Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

Senetas CN 4000/6000 Series Ethernet Encryptors v5.5.0

25 March 2025

606-LSS

V1.0

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (a branch of CSE). This certification report, and its associated certificate, applies 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 Canadian Common Criteria Program, and the conclusions of the testing laboratory 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 Canadian Centre for Cyber Security, 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 Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your organization has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Canadian Centre for Cyber Security
Contact Centre and Information Services
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

OVERVIEW

The Canadian Common Criteria Program provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Testing Laboratory (CCTL) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCTL is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the 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, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCTL.

The certification report, certificate of product evaluation and security target are posted to the Common Criteria portal (the official website of the International Common Criteria Program).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Senetas CN 4000/6000 Series Ethernet Encryptors v5.5.0 (hereafter referred to as the Target of Evaluation, or TOE), from **Senetas Corporation Ltd., distributed by Thales SA (Safenet)** , was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Section 1.1 for the evaluated security functionality.

Lightship Security is the CCTL that conducted the evaluation. This evaluation was completed on **25 March 2025** and was carried out in accordance with the rules of the Canadian Common Criteria Program.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for the TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations, and recommendations in this Certification Report.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list (CPL) for the Canadian Common Criteria Program and the Common Criteria portal (the official website of the International Common Criteria Program).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	Senetas CN 4000/6000 Series Ethernet Encryptors v5.5.0
Developer	Senetas Corporation Ltd., distributed by Thales SA (Safenet)

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

The TOE claims the following conformance:

EAL2+ augmented (ALC_FLR.2)

1.2 TOE DESCRIPTION

The TOE is a high-speed, standards-based encryptor designed to secure voice, data and video information transmitted over Ethernet networks. The TOE also provides access control facilities using access rules for each defined Ethernet connection.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

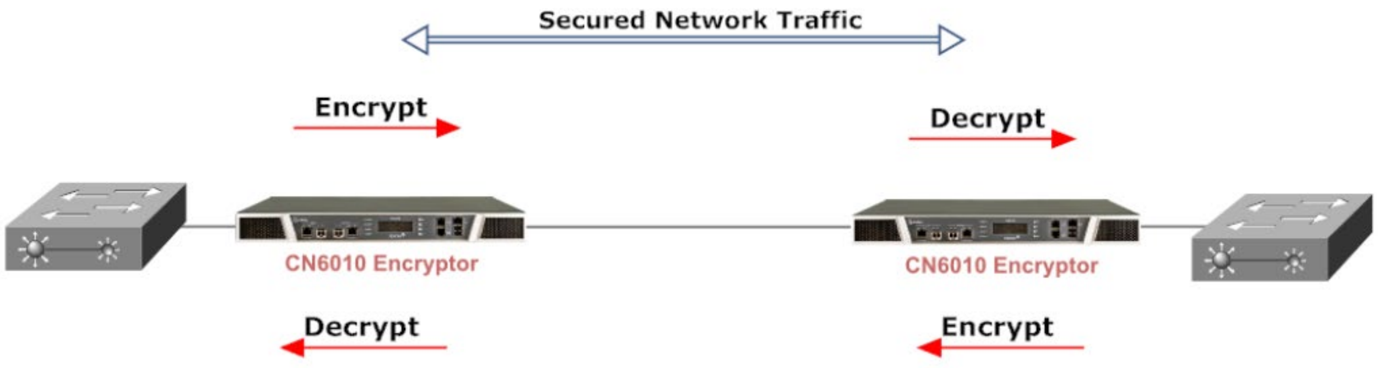

Figure 1: TOE Architecture

2 SECURITY POLICY

The TOE implements and enforces policies pertaining to the following security functionality:

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

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic implementations are used by the TOE and have been evaluated by the CAVP:

Table 2: Cryptographic Implementation(s)

Cryptographic Implementation	Certificate Number
CN Series Common Crypto Library v5.5.0	A3451
CN4010 1G Ethernet Crypto Module v1.10	A3435
CN4010 1G Ethernet TIM Crypto Module v1.10	A3436
CN4020 1G Ethernet Crypto Module v1.10	A3437
CN4020 1G Ethernet TIM Crypto Module v1.10	A3438
CN6010 1G Ethernet Crypto Module v1.10	A3439
CN6010 1G Ethernet TIM Crypto Module v1.10	A3440
CN6110 10G Ethernet Crypto Module v1.11	A3441
CN6110 10G Ethernet TIM Crypto Module v1.11	A3442
CN6110 1G Ethernet TIM Crypto Module v1.10	A3443
CN6110 1G Ethernet Crypto Module v1.10	A3549
CN6140 10G Ethernet TIM Crypto Module v1.11	A3444
CN6140 1G Ethernet Crypto Module v1.10	A3445
CN6140 10G Ethernet Crypto Module v1.11	A3448
CN6140 1G Ethernet TIM Crypto Module v1.10	A3460
CN6140 4x10G Ethernet Crypto Module v1.11	A3492

3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

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

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- The TOE is protected from unauthorized physical access.
- The TOE is appropriately located within the network to protect the desired network traffic.

