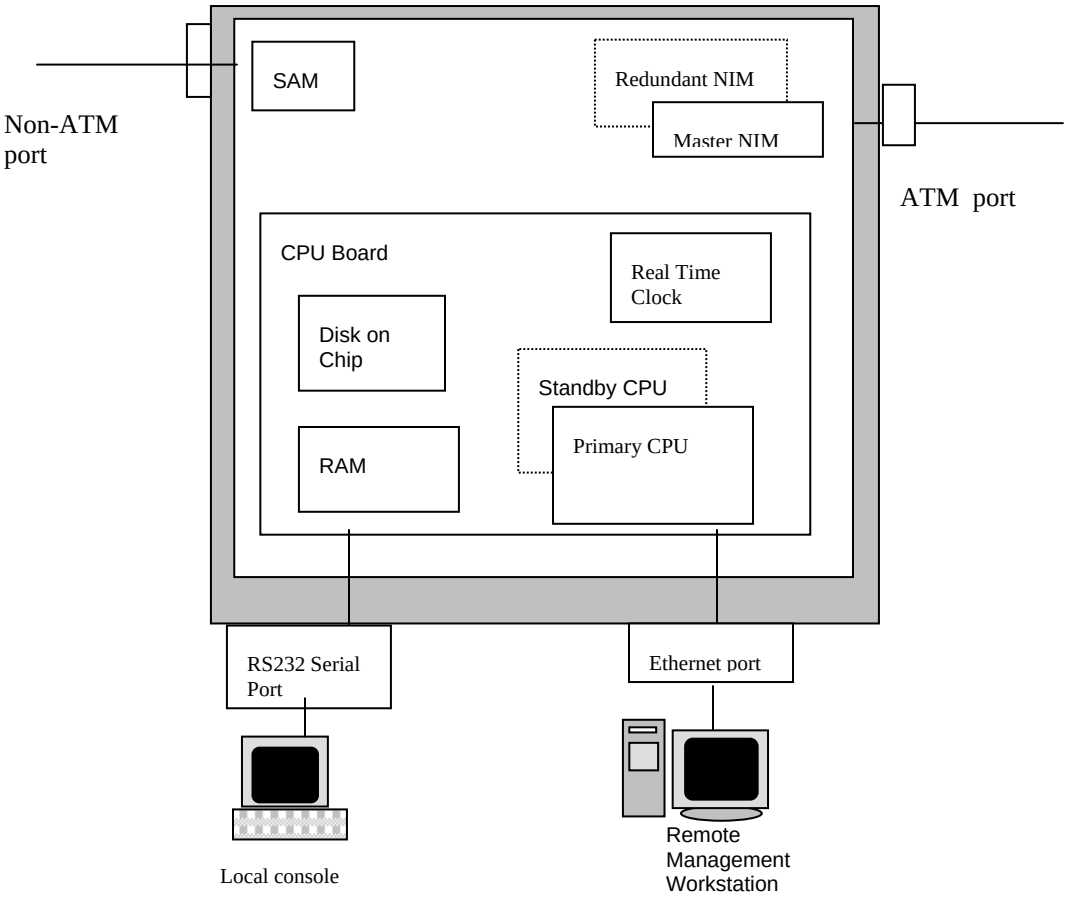

Figure 6-1: The Broadmore architecture

7 SECURITY FUNCTIONALITY

7.1 Identification and Authentication

All access to the system requires identification and authentication before any use of system resources is made. The TOE can also correctly handle authentication failure (i.e. by disallowing access). Non-alphanumeric passwords are permitted. Remote access is encrypted with SSH.

7.2 Audit

The TOE has the capability to collect specified audit data, store it securely, and protect it from modification, deletion, or access by unauthorized users. Since audit logs are the only means of maintaining accountability for administrators, the administrator guidance explicitly warns against altering or removing audit logs. Tools for review of the audit trail are available. All actions are traceable to a single logon ID and provide reliable date, time, and identification of the resources accessed.

7.3 Security Management

This TOE is expected to be transparent to the end users, who do not have any security-related access privileges. Administrative duties are broken up into roles, and role-based access control is used to limit access to users authorized to perform particular functions. Security functions are clearly identified and defined, and the means by which access to each function is limited is delineated.

7.4 TOE Protection

The TOE is designed to disallow attempts to bypass its security functions. Data passing through the device (i.e. the ATM traffic that the device is intended to handle) cannot access any security-relevant resources. Non-administrative users have no access to the TOE. No single user has unlimited privileges to modify the TOE, and as only one administrative user may be logged on at a time and administrative sessions cannot interfere with each other.

