Certification Report

EAL 2 Evaluation of CipherOptics Inc. CipherOptics™ SG-series Network Security Appliance Version 3.1 - Models SG100 and SG1002

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-36
Version: 1.0
Date: October 21, 2005
Pagination: i to iv, 1 to 11

DISCLAIMER

The Information Technology (IT) product identified in this certification report has been evaluated using the *Common Methodology for Information Technology Security Evaluation, Version 2.2 r256*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.2 r256*. The evaluation was conducted by an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS). This certification report and its associated certificate apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment (CSE), or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the CSE, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is DOMUS IT Security Laboratories, located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated October 21, 2005, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at:
http://www.cse-cst.gc.ca/en/services/common_criteria/trusted_products.html

This certification report makes reference to the following trademarked names:
CipherOptics™ which is a trademark of CipherOptics Inc.

TABLE OF CONTENTS

Disclaimer ..... **i**

Foreword ..... **ii**

Executive Summary **1**

1 Identification of Target of Evaluation **3**

2 TOE Description **3**

3 Evaluated Security Functionality **3**

4 Security Target **3**

5 Common Criteria Conformance **4**

6 Security Policy **4**

7 Assumptions and Clarification of Scope **4**

7.1 SECURE USAGE ASSUMPTIONS 4
7.2 ENVIRONMENTAL ASSUMPTIONS 4
7.3 CLARIFICATION OF SCOPE 5

8 Architectural Information **5**

9 Evaluated Configuration **6**

10 Documentation **6**

11 Evaluation Analysis Activities **7**

12 ITS Product Testing **8**

12.1 ASSESSING DEVELOPER'S TESTS 8
12.2 INDEPENDENT FUNCTIONAL TESTING 8
12.3 INDEPENDENT PENETRATION TESTING 8
12.4 CONDUCT OF TESTING 9
12.5 TESTING RESULTS 9

13 Results of the Evaluation **9**

14 Evaluator Comments, Observations and Recommendations **9**

15 Acronyms and Abbreviations **10**

16 References 11

Executive Summary

The CipherOptics™ SG-series Network Security Appliance Version 3.1 - Models SG100 and SG1002, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation.

The CipherOptics™ SG-series Network Security Appliance Version 3.1 - Models SG100 and SG1002, also referred to as the CipherOptics™ SGx, are encryption appliances that provide end-to end data security for IP-based network traffic between remote sites across an unsecured wireless or wireline network.

Compliant with the Internet Protocol Security (IPSec) standard (RFC 2401), the CipherOptics™ SGx provides 3 levels of security:

- Confidentiality – Industry standard algorithms encrypt data: AES, 3DES and DES encryption;
- Integrity – Hash algorithms prevent the undetected alteration of data as it traverses the network: HMAC-SHA-1 and HMAC-MD5
- Authentication – X.509 v3 digital certificates and the digital signature standard (DSS) are used to verify the identity of the peer IP gateway that is the source of the data.

Key management is provided by Internet Key Exchange (IKE), manual keys, and Diffie-Hellman Groups 1, 2 and 5.

DOMUS IT Security Laboratories is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on October 19, 2005, and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for the CipherOptics™ SGx, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the CipherOptics™ SGx are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report[1] for this product provide sufficient evidence that it meets the EAL 2 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 2.2 r256* (with applicable final interpretations), for conformance to the *Common Criteria for IT Security Evaluation, version 2.2 r256*.

[1] The evaluation technical report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

The Communications Security Establishment, as the CCS Certification Body, declares that the CipherOptics™ SGx evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation is the CipherOptics™ SG-series Network Security Appliance Version 3.1 - Models SG100 and SG1002, also referred to as the CipherOptics™ SGx, from CipherOptics Inc.

2 TOE Description

The CipherOptics™ SGx is an encryption appliance that secures IP-based network traffic while it is in transit across an unsecured wireless or wireline network. Operating at Gigabit Ethernet (CipherOptics™ SG1002) and Fast Ethernet (CipherOptics™ SG100) wire-speeds, the CipherOptics™ SGx protects site-to-site links that transmit information where a delay caused by encryption can affect data quality.

The CipherOptics™ SGx is housed in a tamper evident chassis, and complies with the Internet Protocol Security (IPSec) standard (RFC 2401) to provide security services. IPSec is a framework of standards developed by the Internet Engineering Task Force (IETF) to support the secure exchange of packets at the IP layer.

For the purpose of this Evaluation, the CipherOptics™ SGx is configured and operated in the following deployments:

- Using a layer 2 switch in a back to back configuration
- At layer 3 in a routed network

To secure the data traveling between two sites, a CipherOptics™ SGx is deployed at each site with complementary security policies configured on each appliance. Traffic is encrypted between the two CipherOptics™ SGx appliances over an untrusted network, providing end-to-end data security.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the CipherOptics™ SGx is identified in Section 5 of the ST.

