National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

TM

Validation Report
for the
Senetas
Distributed by Thales
CN Series Encryptors 5.5.0

Report Number: CCEVS-VR-VID11485-2024
Dated: December 31, 2024
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers, Ph.D.

Patrick Mallett, Ph.D.

Seada Mohammed

The Aerospace Corporation

Common Criteria Testing Laboratory

Joon Sim

Lightship Security USA, Inc.

Table of Contents

List of Tables

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Senetas Distributed by Thales CN Series Encryptors 5.5.0 provided by Senetas Corporation Ltd, Distributed by Thales SA (SafeNet). It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in December 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the collaborative Protection Profile for Network Devices, Version: 3.0e, Functional Package for Secure Shell (SSH), Version: 1.0.

The TOE is Senetas Distributed by Thales CN Series Encryptors 5.5.0. The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the Security Target and analysis performed by the Validation Team.

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, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Evaluated Product	Senetas Distributed by Thales CN Series Encryptors 5.5.0
Sponsor and Developer	Senetas Corporation Ltd, Distributed by Thales SA (SafeNet) 312 Kings Way, South Melbourne, Victoria 3205, Australia
CCTL	Lightship Security USA, Inc. 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
CEM	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017.

Item	Identifier
Protection Profile	collaborative Protection Profile for Network Devices, Version: 3.0e, Date: 06-December-2023 [NDcPP] Functional Package for Secure Shell (SSH), Version: 1.0, Date 13-May-2021 [PKG_SSH]
ST	Senetas Distributed by Thales CN Series Encryptors 5.5.0 Security Target, v1.7, December 2024
Evaluation Technical Report	Senetas Distributed by Thales CN Series Encryptors v5.5.0 Evaluation Technical Report, Version 1.2, December 2024
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Evaluation Personnel	Joon Sim
CCEVS Validators	Jerome Myers, Patrick Mallett, Seada Mohammed

3. Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The CN Series Encryptors are typically installed between an operator's private network equipment and public network connection and are used to secure data transiting over Ethernet networks. When operating at full bandwidth, the Ethernet Encryptor will not discard any valid Ethernet frame in all modes of operation.

3.1. TOE Evaluated Configuration

The TOE is the encryptor hardware and firmware (Build: 31224). Table 2 shows the TOE models. All TOE models use the same embedded software and share the same hardware architecture.

The TOE interfaces are as follows:

a) CLI. Local management via serial access to the CLI.

b) SSH. Remote management via SSH / SSHS access to the CLI.

c) Syslog. Remote syslog server via SSH / SSHS.

3.2. Physical Boundary

The physical boundary of the TOE is the encryptor hardware and firmware. Table 2 shows the TOE models. All TOE models use the same embedded software (version shown in Section 3.1) and share the same hardware architecture. Table 2 columns are as follows:

a) Model. The TOE model number.
b) CPU & ASIC. The CPU and ASIC for the TOE model.
c) Hardware. The part numbers associated with the hardware enclosure and supported power supply.
d) Power. Type of power supply for each hardware part number for a given model.
e) Protocol / FPGA Bitstream. The supported protocols and related FPGA bitstream, including whether TIM is supported.
f) AES Modes. The supported AES Modes.
g) I/F. The supported local/network port interfaces.
h) LCD/Keypad. Whether the model includes an LCD and Keypad.

Table 2: TOE models

Model	CPU & ASIC	Hardware	Power	Protocol / FPGA Bitstream	AES Modes	I/F	LCD/ Keypad
CN4010	ARM Cortex A9	A4010B	DC (Plug Pack)	1G Ethernet 1G Ethernet TIM	CTR	RJ45	No
CN4020	ARM Cortex A9	A4020B	DC (Plug Pack)	1G Ethernet 1G Ethernet TIM		SFP	No
CN6010	ARM Cortex A9	A6010B A6011B A6012B	AC/AC Dual DC/DC Dual AC/DC Dual	1G Ethernet 1G Ethernet TIM		RJ45 SFP	Yes
CN6110	ARM Cortex A9	A6110B A6111B A6112B	AC/AC Dual DC/DC Dual AC/DC Dual	1G Ethernet 1G Ethernet TIM 10G Ethernet 10G Ethernet TIM		RJ45 SFP+	Yes
CN6140	ARM Cortex A9	A6140B A6141B	AC/AC Dual DC/DC Dual	1Gx1 Ethernet Single Port 1Gx4 Ethernet Multi Port 1Gx1 Ethernet TIM Single Port 1Gx4 Ethernet TIM Multi Port		SFP+	Yes