7.5 Protection against Hardware Failure

The Broadmore device features two redundant power supplies, one redundant CPU (optional), one redundant Network Interface Module (optional), and one redundant SAM for every four production SAMs (optional). It can automatically switch to these backups as needed, without loss of functionality or security. This functionality only applies to models 1700 and 1750.

8 DOCUMENTATION

The following documentation was used as evidence for the evaluation of Carrier Access Broadmore 500, 1700, 1750 release 4.1.1:

8.1 Design documentation

Document	Version	Date
Carrier Access EAL 3 Design Document Broadmore 500, 1700 & 1750	1.6	March 13 2006

8.2 Guidance documentation

Document	Version	Date
Carrier Access EAL 3 Broadmore Installation and Administrative Guidance, CCIG-0001 Ch 2 – 10, Appendix A-D	Rev. 12	June 2006

8.3 Configuration Management and Lifecycle documentation

Document	Version	Date
EAL3 Configuration Management Broadmore 500, 1700, & 1750, CCCM-0001	Rev. 0.9	June 15 2006
EAL-3 Life Cycle Document Broadmore 500, 1700 & 1750, CCL-0001	Rev. 0.5	November 14 2005

8.4 Delivery and Operation documentation

Document	Version	Date
EAL3 Secure Delivery Document Broadmore 500, 1700, & 1750, Version CCDD-0001	0.4	June 1 2005
Carrier Access EAL 3 Broadmore Installation and Administrative Guidance, CCIG-0001 Ch 2 – 10, Appendix A-D	Rev. 12	June 2006

8.5 Test documentation

Document	Version	Date
Carrier Access Broadmore 500, 1700, and 1750 v.4.1.1 Independent Testing Test Plan	1.0	June 15 2006
EAL 3 Test Plan Document Broadmore 500, 1700 & 1750	2.5	May 12 2006
EAL 3 Test Results Document Broadmore 500, 1700 & 1750	2.5	May 12, 2006

8.6 Vulnerability Assessment documentation

Document	Version	Date
EAL 3 Vulnerability Analysis Broadmore 500, 1700, & 1750	Version CCV-0001 Revision 5.0	May 16 2006

8.7 Security Target

Document	Version	Date
Broadmore 1750, 1700, and 500 Release 4.1.1 Security Target	2.0	June 15 2006

9 IT PRODUCT TESTING

9.1 Developer Testing

Evaluator analysis of the developer's test plans, test scripts, and test results indicate that the developer's testing is adequate to satisfy the requirements of EAL 3.

The developer's tests consisted of a suite of tests that covered the security functions claimed in the ST. The tests verified the basic functionality of the TOE, and exercised the parameters and verified the exception conditions documented in the user and administrative guidance.

For each of the developer tests, the evaluators analyzed the test procedures to determine whether the procedures were relevant to, and sufficient for, the function being tested. The evaluators also verified that the test documentation showed results that were consistent with the expected results for each test case. The evaluation team elected to run approximately 75% of the developer's test suite, focusing on security-relevant tests. All tests completed successfully.

9.2 Evaluator Testing

9.2.1 Functional Testing

In addition to developer testing, the CCTL conducted its own suite of functional tests, which were created independently of the developer. All tests completed successfully. These tests were designed to verify the claimed functionality of TOE security functions, including:

- Protection of the audit trail from unauthorized modification
- Institution of a time delay after successive unsuccessful logons
- Enforcement of minimum user ID and password lengths
- Restriction of privileged functions to privileged users

9.2.2 Vulnerability Testing

The evaluators developed vulnerability tests to address both management functions and security functions controlling access to the TOE, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

9.2.3 Penetration testing

The evaluation team attempted to break the security of the TOE with the following results:

- Modification of the audit trail by any user other than a privileged user was denied.
- Commands run with unexpected or invalid input did not place the system into an unsecure state.

10 EVALUATED CONFIGURATION[5]

- Chassis assembly: Broadmore 7665-1750 set with dual CPU and I/O modules included
- CPU 7660-007 (includes I/O modules)
- 7660-317 OC-3 Set (includes I/O modules)
- 7660-114 OC-12 Set (includes I/O modules)
- 7660-034 DS3 SAM
- Multimode Fiber for OC-12 connections
- Redundant DC Power Supply
- Power supply and power cords for equipment

[5] Drawn from ATE_IND.2 v1.0, dated June 16 2006

11 RESULTS OF THE EVALUATION

The evaluation was conducted based upon the Common Criteria (CC), Version 2.2, dated August 1999 [1,2,3,4]; the Common Evaluation Methodology (CEM), Version 1.0, dated August 1999 [6]; and all applicable International Interpretations in effect on 1 April 2004. The evaluation confirmed that the Carrier Access Broadmore 500, 1700 and 1750 product is compliant with the Common Criteria Version 2.2, functional requirements (Part 2), and assurance requirements (Part 3) for EAL 3. The details of the evaluation are recorded in the CCTL's evaluation technical report, *Evaluation Technical Report for Carrier Access Broadmore 500, 1700, and 1750 Release 4.1.1*, version 1.0 (June 16 2006). The product was evaluated and tested against the claims presented in the *Broadmore 1750, 1700, and 500 Release 4.1.1 Security Target*, version 2.0, dated June 15 2006.

