National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Blue Ridge Networks

BorderGuard Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2

Report Number: CCEVS-VR-04-0071

Dated: 9 August 2004

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

ACKNOWLEDGEMENTS

Validation Team

Mike Allen

Aerospace Corporation

Columbia, Maryland

Common Criteria Testing Laboratory

COACT, Incorporated

Columbia, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP validator's assessment of the evaluation of Blue Ridge Networks BorderGuard Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2. 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 COACT Incorporated, and was completed during July 2004. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by COACT. The evaluation determined that the product is both **Common Criteria Part 2 and Part 3 conformant,** and meets the assurance requirements of **EAL 2.** The product is not conformant with any published Protection Profiles, but rather is targeted to satisfy the needs for protection of sensitive information as defined by DoD Standard 8500.2. All security functional requirements are derived from Part 2 of the Common Criteria.

The product family enables multiple sites (enclaves) to communicate securely over an untrusted communication network (i.e. the internet). It provides a secure communications infrastructure that allows access to corporate information from anywhere, at any time, with appropriate security. Each enclave is protected by a BorderGuard 3140 or 4000 device that encrypts IP address-selected communications between peer BorderGuard devices establishing a "Virtual" Private channel across a public network. A separate BorderGuard device is assigned as the VPN manager's device and establishes encrypted management links to all of the BorderGuard devices it is assigned to manage. The VPN Manager Application software operates on a Windows 2000 or Windows NT workstation. A graphic interface allows the VPN Manager to configure filtering rules, monitor connections and review logs. The manager's workstation is used for initial configuration of the TOE, BorderGuard management, trouble shooting, setting the clock and additional management functions.

NOTE: The use of the International Data Encryption Algorithm (IDEA), which is the default setting of the BorderGuard Cryptoservers, is not part of the evaluated configuration since IDEA is not FIPS 140.1 or 140.2 compliant. VPN managers must manually select one of the other data encryption algorithms (AES or 3DES) to ensure compliance with this evaluation. In addition, the BorderGuard Administration Guides speak of using VPN Client software on workstations to allow "dial-in" or remote access. The VPN Client software was not part of the evaluation and should not be used in the evaluated configuration. Finally, in the *Site to Site VPN Administrator's Guide* there is a discussion of allowing Blue Ridge Networks to act as the VPN Manager for a customer's installation. This was explicitly disallowed by the Security Target since it was assumed the customer will provide their own VPN administration. Customers should NOT use Blue Ridge Networks as their VPN manager.

The validator monitored the activities of the COACT evaluation team, participated in team meetings, 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., the CEM work units), and reviewed successive versions of the 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 COACT findings are accurate, the conclusions justified, and the conformance claims correct.

2. 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 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.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Blue Ridge Networks BorderGuard Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2
Protection Profile	None
Security Target	*Blue Ridge Networks BorderGuard Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2 Security Target R.1.10*, December 17, 2003.
Evaluation Technical Report	*Evaluation Technical Report for the Blue Ridge Networks BorderGuard Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2.*, August 4, 2004
Conformance Result	Part 2 and Part 3 conformant, EAL 2
Sponsor	Blue Ridge Networks
Developer	Blue Ridge Networks
Evaluators	COACT Incorporated
Validator	The Aerospace Corporation

3. SECURITY POLICY

The BorderGuard VPN suite enforces the following security policies:

3.1. Security Audit Policy

The Audit function is performed by both components of the TOE. The VPN Manager is the central component for all audit data for the VPN. The BorderGuard 3140/4000 Firmware sends audit events to the VPN Manager. These event messages are transmitted to the VPN Manager over the encrypted secure management channel that exists between each Cryptoserver and the Secure Administrator Device. The connection between the Secure Administrator Device and the VPN Manager computer is secured physically by connecting the Secure Administrator Device directly to the VPN Manager, using an Ethernet cross-over cable, with no other network appliances in between. The VPN Manager formats event messages that it generates, and those received from the Firmware, and reports them to the local Windows Application Event log using Windows APIs embedded in the VPN Manager program. The Windows NT Event log provides the storage for the audit trail and allows audit review by the authorized administrator.

3.2. Cryptographic Policy

The Cryptographic function is performed by the Cryptographic subsystem of the BorderGuard 3140/4000 Firmware. The Cryptographic subsystem's core function is to establish and maintain the cryptographic tunnels (sleeves) between Cryptoservers. To provide this functionality, the BorderGuard 3140/4000 Firmware performs key generation, key distribution, key destruction, encryption, decryption, replay protection, integrity checking and authentication. The default encryption algorithm assumed by a Cryptoserver is the International Data Encryption Algorithm (IDEA). Since IDEA has not been certified in accordance with FIPS 140.1 or 140.2, the VPN manager must manually select one of the other algorithms used by the Cryptoserver (AES or 3DES).