4 Security Target

The ST associated with this Certification Report (CR) is identified by the following nomenclature:

Title: CipherOptics SG-series Security Target
Version: Revision A
Date: February 8, 2005

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 2.2 r256*, for conformance to the *Common Criteria for IT Security Evaluation, version 2.2 r256* incorporating all final interpretations issued prior to 15 October 2004. The CipherOptics™ SG-series Network Security Appliance Version 3.1 - Models SG100 and SG1002 is:

a) Common Criteria Part 2 conformant, with security functional requirements based only upon functional components in Part 2;
b) Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and
c) Common Criteria EAL 2 conformant, with all the security assurance requirements in the EAL 2 package.

6 Security Policy

The CipherOptics™ SGx implements an information flow control policy. The subjects under the control of this policy are external IT entities sending information through the TOE to internal IT entities, and internal IT entities sending information through the TOE to external IT entities. Policy detail can be found in Section 5.4 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the CipherOptics™ SGx should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will help to ensure the proper and secure operation of the CipherOptics™ SGx.

7.1 Secure Usage Assumptions

For purposes of this evaluation, the administrative personnel are assumed to be trusted and not careless, wilfully negligent, or hostile. The administrative users must follow and abide by the instructions provided by the administrator documentation. These documents are listed in Section 10.

7.2 Environmental Assumptions

For purposes of this evaluation, the CipherOptics™ SGx is assumed to be located at a physically secure location, with appropriate physical security measures.

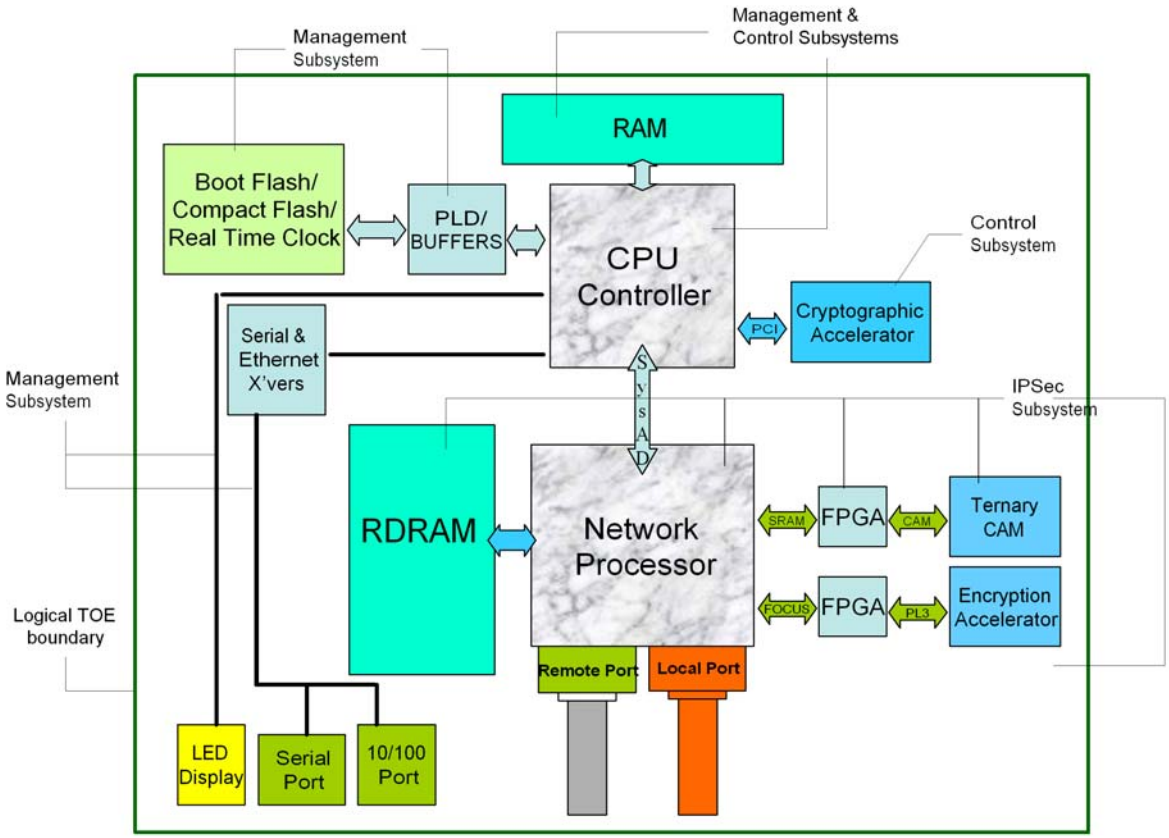
7.3 Clarification of Scope

The CipherOptics™ SGx can not prevent authorized administrators from carelessly configuring the TOE such that the information flow control policy is compromised.

It provides a level of protection that is appropriate for an assumed non-hostile and well-managed user community. While it is designed to protect its user community against inadvertent or casual attempts to breach system security, it is not intended for situations in which determined attempts by hostile and well-funded attackers use sophisticated attacks from within the physical zone.

