Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report
2012/83

17 Dec 2012
Version 1.0

Amendment Record

Version	Date	Description
1.0	17/12/2012	Final release

Executive Summary

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

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.

The CS series encryptors are software based (non FPGA) store and forward packet processing encryptors designed to provide an integrated data security solutions for point to point or meshed Ethernet links up to 100 Megabits per second. The CS series has been designed to transparently and simply integrate into network architectures.

The CM management application is a Graphical User Interface (GUI) software package that runs on Windows platforms. It can act as a Certification Authority (CA) for signing X.509 certificates or alternatively supports the use of external CA PKI environments. It provides secure remote installation of X.509 certificates into the Senetas encryptors using SNMPv3, and is also used to securely manage the encryptors.

This report describes the findings of the IT security evaluation of Senetas CN/CS Encryptor Range & Senetas CM Management Application to the Common Criteria (CC) to 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 22 November 2012.

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

a) should operate the CM Management Application from a secure location.

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

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, CN/CS Series Encryptor Range & Senetas CM Management Application., 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/CS Series Encryptor Range & Senetas CM Management Application.

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program.
TOE	The Senetas CN/CS Series Encryptor Range & Senetas CM Management Application.
Hardware Models	A6040B; A6041B; A6042B; A6100B; A6101B; A6102B; A4201B; and A4203B.
Software Version	CN Series Application Software 2.2.0 which applies to all CN units. CS Series Application Software 2.2.0 which

	applies to all CS units. CN Management Series Application Software 7.1.0 which applies to all units.
Security Target	Security Target for Senetas CN/CS Series Encryptor Range & Senetas CM Management Application 22 November 2012.
Evaluation Level	EAL2+
Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1 Revision 3, CCIMB-2009-07-004, July 2009 with interpretations as of 3 August 2012.
Conformance	Common Criteria Part 2 extended. 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

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 two styles of 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 CN series Fibre Channel provides encryption over point to point (link) network segments. The same interface provides encryption at 1, 2 and 4 Gbps to support future network upgrades.

a) The CS series encryptor range connects to a LAN or WAN using 10/100 BaseT RJ45.The CS series is designed to be a cost effective solution to interconnect branch and head offices. It is compatible with the CN series encryptors and can operate in point to point and mesh configurations.

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:

a) **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.

b) **Management Subsystem**

The management subsystem provides the following functionality:

1) Creation and maintenance of the audit log;
2) Audit trail analysis and review;
3) Creation and maintenance of user files;
4) Identification and authentication of users;
5) Remote management using SNMPv3;
6) Local management using the RS232 console port;
7) Creation and maintenance of the Connection Identifier Table;
8) Random number generation for keys;
9) A real time clock;
10) 3-way messaging function;
11) Multicast/VLAN operations;
12) Running of self tests during start-up; and
13) Automatic destruction of keys and user passwords if either of the interface cards are 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.

CS Crypto Subsystem

The CS Crypto subsystem provides the encryption and decryption functionalities of the CS encryptor Range for traffic transmitted between encryptors. The subsystem is implemented in a software library and is configured by the Management Subsystem with user desired algorithms and associated parameters.

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 126 bit AES encryption in Cipher Feedback Mode (CFB), Counter mode, or Galois Counter Mode on the internet frame payload or hardware bases 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 2.2.0 loaded on the Encryptor Hardware Module; the CS application software version 2.2.0 loaded onto the Encryptor Hardware Module; and a single version of the CM management Software: 7.1.0.

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

Table 3 TOE Components (CS)

CS ENCRYPTORS	
Identification	**Description**
A4201B	A4201B CYPHERSTREAM ETHERNET 10M AC UNIT
A4203B	A4203B CYPHERSTREAM ETHERNET 100M AC 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. 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) CN and CS series Encryptors Product Manual release 02 Oct 2012 (Ref [3]).

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:

i. Windows NT 4.0 /2000sp or higher;
ii. 166 MHz or higher speed processor;
iii. 64 MB of memory;
iv. Hard disk drive with a minimum of 5MB of available application space;

v. CD drive for installation;
vi. SVGA or better display resolution;
vii. Mouse or other pointing device;
viii. Network adapter card; and
ix. 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 3 (Refs [4], [5] and [6]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 3 (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.

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/CS Series Encryptor Range & Senetas CM Management Application performed by the Australasian Information Security Evaluation Program CSC. CSC has found that CN/CS Series Encryptor Range & Senetas CM Management Application 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 [3]), the ACA also recommends that users and administrators:

a) should operate the CM from a secure location.

Annex A - References and Abbreviations

A.1 References

1. ST – Security Target for Senetas CN/CS Series Encryptor Range & Senetas CM Management Application, version 1.0, 22 November 2012

2. 2012 Australian Government Information Security Manual (ISM), Defence Signals Directorate, (available at www.dsd.gov.au).

3. User Guidance: Senetas CN and CS Series Encryptors Product Manual, Release 02, Oct 2012.

4. Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-001.

5. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-002.

6. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-003.

7. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-209-07-004.

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/CS Encryptor Range Evaluation Technical Report Version B.0 22 November 2012.

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	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TLS	Transport Layer Security
+	Augmented