Model	CPU & ASIC	Hardware	Power	Protocol / FPGA Bitstream	AES Modes	I/F	LCD/ Keypad
		A6142B	AC/DC Dual	10Gx1 Ethernet Single Port 10Gx2 Ethernet Multi Port			
				10Gx1 Ethernet TIM Single Port 10Gx4 Ethernet TIM Multi Port			
				10Gx4 Ethernet Multi Port			
CN9120	ARM Cortex A9	A9120B A9121B A9122B	AC/AC Dual DC/DC Dual AC/DC Dual	100G Ethernet		QSFP 28	Yes

3.3. Required Non-TOE Hardware, Software, and Firmware

The TOE operates with the following components in the environment:

a) Audit Server. Remote syslog server.

4. Security Policy

This section summarizes the security functionality of the TOE:

4.1. Security Audit

The TOE generates audit records of user and administrator actions. The TOE includes the user identity in audit events resulting from actions of identified users. The Security Administrator can configure the TOE to send logs in real-time to a syslog server via SSH.

4.2. Cryptographic Support

The TOE implements a cryptographic module. The cryptographic module has the ability to generate, destroy cryptographic keys, authenticate keys, perform key exchanges in protected communications and validate signatures in image upgrades. Cryptographic functions are primarily used with the SSH protocol. Relevant Cryptographic Algorithm Validation Program (CAVP) certificates are shown in Table 4 of the ST.

4.3. Identification and Authentication

The TOE ensures that all users must be authenticated before accessing its functions and data. The TOE uses public keys for authentication for SSH.

4.4. Security Management

The TOE enables secure management of its security functions, including:

i) Administrator authentication with passwords
ii) Configurable password policies
iii) Role Based Access Control
iv) Access banners
v) Management of critical security functions and data
vi) Protection of cryptographic keys and passwords

4.5. Protection of the TSF

The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions. The TOE performs diagnostic self-tests and cryptographic module self-tests during start-up and generates audit records to record a failure. Self-tests comply with the FIPS 140-2 requirements for self-testing.

4.6. TOE Access

TOE can be accessed directly via serial connection or remotely via SSH connection. When a user account has sequentially failed authentication the configured number of times, the account will not be locked.

4.7. Trusted Path/Channels

The TOE protects the integrity and confidentiality of communications using cryptographic algorithms as described in Table 4 of the ST.

5. Assumptions

Identifier	Description
A.PHYSICAL_ PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_ FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2 of the ST, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.
A.NO_THRU_ TRAFFIC_ PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).

Identifier	Description
A.REGULAR_ UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_ CREDENTIALS_ SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_ INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

6. Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_ND_V3.0E/PKG_SSH_V1.0 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made in accordance with the evaluation activities specified in cPP_ND_v3.0e-SD/ PKG_SSH_V1.0 and performed by the Evaluation team
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the CPP_ND_V3.0E/PKG_SSH_V1.0 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

Functions not included in the TOE Evaluation:

- Point-to-point and Point-to-Multipoint Layer2 Encryption
- CM7
- RESTful SNMP MIB Interface
- Keypad Hardware panel
- SNMPv3

7. Documentation

The following guidance documents were made available with the TOE for evaluation. They are provided with the TOE upon delivery.

