



**Australian Government**  
**Department of Defence**

# **Australasian Information Security Evaluation Program**

**Certification Report**  
**2014/89**

**18 Aug 2014**  
**Version 1.0**

Commonwealth of Australia 2014

Reproduction is authorised provided  
that the report is copied in its entirety.

# Amendment Record

Version	Date	Description
1.0	18/08/2014	Final

## Executive Summary

The TOE is the Senetas CN Series Encryptor Range & CM Management Application Software.

The CN series encryptors are high-speed, standards based multi-protocol encryptors specifically designed to secure voice, data and video information transmitted over Ethernet and Fibre Channel data networks at data rates up to 10 Gigabits per second. It also provides access control facilities using access rules for each defined Ethernet or Fibre Channel connection.

This report describes the findings of the IT security evaluation of Senetas CN Series Encryptor Range & CM Management Application Software to the Common Criteria (CC) evaluation assurance level EAL2+. The report concludes that the product has met the target assurance level of EAL2+ and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by CSC and was completed on 17 July 2014.

With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that authorised users:

- a) should operate the CM Management Application from a secure location.
- b) should enter the time according to UTC 0 and then select the desired time zone to ensure correct time is maintained.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target at Ref [1] and read this Certification Report prior to deciding whether to purchase the product.

# Table of Contents

<b>1. Executive Summary .....</b>	<b>iv</b>
<b>2. Table of Contents.....</b>	<b>v</b>
<b>3. Chapter 1 – Introduction .....</b>	<b>1</b>
<i>Overview.....</i>	<i>1</i>
<i>Purpose.....</i>	<i>1</i>
<i>Identification.....</i>	<i>1</i>
<b>4. Chapter 2 - Target of Evaluation .....</b>	<b>3</b>
2.1 <i>Overview.....</i>	<i>3</i>
2.2 <i>Description of the TOE.....</i>	<i>3</i>
2.3 <i>Security Policy.....</i>	<i>3</i>
2.4 <i>TOE Architecture.....</i>	<i>3</i>
2.5 <i>Clarification of Scope .....</i>	<i>4</i>
2.5.1 <i>Evaluated Functionality .....</i>	<i>5</i>
2.5.2 <i>Non-evaluated Functionality and Services.....</i>	<i>6</i>
2.6 <i>Usage.....</i>	<i>6</i>
2.6.1 <i>Evaluated Configuration .....</i>	<i>6</i>
2.6.2 <i>Delivery procedures .....</i>	<i>7</i>
2.6.3 <i>Determining the Evaluated Configuration .....</i>	<i>8</i>
2.6.4 <i>Documentation.....</i>	<i>8</i>
2.6.5 <i>Secure Usage.....</i>	<i>8</i>
<b>5. Chapter 3 - Evaluation.....</b>	<b>10</b>
3.1 <i>Overview.....</i>	<i>10</i>
3.2 <i>Evaluation Procedures .....</i>	<i>10</i>
3.3 <i>Functional Testing.....</i>	<i>10</i>
3.4 <i>Penetration Testing.....</i>	<i>10</i>
3.5 <i>Certification Result.....</i>	<i>10</i>
3.6 <i>Assurance level .....</i>	<i>11</i>
3.7 <i>Recommendations.....</i>	<i>11</i>
<b>6. Annex A - References and Abbreviations.....</b>	<b>12</b>
A.1 <i>References .....</i>	<i>12</i>
A.2 <i>Abbreviations .....</i>	<i>13</i>

# Chapter 1 – Introduction

## Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

## Purpose

The purpose of this Certification Report is to:

- a) report the certification of results of the IT security evaluation of the TOE, Senetas CN Series Encryptor Range & CM Management Application Software against the requirements of the Common Criteria (CC) evaluation assurance level EAL2+, and
- b) provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target (Ref [1]) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

## Identification

The TOE is CN Series Encryptor Range & CM Management Application Software.

**Table 1 Identification Information**

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program.
TOE	Senetas CN Series Encryptor Range & CM Management Application Software
Hardware Models	A6040B, A6041B, A6042B, A6100B, A6101B, A6102B, A6010B, A6011B, A6012B, A4010B
Software Version	CN Series Application Software 2.4.0 which applies to all CN units. CM Management Series Application Software

	7.3.0
Security Target	Security Target for Senetas CN Series Encryptor Range & Senetas CM Management Application 5 August 2014.
Evaluation Level	EAL2+
Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1 Revision 4, CCIMB-2012-09-004, September 2012 with interpretations as of 11 March 2014.
Conformance	Common Criteria Part 2 Common Criteria Part 3 augmented (EAL2 + ALC_FLR.2).
Sponsor	Senetas, Level 1, 11 Queens Road, Melbourne, Victoria , Australia
Developer	Senetas, Level 1, 11 Queens Road, Melbourne, Victoria, Australia
Evaluation Facility	CSC Australia Pty Limited, 217 Northbourne Ave, Turner, ACT 2612

Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.6.1 Evaluated Configuration.