The validator followed the procedures outlined in the Common Criteria Evaluation Scheme Publication Number 3 for Technical Oversight and Validation Procedures. The validator has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validator therefore concludes that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the Evaluation Technical Report provided by the CCTL.

11.1 Evaluation of the Security Target (ASE)

The evaluation team read and analyzed the TOE's security target. They determined that the ST presented a clear, consistent, precise, and accurate picture of the TOE's security goals and the methods used to achieve those goals.

11.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team analyzed the CM documents describing the developer's system for tracking changes to the product and maintaining the configuration of TOE components. They found that the CM documentation provides a clear picture of the steps and processes required to correctly configure the TOE.

11.3 Evaluation of the Delivery and Operation Documents (ADO)

The purpose of the ADO evaluation is to make sure that the procedures in place to deliver, install, and configure the TOE securely are adequate. The team found that the vendor has procedures in place to ensure that the correct version of the TOE is delivered; both technological, e.g., a checksum of the software, and procedural, e.g. using a particular website or manually verifying the unit's serial number. The team also tested the installation and configuration procedures in the Configuration Guide to ensure that the prescribed procedures result in a secure installation.

11.4 Evaluation of the Development (ADV)

The evaluation team assessed the design documentation and found it a clear, consistent, and complete explanation of how the TSF provides its security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also verified that the actual implementation of the TOE was a correct and complete interpretation of the high-level design.

11.5 Evaluation of the Guidance Documents (AGD)

The evaluation team verified that the user guidance was sufficient to describe how to use the operational TOE, and that the administrator guidance was sufficient to describe how to securely administer the TOE. The team found that the guidance documents provided adequate guidance for these purposes.

11.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team assessed the adequacy of the developer procedures to protect the TOE and the TOE documentation during development and maintenance, to reduce the risk of introducing new vulnerabilities into the TOE. These included technological measures such as the protection of source code, physical measures such as limiting access to the development facility, and personnel measures such as hiring practices. The team found that the vendor's management of lifecycle issues is adequate.

11.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team ensured that the TOE performs as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. The evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. In addition to executing a sample of the vendor test suite, the team devised and ran their own independent set of functional tests. These independent tests were designed to complement the set of vendor tests; they tested critical TSFs that, in the evaluator's opinion, were not adequately tested by the vendor test suite. TSFs judged to be especially critical and/or difficult to implement correctly were also subjected to independent tests. The set of these tests verified, for example, that traffic claimed by the TOE to be encrypted was in fact encrypted and that the TOE did require a successful login before granting access. The team also performed penetration tests, including attempts to exploit buffer overflows and checks for improperly configured network ports, which did not uncover any vulnerabilities. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

11.8 Vulnerability Assessment Activity (AVA)

This work unit, in addition to the development and execution of penetration tests, requires two separate analyses:

1. a strength of function (SOF) analysis determines whether the claimed protection level is substantiated;

2. a vulnerability analysis examines public information to determine if there are known vulnerabilities that may affect the TOE (for example, vulnerabilities affecting the underlying operating system).

These analyses found a high level of confidence that no serious vulnerabilities are known to exist in the TOE.

11.9 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence verifies that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor tests suite, the independent tests, and the penetration testing also demonstrated the accuracy of the claims in the ST.

12 VALIDATOR COMMENTS

The TOE makes use of cryptographic functions evaluated under the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2. This is a separate standard from the Common Criteria, and these functions were not evaluated further during this evaluation.

13 SECURITY TARGET

Broadmore 1750, 1700, and 500 Release 4.1.1 Security Target, version 2.0, dated June 15 2006

14 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.2.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.2.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.2.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.2.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[7] Broadmore 1750, 1700, and 500 Release 4.1.1 Security Target, version 2.0, dated June 15 2006

[8] Evaluation Technical Report for Carrier Access Broadmore 500, 1700, and 1750 Release 4.1.1, version 1.0, dated June 16 2006