a) Senetas Distributed by Thales CN4000/CN6000/CN9000 Series Ethernet Encryptors Firmware Version 5.5.0 Operational User Guidance (AGD_OPE.1), v1.1, 16 December 2024
b) Senetas Corporation CN4010 Encryptor All Operational Modes, Rev 55-24-010, October 2024
c) Senetas Corporation CN4020 Encryptor All Operational Modes, Rev 55-24-010, October 2024
d) Senetas Corporation CN6010 Encryptor All Operational Modes, Rev 55-24-010, October 2024
e) Senetas Corporation CN6110 Encryptor All Operational Modes, Rev 55-24-010, October 2024
f) Senetas Corporation CN6140 Encryptor All Operational Modes, Rev 55-24-010, October 2024
g) Senetas Corporation CN9120 Encryptor Ethernet Mode, Rev 55-24-010, October 2024

All documentation delivered with the product is relevant to and within the scope of the TOE. Only the Administrator Guides listed above, and the specific sections of the other documents referenced by the guides should be trusted for the installation, administration, and use of this product in its evaluated configuration.

8. IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in *Senetas Distributed by Thales CN Series Encryptors v5.5.0 Assurance Activity Report, v1.2* provides an overview of testing and the prescribed evaluation activities.

8.1. Developer Testing

No evidence of developer testing is required in the SARs or Evaluation Activities.

8.2. Evaluation Team Independent Testing

The Evaluation team conducted independent testing at Lightship Security USA in Baltimore, MD from June 2024 until December 2024. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Evaluation Activities.

Each Evaluation Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

The specific test configurations and test tools utilized may be found in the AAR section 9.5.

8.3. Evaluated Configuration

The TOE testing environment components are identified in Figure 1 and Table 3 below.

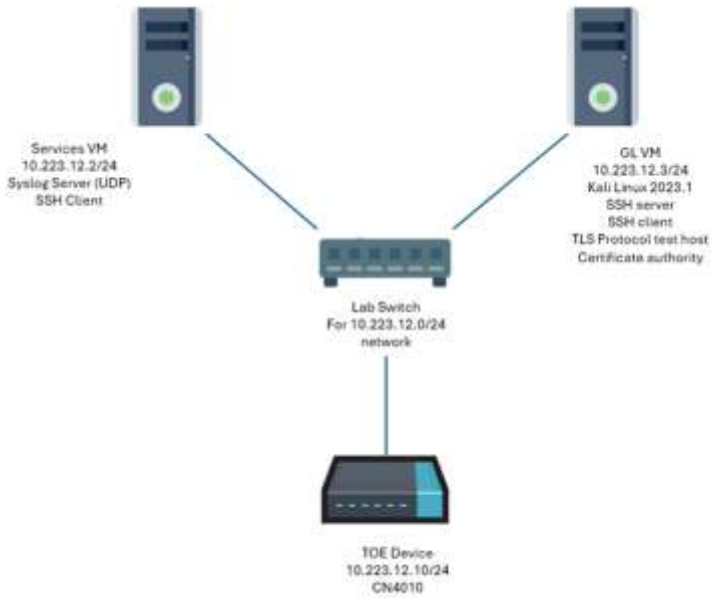

Figure 1: Testing Environment Overview

Table 3: Tools Used for Testing

Tool name	Version	Description
Lightship Greenlight	3.0.35	Tool used for TLS and SSH handshake modification
OpenSSL	1.1.1m	OpenSSL was used for simple TLS server or TLS client connections
Wireshark	4.0.8 (Linux) & 3.6.16 (Windows)	Used for packet capture and analysis
Tcpdump	4.99.1	Used for packet capture and analysis
Python	3.11.4 (GL VM) 2.7.16 (Services VM)	HTTP server
OpenSSH	OpenSSH 8.8p1	SSH client for accessing the Remote CLI
Syslog-ng	3.19.1	Syslog server

9. Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that all activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC Version 3.1 Revision 5 and CEM Version 3.1 Revision 5. The evaluation determined Senetas Distributed by Thales CN Series Encryptors 5.5.0 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Evaluation Activities specified in cPP_ND_v3.0e-SD/ PKG_SSH_V1.0.