## **Chapter 2 - Target of Evaluation**

### **2.1 Overview**

This chapter contains information about the Target of Evaluation (TOE), including: a description of functionality provided; its architectural components; the scope of evaluation; security policies; and its secure usage.

### **2.2 Description of the TOE**

The TOE comprises of a management application and encryptors.

- a) The management application generates and installs X.509 certificates into the encryptors.
- b) The CN series encryptors are high-speed, standard based multi-protocol encryptors specifically designed to secure voice, data and video information transmitted over Fibre channel and Ethernet Networks. It connects to a Local Area Network (LAN) or Wide Area Network (WAN) using 10/100/1000 BaseT RJ45 or optical fibre connectors. The Senetas CN series Fibre Channel connects to Fibre Channel links to provide traffic encryption over point-to-point (link) network segments. The one interface provides Fibre Channel link encryption at 1, 2 and 4G to support future network upgrades. 1G and 10G Ethernet is also available.

### **2.3 Security Policy**

The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. The Security Target (Ref [1]) contains no explicit security policy statements.

### **2.4 TOE Architecture**

The TOE consists of the following major subsystems:

#### **Management Console Subsystem**

The management console subsystem provides a Graphical User Interface (GUI) for remote management of encryptors. It utilises encrypted SNMPv3 communications over an out-of band management interface or in-band via the local and network interfaces.

#### **Management Subsystem**

The management subsystem provides the following functionality:

- a) Creation and maintenance of the audit log
- b) Audit trail analysis and review
- c) Creation and maintenance of user files
- d) Identification and authentication of users
- e) Remote management using SNMPv3
- f) Local management using the RS232 console port
- g) Creation and maintenance of the Connection Identifier Table
- h) Random number generation for keys
- i) A real time clock
- j) 3-way messaging function
- k) Multicast/VLAN operations
- l) Running of self tests during start-up and
- m) Automatic destruction of keys and user passwords if either of the interface cards is removed

### **Local and Network Interface Subsystems**

Both the network and local interface subsystems convert the physical signal received from the network and translate it to a suitable logical format for the frame/cell /bit stream /packet to be processed by the encryptor.

### **Software Crypto subsystem**

The software crypto subsystem provides cryptographic support services to the management. The subsystem is built using the open source OpenSSL libraries, and provides such functionality as session key establishment, certification generation, authentication and provision of SNMP authentication and privacy services.

### **FPGA Crypto Subsystem**

The CN encryptors use a Field Programmable Gate Array (FPGA) to conduct encryption and decryption of protected traffic between encryptors. The cryptographic functions are performed at very high speed as the process occurs in hardware.

## ***2.5 Clarification of Scope***

The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]) and includes the following.

- a) Security Audit
- b) Cryptographic support
- c) User data Protection
- d) Identification and authentication
- e) Security management
- f) Protection of the TOE security functions
- g) TOE access and
- h) Trusted path channels.

### **2.5.1 Evaluated Functionality**

The TOE provides the following evaluated security functionality:

**a) Audit**

The TOE generates system events associated with the operations that occur in the encryptors. The results are stored in non-volatile memory and accessible to administrators either remotely using CM Management Application (SNMPv3) or via the console.

**b) Certificate Management.**

The TOE generates and installs X.509 Certificates into the encryptors. Signed X.509 certificates are used by the TOE to establish trusted communication channel between itself and other encryptors. Both encryptors must have a valid X.509 certificate, which has been signed by a Certificate Authority which is either an encryptor itself or a third party Certificate Authority (CA), to protect the confidentiality and integrity of transmitted information.

**c) Data exchange**

The TOE performs hardware or software based 128 or 256 bit AES encryption in Cipher Feedback Mode (CFB), Counter mode, or Galois Counter Mode on the internet frame payload or hardware based 256 bit AES encryption in CFB mode on the fibre channel payload and a user configurable portion of the header.

**d) Identification**

The TOE enforces identification and authentication prior to allowing an authorised administrator the ability to view or modify any TOE security attributes.

**e) Key Management**

The TOE manages all the necessary keys and mechanisms to support the cryptographic operations including public and private keys for the TOE.

**f) Information Flow Control**

The TOE determines the action to take on any given cell, frame or bit stream by examining the list of entries in the Connection Identifier (CI) Table. The possible actions the TOE can apply to the traffic flows matching CI entries are encrypt /decrypt, discard or bypass.