3.3. Filtering Policy

The Filtering function resides in the BorderGuard 3140/4000 Firmware. It uses packet filter policies to monitor and control the flow of packets through the Cryptoserver based on policy rules. The TOE has two distinct information flows, management data and user data. The two information flows use sleeves to secure the data. Management data is data that terminates at BorderGuard 3140/4000 Firmware or at the VPN Manager. User data is data that is destined for a subnet protected by a Cryptoserver in the VPN, which is running BorderGuard 3140/4000 Firmware. Both information flows use the rules set in the packet filter policy definitions to determine the appropriate action for a given packet.

The Authorized Administrator sets the packet filtering policy definitions via the VPN Manager Application software. When a policy is created or modified, the affected Cryptosevers are uploaded with the new definitions. Upon initial installation, The VPN Manager enables each instance of the BorderGuard 3140/4000 Firmware with a default set of secure packet filtering policies.

3.4. Identification and Authentication Policy

The BorderGuard 3140/4000 Firmware and the VPN Manager require the Authorized Administrator to be identified and authenticated prior to allowing any security function actions to be taken. The TOE has one role, the Authorized Administrator. The Authorized Administrator logs onto the VPN Manager computer using their valid Windows NT user id and password. Once successfully authenticated by Windows, the Authorized Administrator has access to the VPN Manager Application Software. To access an individual Cryptoserver, the Authorized Administrator must then log in to the Firmware running on each device. This process is managed by the VPN Manager Application Software, which communicates (via a secure channel) to the target Cryptosever Firmware.

3.5. Security Management

The VPN Manager Application Software provides the interface to management functions for the TOE. The VPN Manager centrally manages the Firmware on the Cryptoservers. One security role is maintained, that of the Authorized Administrator. The VPN Manager Application Software allows the following control: firmware initialization, changes to initial values, add and remove Cryptoservers, monitor Cryptoserver status, define Cryptoserver policies, change passwords, access audit data, generate, delete or assign cryptographic key attributes, and modify, delete or assign authentication data.

3.6. Self Test Policy

The Self Test function of the TOE performs abstract machine testing. During start up the BorderGuard 3140/4000 Firmware performs a series of tests on the underlying hardware of the Cryptoserver. If any test fails, the Cryptoserver is considered defective and the boot process halts. The reason for the test failure is provided to the Authorized Administrator in the Cryptoserver display.

4. ASSUMPTIONS

4.1. Usage Assumptions

Administrators are assumed to be trusted (i.e., non-malicious) and competent to carry out their responsibilities.

Peer Cryptoservers will enforce compatible security policies.[1]

Information can not flow between protected enclaves without passing through the Cryptoserver firmware.

4.2. Environmental Assumptions

The Cryptoservers and VPN Manager software have been delivered, installed, and configured in accordance with documented procedures.

The Cryptoservers and VPN Manager workstation are located in a physically protected and secure facilities to prevent physical access to the TOE by anyone other than authorized personnel.

The Windows NT environment provides reliable timestamps.

The Windows NT environment provides adequate Identification and Authentication.

The Windows NT environment provides adequate Audit logging and review capability.

[1] Compatible is defined to mean that a core set of policy rules are identical and any differences are more restrictive.

5. ARCHITECTURAL INFORMATION

The Target of Evaluation (TOE) consists of two distinct components:

- the BorderGuard 3140/4000 Firmware, release 6.2; and,
- the VPN Manager Application Software, release 2.2.

The BorderGuard 3140/4000 Firmware resides on the *Blue Ridge Networks* VPN Cryptoserver device. The VPN Manager Application Software resides and executes on a dedicated Windows based PC. The TOE provides the functionality for the *Blue Ridge Networks* Virtual Private Network (VPN). The fundamental concept of operation for a *Blue Ridge Networks* VPN is a network of Cryptoservers centrally managed by a VPN Manager.

- BorderGuard Firmware

The BorderGuard Firmware provides the cryptographic functions to protect the flow of IP packets into and out of the cryptographically secure sleeves established between peer server devices. Audit data is generated by the firmware and relayed to the VPN Manager software via the cryptographically protected management sleeve. A self test function is invoked whenever the firmware is initialized.

- VPN Manager Application Software

The VPN Manager interface allows an authorized administrator to: initialize the Borderguard firmware, change the initial values, add and remove Cryptoservers, monitor Cryptoserver status, define Cryptoserver policies, change passwords, access audit data, generate, delete or assign cryptographic key attributes, and modify, delete or assign authentication data.

6. DOCUMENTATION

The following documentation was used as evidence for the evaluation of the Blue Ridge Networks BorderGuard Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2.