9.1. Evaluation of Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Senetas Distributed by Thales CN Series Encryptors 5.5.0 that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.2. Evaluation of Development Documentation (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST and Guidance documents. Additionally, the evaluator performed the Evaluation Activities related to the examination of the information contained in the TSS.

The Validation reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.3. Evaluation of Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the

evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.4. Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

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

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the Test Evaluation Activities and recorded the results in a Test Report, summarized in the AAR.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.6. Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Senetas Distributed by Thales CN Series Encryptors v5.5.0 Vulnerability Assessment, v1.1 report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on October 24 and December 12, 2024, did not uncover any residual vulnerability.

The Evaluation team searched:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- US-CERT: http://www.kb.cert.org/vuls/html/search
- Tenable Network Security: https://www.tenable.com/cve
- Tipping Point Zero Day Initiative: https://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

The Evaluation team performed a search using the following keywords:

- Senetas CN Series Encryptors v5.5.0
- CN4010
- CN4020

- CN6010
- CN6110
- CN6140
- CN9120
- ARM Cortex A9
- OpenSSL 1.1.1n
- OpenSSH 8.4p1
- Common Crypto Library
- Coreutils v.8.3.2
- Bash v. 5.1-2+deb11u1
- Curl v.7.74.0
- Net-snmp v.5.9
- Microhttpd v.0.9.59
- Ulfius v.2.1
- Pamtacplus v.1.3.8
- Keysecure v.8.4.2cd
- Busybox v. 1:1.30.1-6+b3
- ppp v.2.4.7-1+4
- lcd4linux v. 0.11.0-SVN-1092
- Liboqs v.0.7.0
- Liboqse v.0.7.0
- Lxc v.4.0.6
- Serdisplib v.1.98.0

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.7. 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 test activities also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM and performed the Evaluation Activities in cPP_ND_v3.0e-SD/ PKG_SSH_V1.0, and correctly verified that the product meets the claims in the ST.

10. Validator Comments

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documentation referenced in Section 7 of this Validation Report. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness. No versions of the TOE and software, either earlier or later, were evaluated.

11. Annexes

Not applicable.

12. Security Target

Senetas Distributed by Thales CN Series Encryptors 5.5.0 Security Target, v1.7, December 2024.

13. GLOSSARY

- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance:** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature:** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
DHCP	Dynamic Host Configuration Protocol
ETR	Evaluation Technical Report
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFD	Multi-Function Device
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

15. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001*, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security ffunctional requirements, CCMB-2017-04-002*, Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security aassurance requirements, CCMB-2017-04-003*, Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004*, Version 3.1, Revision 5, April 2017
5. Collaborative Protection Profile for Network Devices, Version: 3.0e, Date: 06-December-2023
6. Functional Package for Secure Shell (SSH), Version: 1.0, Date: 13-May-2021
7. Senetas Distributed by Thales CN Series Encryptors 5.5.0 Security Target, v1.7, December 2024
8. Senetas Distributed by Thales CN4000/CN6000/CN9000 Series Ethernet Encryptors Firmware Version 5.5.0 Operational User Guidance (AGD_OPE.1), v1.1, 16 December 2024
9. Senetas Corporation CN4010 Encryptor All Operational Modes, Rev 55-24-010, October 2024
10. Senetas Corporation CN4020 Encryptor All Operational Modes, Rev 55-24-010, October 2024
11. Senetas Corporation CN6010 Encryptor All Operational Modes, Rev 55-24-010, October 2024
12. Senetas Corporation CN6110 Encryptor All Operational Modes, Rev 55-24-010, October 2024
13. Senetas Corporation CN6140 Encryptor All Operational Modes, Rev 55-24-010, October 2024
14. Senetas Corporation CN9120 Encryptor Ethernet Mode, Rev 55-24-010, October 2024
15. Senetas Distributed by Thales CN Series Encryptors v5.5.0 Assurance Activity Report, v1.2, Date: December 2024