**g) Role Based Access**

The TOE can assign and control differing privilege levels to administrative users of the TOE, thereby controlling the attributes which each administrator can view, modify or delete. The TOE maintains the roles of administrator, supervisor and user.

**h) Secure Remote Management**

The TOE can encrypt SNMPv3 management data packets using 128-bit AES. The remote management session is initiated by the user via CM Management Application software on their workstation.

**i) Self protection**

The TOE will erase all key material and user passwords if the case is tampered. The TOE also runs self tests on start-up to verify the underlying functionality of the device is correct.

## **2.5.2 Non-evaluated Functionality and Services.**

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information Security Manual (ISM) (Ref [2]) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

## **2.6 Usage**

### **2.6.1 Evaluated Configuration**

This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in this defined evaluated configuration. Australian Government users should refer to the ISM (Ref [2]) to ensure that configuration meet the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

The TOE consists of the CN application Software version 2.4.0 loaded on the Encryptor Hardware Module and a single version of the CM management Software: 7.3.0.

The hardware models in scope for this evaluation are as follows. Ethernet and Fibre channel models have been identified as appropriate.

**Table 2 TOE Components (CN)**

CN ENCRYPTORS	
Identification	Description
A6040B	CN6040 1G ETHERNET + 1/2/4G Fibre Channel (SFP+RJ45) AC UNIT
A6041B	CN6040 1G ETHERNET + 1/2/4G Fibre Channel (SFP+RJ45) DC UNIT
A6042B	CN6040 1G ETHERNET + 1/2/4G Fibre Channel (SFP+RJ45) AC/DC UNIT
A6100B	CN6100 10G ETHERNET (XFP) AC UNIT
A6101B	CN6100 10G ETHERNET (XFP) DC UNIT
A6102B	CN6100 10G ETHERNET (XFP) AC/DC UNIT
A6010B	CN6010 1G ETHERNET (SFP+RJ45) AC UNIT
A6011B	CN6010 1G ETHERNET (SFP+RJ45) DC UNIT
A6012B	CN6010 1G ETHERNET (SFP+RJ45) AC/DC UNIT
A4010B	CN4010 1G ETHERNET UNIT

## 2.6.2 Delivery procedures

### Hardware

Shipment of units from Senetas to the user is via commercial courier company who will pick up from Senetas and deliver it directly to the customer.

After placing an order, Senetas will issue the Order Acknowledgement Form listing the assigned user order number, the model numbers, serial numbers and expected date of delivery. When items are received, the customer must ensure that the serial number on the outside of the packaging, the serial number attached to the encryptor itself and the number listed on the acknowledgement match.

The customer must also verify that the tamper proof seal on the outside of the unit is intact. If the seal is broken then the integrity of the encryptor cannot be assured and Senetas should be informed immediately.

### Software

A software upgrade notice will be sent to the user before shipping any software upgrades. It will list the user name, software maintenance agreement number, software identification number, software version number, a random shipment identification number and expected date of delivery.

A Shipment Identification Number label is attached to software media and it is sealed in an envelope and a tamper proof seal attached across the seal of the envelope before shipping any software upgrades.

The customer must verify the information in the Shipment Identification label matches the Software Upgrade Notice upon delivery. The customer must also verify that the tamper proof seal is intact. If the seal is broken or the information does not match, Senetas should be informed immediately.

### **2.6.3 Determining the Evaluated Configuration**

To ensure the hardware received is the evaluated product the customer must check the models received against the list of TOE hardware models defined in the Security Target [1]. In addition to verifying model numbers for hardware components, the software versions must also be verified by the recipient. Software versions can be checked using the 'version' command over the encryptors CLI.

### **2.6.4 Documentation**

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available upon request from Senetas:

- a) Senetas CN46 Series Encryptors Product Manual , Release 02 May 2014
- b) User Guidance: SafeNet Inc,CN46 Series Encryptors, User Guide, Document CN46\_ETH\_FC\_CM7 Release 02, May 2014

### **2.6.5 Secure Usage**

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met. The intended application of the TOE is to provide a secure tunnel(s) between trusted networks.

a) A.CM

The management console, CM is assumed to be located within control access facilities, which will aid in prevent unauthorised users from attempting to compromise the security functions of the TOE.