1. Blue Ridge Networks BorderGuard Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2 Security Target R.1.10, December 17, 2003.
2. Configuration Management Plan, Version R.4.0, November 10, 2003.
3. Delivery & Release Plan, Version R.1.0, November 8, 2002.
4. Blue Ridge VPN Manager Quick Start Manual R.3.0, May 4, 2004.
5. Blue Ridge VPN Functional Specification, Revision 1.4, October 6, 2003.
6. VPN Manager User Guide, Revision 2.2, January 2, 2003.
7. Site to Site VPN Administrator's Guide, Revision 4.1, August 28, 2002.
8. High Level Design For Blue Ridge Networks BorderGuard Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2; Revision 4.0, October 10, 2003.
9. Blue Ridge VPN Correspondence Analysis, Revision 3, October 28, 2003.
10. Blue Ridge Networks Security Test Plan & Procedures, Revision 1.2, October 6, 2003.
11. Blue Ridge Networks Security Test Coverage, Revision 1.1, October 6, 2003.
12. Blue Ridge Networks Security Test Procedure Results, Revision 1.0, January 6, 2004.
13. Evidence Documentation Supporting The Strength of TOE Security Function For Blue Ridge Networks BorderGuard 3140/4000 Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2, Revision 1.0, May 19, 2004.

7. IT PRODUCT TESTING

7.1. 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 EAL2.

The developer's tests were largely focused on the Administrator's interface to the TOE, with security testing of the authentication mechanism, and audit trail functions. The developer's test suite also tested all of the available encryption mechanisms and the management of the encryption keys as well as the proper flow control of IP packets through the Cryptoservers and the Self-Test functions of these devices.

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. They also verified that the test documentation showed results that were consistent with the expected results for each test script.

7.2. Evaluator Testing

Although the developer's testing was considered adequate, the evaluators also partially tested each of the security functions as defined in the Security Target. Specifically:

- VPN Manager Authentication
- Audit File Generation and Alarms
- Cryptographic Operation
- VPN Interface Filtering
- Self-Test Errors

During penetration testing, the evaluators also executed a number of tests to determine whether the TOE is vulnerable to audit trail overflow vulnerabilities or a Denial-of-service tear-drop attack.

7.2.1. VPN Manager Authentication

Evaluator tests were performed to verify that valid passwords are required to access all elements of the TOE, including the VPN Managers console and each VPN Cryptoserver. This tested the identification and authentication ability of the devices and corresponding software.

7.2.2. Audit File Generation and Alarms

Evaluator tests were performed to confirm that the VPN Manager can detect alarms from the managed VPN devices and that these alarms protect the integrity of the VPN. The alarms are viewed in Windows Event Viewer. This series of tests assessed the Audit Security Function. The following Alarm states were tested:

- Login failure
- Sleeve down/sleeve up
- Sleeve failure
- New public key
- Sleeve definition added

7.2.3. Cryptographic Operation

The evaluators performed tests to confirm that data passing through the cryptographic sleeve was indeed unreadable by an eavesdropper. Both encrypted and unencrypted traffic flows were captured and analyze during this test.

7.2.4. VPN Interface Filtering

The evaluators performed tests to verify the security of the VPN, the VPN Manager including the Secure Admin (SA) device and the devices not part of the VPN. The security testing that was covered included User Data Protection, Identification and Authentication, and the Security Management. During these tests, the team determined the capability to traceroute or telnet from various devices one to another, some part of the VPN and others outside the VPN but attempting to join. Filters prevent the telnet and traceroute when the device is not part of the VPN system.

7.2.5. Self-Test Errors

The evaluators performed tests to confirm the proper operation of the Cryptoserver self test functions. Both good and bad Cryptoserver configurations were used. The following list documents the configurations tested:

- Good (properly configured Cryptoserver)
- Internal memory card failure (memory card removed)
- Short in the Flash memory
- Internal battery failure (removed)

7.2.6. Vulnerability Testing

The evaluators tested the ability of the TOE to handle Denial of Service attacks and Audit trail overflows.

8. EVALUATED CONFIGURATION

The evaluated configuration consists of a group of Blue Ridge Networks BorderGuard 3140/4000 Cryptoservers running the Blue Ridge Networks BorderGuard Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and managed by at least one Windows workstation running the Blue Ridge Networks VPN Manager Application Software Release 2.2 and protected by a separate 3140/4000 Cryptoserver. The evaluated configuration requires:

- Local logging and storage of audit records on the Windows workstation.
- Local Windows timestamp generator for use in audit records.
- The Ethernet port used to manage the TOE is connected via a cross-over cable to the VPN Manager's Cryptoserver.
- Physical access to the TOE both locally and at remote sites is limited to trusted administrators of the TOE.

The default configuration for the 3140/4000 Cryptoservers is for the use of IDEA as the data encryption algorithm. This configuration was **not** evaluated and must be manually changed by the VPN Manager to use either AES or 3DES as the encryption algorithm.