3.2 CLARIFICATION OF SCOPE

The following security functions were not enabled or tested for the evaluation:

- Remote authentication via TACACS+.
- KeyVault – The TOE can sign certificates from credentials held within a key vault.
- Hybrid Keys - The TOE supports the use of hybrid key establishment schemes combining NIST approved algorithms with candidate QKD/QRA systems.
- Log Offloading – The TOE supports sending logs to a remote syslog server.
- REST API – The TOE supports a RESTful HTTP(S) interface used for remote monitoring and issue detection.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

TOE Software/Firmware	TOE Firmware v5.5.0 Build: 31224	
TOE Hardware	● CN4010 ● CN4020 ● CN6010	● CN6110 ● CN6140
Environmental Support	● CM7 Application ● File Server (for firmware upgrades) ● Key Server. Remote KMIP or NAE service.	

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a) Ethernet Encryptor CN4010 User Guide, (WindowsTM / All Modes), Revision Date: January 2024
b) Ethernet Encryptor CN4020 User Guide, (WindowsTM / All Modes), Revision Date: January 2024
c) Ethernet Encryptor CN6010 User Guide, (WindowsTM / All Modes), Revision Date: January 2024
d) CN6110 Ethernet Encryptor User Guide, (WindowsTM / All Modes), Revision Date: January 2024
e) Ethernet Encryptor CN6140 User Guide, (WindowsTM / All Modes), Revision Date: January 2024
f) Senetas, Distributed by Thales, CN 4000/6000 Series Ethernet Encryptors v5.5.0 Preparative Procedures (AGD_PRE.1), v1.2
g) Senetas, Distributed by Thales, CN 4000/6000 Series Ethernet Encryptors v5.5.0 Operational User Guidance (AGD_OPE.1), v1.2

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance and determined that they are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all the procedures required to maintain the integrity of the TOE during distribution to the consumer.

6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent tests, and performing a vulnerability analysis.

6.1 ASSESSMENT OF DEVELOPER TESTS

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the Evaluation Test Report (ETR). The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT TESTING

During this evaluation, the evaluator developed independent functional & penetration tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

a. Repeat of Developer's Tests: The evaluator repeated a subset of the developer's tests.

b. TRANSEC data through-put: The evaluator verified that the data through-put remains constant regardless of channel usage.

c. TIM mode encryption: The evaluator verified that traffic is encrypted when using TIM mode.

d. Cryptographic Implementation Verification: The evaluator verified that the claimed cryptographic implementations were present.

e. Supported SNMP modes: The evaluator verified that only the claimed SNMP modes are supported.

6.3.1 INDEPENDENT TESTING RESULTS

The developer's tests and the independent tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

6.4 VULNERABILITY ANALYSIS

The vulnerability analysis focused on 4 flaw hypotheses.

- Public Vulnerability based (Type 1)
- Technical community sources (Type 2)
- Evaluation team generated (Type 3)
- Tool Generated (Type 4)

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases and technical community sources (Type 1 & 2). Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities (Type 4). Based upon this review, the evaluators formulated flaw hypotheses (Type 3), which they used in their vulnerability analysis.

Type 1 & 2 searches were conducted on **6 March 2025** and included the following search terms:

TOE name and models (Section 4)	Senetas	Xilinx Zynq-7000	Arm Cortex A9
Debian Linux 11.7	OpenSSH 8.4p1	CoreUtils 8.32	Curl 7.74.0
Net-SNMP 5.9	MicroHTTP	Ulfius 2.2.1	PamTacPlus
OpenSSL 1.1.1n	KeySecure		

Vulnerability searches were conducted using the following sources:

NIST National Vulnerabilities Database (NVD) https://web.nvd.nist.gov/view/vuln/search	CISA - Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
OpenSSL Vulnerabilities: https://openssl-library.org/news/vulnerabilities-1.1.1/	

6.4.1 VULNERABILITY ANALYSIS RESULTS

The vulnerability analysis did not uncover any security relevant residual exploitable vulnerabilities in the intended operating environment.

7 RESULTS OF THE EVALUATION

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security. This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

This evaluation has provided the basis for the conformance claim documented in Section 1.1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

The TOE provides line encryption functionality. The developers are responsive to potential vulnerabilities, patching the TOE quickly to address these potential vulnerabilities.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCTL	Common Criteria Testing Laboratory
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
ST	Security Target
TIM	Transport Independent Mode
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Security Target Senetas CN 4000/6000 Series Ethernet Encryptors v5.5.0, 2025-03-21, v1.4.
Evaluation Technical Report Senetas CN 4000/6000 Series Ethernet Encryptors v5.5.0, 2025-03-25, v1.3.