8 Architectural Information

The CipherOptics™ SGx is comprised of three subsystems, which are illustrated in the functional block diagram view below. The sub-systems include: an IPSec Subsystem, a Control Subsystem, and a Management Subsystem. For additional architectural information please refer to Section 2 of the ST.



9 Evaluated Configuration

The following CipherOptics™ SGx configurations have been evaluated.

Model	Hardware Version	Firmware
CipherOptics™ SG100	Revision A	3.1
CipherOptics™ SG1002	Revision A	3.1

In the evaluated configuration, encrypted traffic must use the IPSec policy specified below.

Parameter	Value
Mode	Tunnel
Authentication	Certificates
IKE Phase 1	
Cipher algorithm	AES-256
Hash algorithm	SHA-1
Negotiation mode	Main mode
IPSec Phase 2	
IPSec protocol	ESP
Cipher algorithm	AES-256
Hash algorithm	SHA-1

10 Documentation

The documentation for the CipherOptics™ SGx consists of the following:

- CipherOptics™ SG-Series Network Security Appliance User Guide IPS Version 3.1 Revision 3,
- CipherOptics™ SG-Series Network Security Appliance Common Criteria Evaluated Installation and Configuration Guide IPS Version 3.1 Revision 1,
- CipherOptics™ SG100 Network Security Appliance Installation Guide Rev. 2, and
- CipherOptics™ SG1002 Network Security Appliance Installation Guide Rev. 2

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the CipherOptics™ SG-series Network Security Appliance Version 3.1 - Models SG100 and SG1002, including the following areas:

Configuration management: An analysis of the CipherOptics™ SGx development environment and associated documentation was performed. The evaluators found that the CipherOptics™ SGx configuration items were clearly marked and that control was exercised over all modifications to the configuration items. The developer's configuration management system was observed during the site visit, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the CipherOptics™ SGx during distribution to the consumer. The evaluators examined the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the CipherOptics™ SGx functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the CipherOptics™ SGx administrator documents and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators assessed the development security procedures during a site visit and determined that the procedures detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the CipherOptics™ SGx design and implementation.

Vulnerability assessment: The CipherOptics™ SGx Security Target's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis, and found that it sufficiently described each of the potential vulnerabilities along with sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer had considered all potential vulnerabilities. Limited penetration testing was conducted by evaluators, which exposed residual vulnerabilities not exploitable in the intended operating environment of the CipherOptics™ SGx.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing independent vulnerability tests.

12.1 Assessing Developer's Tests

The evaluators verified that the developer had met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the Evaluation Technical Report (ETR)[2].

The evaluators analyzed the developer's test coverage analysis, and found it to be complete and accurate. The correspondence between tests identified in the developer's test documentation and the functional specification was complete.

12.2 Independent Functional Testing

During this evaluation, the evaluators developed independent functional tests by examining the design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results.

Based on a review of the developer's tests, independent testing concentrated on the following areas:

a. audit;
b. identification and authentication;
c. information flow control; and
d. security management

Tests were selected which demonstrate that the TOE satisfies the security functional requirements specified in the Security Target.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis and test activities, limited independent evaluator penetration testing was conducted. Penetration testing did not uncover any exploitable vulnerabilities for the CipherOptics™ SGx in the anticipated, restrictive operating environment.

[2] The evaluation technical report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

12.4 Conduct of Testing

The CipherOptics™ SGx was subjected to a comprehensive suite of formally-documented, independent functional tests. The testing took place at the DOMUS IT Security Laboratories located in Ottawa, Ontario. The CCS Certification Body witnessed a portion of the independent testing.

The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in the ETR.

12.5 Testing Results

The developer tests and independent functional tests yielded the expected results, giving assurance that the CipherOptics™ SGx behaves as specified in its ST and functional specification.

13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 2** level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The CipherOptics™ SG-series Network Security Appliance Version 3.1 - Models SG100 and SG1002 includes comprehensive guides for the installation, configuration and operation of the product.

15 Acronyms and Abbreviations

Acronym/Abbreviation/Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCRA	Arrangement on the Recognition of Common Criteria Certificates
CCS	Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CR	Certification Report
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPSec	Internet Security Protocol
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
UDP	User Datagram Protocol

16 References

This section lists all documentation used as source material for this report:

a) Common Criteria for Information Technology Security Evaluation, CCIMB-2004-01-001/002/003, Version 2.2 r256, January 2004.

b) Common Methodology for Information Technology Security Evaluation, CCIMB-2004-01-004, Evaluation Methodology, Version 2.2 r256, January 2004.

c) CCS #4: Technical Oversight for TOE Evaluation, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 1.0, 3 October 2002.

d) Security Target – CipherOptics SG-series Security Target, 007-101-001 Revision A.

e) Evaluation Technical Report (ETR) Version 1.3 CipherOptics™ SG-series Network Security Appliance Version 3.1 - Models SG100 and SG1002 EAL 2, October 19, 2005.