In addition, the Administration Guides discuss the use of Client Software on remote workstations that allow remote access to Cryptoservers. This software was **not** evaluated and should not be used in the evaluated configuration.

Finally, the *Site to Site VPN Administrator's Guide* discusses the use of Blue Ridge Networks as the VPN manager for a customer's VPN. This option was specifically excluded from the Security Target and not evaluated as part of this effort.

9. RESULTS OF THE EVALUATION[2]

The evaluation was conducted based upon the Common Criteria (CC), Version 2.1, dated August 1999 [1,2,3,4]; the Common Evaluation Methodology (CEM), Version 1.0, dated August 1999 [6]; and all applicable National and International Interpretations in effect on 21 January 2003. The evaluation confirmed that the Blue Ridge Networks BorderGuard Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2 products are compliant with the Common Criteria Version 2.1, functional requirements (Part 2) and assurance requirements (Part 3) for EAL2. The details of the evaluation are recorded in the CCTL's evaluation technical report, Evaluation Technical Report for the Blue Ridge Networks BorderGuard Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2, August 4, 2004. The product was evaluated and tested against the claims presented in the Blue Ridge Networks BorderGuard Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2 Security Target R.1.10, August 3, 2004.

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.

9.1. Evaluation of the Security Target (ASE)

The evaluation team applied each EAL 2 ASE CEM work unit. Evaluation team action during the course of the ST evaluation ensured that the ST contained a description of the environment in terms of threats, assumptions and policies; a statement of security requirements claimed to be met by the BorderGuard TOE that are consistent with the Common Criteria; and product security function descriptions that support the requirements.

9.2. Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 2 ACM CEM work unit. The ACM evaluation ensures that the integrity of the TOE is adequately preserved; in particular, that configuration management provides confidence to the consumer that the TOE and documentation used for evaluation are the ones prepared for distribution. It also ensures that the TOE is accurately and uniquely identified such that the consumer is able to identify the evaluated TOE and discern one version from another. Configuration Management (CM) systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking changes and by ensuring that all changes are authorized. The Evaluation Team identified and analyzed the Blue Ridge CM process to

[2] The terminology in this section is defined in CC Interpretation 008, specifying new language for CC Part 1, section/Clause 5.4.

ensure that its documented procedures were followed and the procedures were employed during the course of this evaluation. The evaluation team ensured that the following items were considered configuration items: TOE implementation, design documentation, test documentation, and user guidance.

9.3. Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to securely deliver, install, configure, and operationally use the TOE; and ensured that the security protection offered by the TOE was not compromised during that process.

9.4. Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF implements/employs the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

9.5. Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 2 AGD CEM work unit. The evaluation team verified the adequacy of the administrator guidance in describing how to securely administer the BorderGuard TOE.

9.6. Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements. The evaluation team performed a sample of the Blue Ridge test suite, and devised an independent set of team tests and penetration tests. The Blue Ridge tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

9.7. Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain obvious vulnerabilities that can be exploited in the evaluated configuration, based upon the Blue Ridge strength of function analysis and the Blue Ridge vulnerability analysis as well as the evaluation team’s performance of penetration tests.

9.8. Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s performance of the vendor test suite, several independent tests, and the penetration test further demonstrated the claims in the ST.

10. EVALUATOR COMMENTS

The validator observations support the evaluation teams conclusion that Blue Ridge Networks BorderGuard Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2 meet the claims stated in the Security Target. The validator also wishes to emphasize that the TOE must be installed and operated in the evaluated configuration in order to ensure that the TOE provides the security functionality described in the security target. This is particularly important when selecting the data encryption algorithm for the Cryptoservers. IDEA is the default algorithm but was not evaluated as part of the evaluated configuration. Either the Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) must be manually selected by the VPN Manager to ensure appropriate security. Also, the remote access configuration, where the VPN Client software is installed on a remote workstation to allow encrypted communication with a Cryptoserver, was NOT evaluated and the use of this capability, which is discussed in detail in the Administration Guides, removes the system from the evaluated configuration. In addition, the *Site to Site VPN Administrator's Guide* discusses allowing Blue Ridge Networks to act as the VPN Manager for a customer's installation. This option was explicitly removed from the security target for evaluation purposes.

11. SECURITY TARGET

Blue Ridge Networks BorderGuard Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2 Security Target R.1.10, December 17, 2003.

12. GLOSSARY

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
API	Application Program Interface
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CM	Configuration Management
DoD	Department of Defense
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
IDEA	International Data Encryption Algorithm
IP	Internet Protocol
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PKI	Public Key Infrastructure

PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface
VPN	Virtual Private Network

13. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[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] Blue Ridge Networks BorderGuard Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2 Security Target R.1.10, December 17, 2003.

[8] Evaluation Technical Report for the Blue Ridge Networks BorderGuard Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2, August 4, 2004