It is assumed that the CM will be installed on a computer with the following minimum system configuration:

- Windows NT 4.0 /2000s/XP or higher
- 166 MHz or higher speed processor
- 64 MB of memory
- Hard disk drive with a minimum of 5MB of available application space
- CD drive for installation
- SVGA or better display resolution
- Mouse or other pointing device
- Network adapter card and
- TCP/IP connectivity

b) A.Locate

It is assumed that the encryptor is located in a secure area at the boundary of the site to be protected. It is required to be in a secure area to ensure that the unit is not physically bypassed.

c) A.Admin

It is assumed that one or more administrators, together with other supervisors or operators, who are assigned as authorised users, are competent to manage the TOE and can be trusted not to deliberately abuse their privileges so as to undermine security.

d) A.Audit

It is assumed that appropriate audit logs are maintained and regularly examined. Without capturing security relevant events or performing regular examination of audit logs, a compromise of security may go undetected.

e) A.PrivateKey

Where CM is configured as the Certificate Authority (CA), it is assumed that a password used to protect the private key of the CM remote management station is restricted to Administrators.

f) A.Install

It is assumed that the encryptor is installed on the boundary of the protected and unprotected network. The encryptor needs to be installed on the boundary to ensure confidentiality of transmitted information.

In addition, the following organisational security policies must be in place:

a) P.Crypto

All encryption services including confidentiality, authentication, key generation, Must conform to standards specified in ISM and FIPs PUB 140-2.

b) P.Inflow

Traffic flow is controlled on the basis of the information in the Ethernet frame or Fibre Channel frame and the action specified in the Connection Identifier Table. Any Ethernet frame or Fibre Channel for which there is no CI entry is discarded by default. By default all Ethernet and Fibre frames are discarded.

This policy ensure that the correct protective action of bypass, discard or encrypt is applies to any given Ethernet Frame or Fibre Channel Frame received by the TOE.

c) P.Roles

Administration of the TOE is controlled through the definition of roles, which assign different privilege levels to different types of authorised users (administrators, supervisors and operators). The P.Roles policy ensures the administration of the TOE is performed in accordance with the concept of least privilege.

## **Chapter 3 - Evaluation**

### **3.1 Overview**

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

### **3.2 Evaluation Procedures**

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4 (Refs [4], [5] and [6]).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4 (CEM) (Ref [7]).

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [8], [9] and [10]).

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [11]) were also upheld.

### **3.3 Functional Testing**

To gain confidence that the developers testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining: test coverage; test plans and procedures; and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers. The evaluators have observed that the TOE does not maintain correct time and timestamps after a power reset. An updated Security Target was provided that states that the administrator should enter the time according to UTC 0 and then select the desired time zone to ensure correct time is maintained.

### **3.4 Penetration Testing**

The developer performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE.

### **3.5 Certification Result**

After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref [12]), the Australasian Certification Authority certifies the evaluation of CN Series Encryptor Range & Senetas CM

Management Application Software performed by the Australasian Information Security Evaluation Facility CSC. CSC has found that CN Series Encryptor Range & CM Management Application Software upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL2+.

Certification is not a guarantee of freedom from security vulnerabilities.

### **3.6 Assurance level**

EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain), and independent testing based upon more detailed TOE specifications.

### **3.7 Recommendations**

Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref [2]) and New Zealand Government users should consult the GCSB.

In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref [2]), the ACA also recommends that users and administrators:

- a) should operate the CM Management Application from a secure location.
- b) should enter the time according to UTC 0 and then select the desired time zone to ensure correct time is maintained.

# Annex A - References and Abbreviations

## A.1 References

1. ST – Security Target for Senetas CN Series Encryptor Range & CM Management Application, version 1.0, 5 Aug 2014
2. 2014 Australian Government Information Security Manual (ISM), Australian Signals Directorate, (available at [www.asd.gov.au](http://www.asd.gov.au)).
3. User Guidance: SafeNet Inc, CN46 Series Encryptors, User Guide, Document CN46\_ETH\_FC\_CM7 Release 02, May 2014
4. Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model September 2012 Version 3.1 Revision 4 Final CCMB-2012-09-001.
5. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2012 Version 3.1 Revision 4 Final CCMB-2012-09-002.
6. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2012 Version 3.1 Revision 4 Final CCMB-2012-09-003.
7. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2012 Version 3.1, Revision 4, CCMB-2012-09-004.
8. AISEP Policy Manual, APM, Version 4.0, August 2011, Defence Signals Directorate.
9. AISEP Certifier Policy, ACP. Version 4.0, August 2011, Defence Signals Directorate.
10. AISEP Evaluator Policy, AEP. Version 4.0, August 2011, Defence Signals Directorate.
11. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.
12. Evaluation Technical Report: Senetas CN Encryptor Range Evaluation Technical Report Version 1.0, 12 August 2014.

## ***A.2 Abbreviations***

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CA	Certification Authority
CC	Common Criteria
CEM	Common Evaluation Methodology
CFB	Cipher Feedback (Mode)
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FPGA	Field Programmable Gate Array
GCSB	Government Communications Security Bureau
NTP	Network Time Protocol
PP	Protection Profile
SFP	Small Form Factor Pluggable (Fibre connection context)
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TLS	Transport Layer Security
+	Augmented