Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2011/77

5 Sept 2011

Version 1.0

Amendment Record

Version	Date	Description
0.1	01/09/2011	Internal release.
0.2	05/09/11	Extended review.
1.0	07/09/2011	Public release.

Executive Summary

1 Senetas Ethernet Encryptor Range is a family of products of high-speed, standards based Ethernet encryptors specifically designed to secure voice, data and video information transmitted over Ethernet Networks. Senetas Ethernet Encryptor Range is the Target of Evaluation (TOE).

2 This report describes the findings of the IT security evaluation of Senetas' Senetas Ethernet Encryptor Range, to the Common Criteria (CC) evaluation assurance level EAL 4+ ALC_FLR.2. The report concludes that the product has met the target assurance level of EAL 4+ ALC_FLR.2 and that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by CSC and was completed on the 19th of August 2011.

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

a) The encryptors are located within controlled access facilities, to aid in preventing unauthorised users from attempting to compromise the security functions of the TOE;

b) Encryptors should be located on the border of the trusted and untrusted network and configured to encrypt, discard and bypass traffic based on information contained in the Connections Action Table (CAT);

c) While the encryptors provide VLAN encryption capabilities, they rely solely on the underlying infrastructure in the environment (i.e. switches and routers) to correctly enforce VLAN separation. It is therefore necessary to ensure that switches and other network infrastructure be configured securely to protect against VLAN hopping attacks.

d) One or more administrators, together with any 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; and

e) The appropriate audit logs are maintained and regularly examined.

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

5 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 (Ref [1]) and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

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

1.2 Purpose

7 The purpose of this Certification Report is to:

a) Report the certification of results of the IT security evaluation of the TOE: Senetas Ethernet Encryptor Range, against the requirements of the Common Criteria (CC) evaluation assurance level EAL 4+ ALC_FLR.2, and

b) Provide a source of detailed security information about the TOE for any interested parties.

8 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.

1.3 Identification

9 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.

Table 1: Identification Information

Item	**Identifier**
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Senetas Ethernet Encryptor Range
TOE Version	**CN Series Models** A5137B CN1000 Ethernet 100M (SFP+RJ45) AC UNIT A5139B CN1000 Ethernet 10M (SFP+RJ45) AC UNIT A5135B CN1000 Ethernet 1G (SFP) AC UNIT A5141B CN1000 Ethernet 1G (SFP+RJ45) AC UNIT A5203B CN3000 Ethernet 10G AC UNIT A5204B CN3000 Ethernet 10G DC UNIT **CS Series Models** A4201B CypherStream Ethernet 10M AC UNIT A4203B CypherStream Ethernet 100M AC UNIT
Security Target	Security Target for Senetas CN Series Ethernet Encryptor, Senetas CS Series Ethernet Encryptor, CypherManager. V3.0
Evaluation Level	EAL 4+ ALC_FLR.2
Evaluation Technical Report	CSC-EFC-T0069-ETR Issue 1.1, 19 August 2011.

Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. CCMB-2009-07-001, CCMB-2009-07-002, & CCMB-2009-07-003
Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1 Revision 3, CCMB-2009-07-004.
Conformance	CC Part 2 Conformant CC Part 3 Conformant Augmented with FLR_ALC.2
Developer	Senetas, Level 1, 11 Queens Road, Melbourne, Victoria, Australia
Evaluation Facility	CSC Australia Pty Ltd

Chapter 2 - Target of Evaluation

2.1 Overview

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

2.2 Description of the TOE

11 The TOE is the Senetas Ethernet Encryptor Range developed by Senetas. This consists of:

- CN Series Ethernet encryptors;
- CS Series Ethernet encryptors; and
- CypherManager

12 These are high-speed, standards based multi-protocol encryptors specifically designed to secure voice, data and video information transmitted over Ethernet networks. It can be deployed within networks employing data rates up to 10 Gigabits per second and provides support for AES algorithms. The encryptors also provide access control facilities using access rules for each defined connection. Plug in interface cards enable the encryptors to be customised in the field for connection to the required network.

13 The Senetas CN Series Ethernet Encryptor connects to the Local Area Network (LAN) or Wide Area Network (WAN) using 10/100/1000 Base T RJ45 or Optical Fibre connectors. When operating at full bandwidth, the

encryptor will not discard any valid Ethernet frames for all modes of operation.

14 The Senetas CS series encryptor connects to the Local Area Network (LAN) or Wide Area Network (WAN) using 10/100 BaseT RJ45. The Senetas CS encryptor is specifically designed to be a cost-effective solution to interconnect branch and head offices. It is compatible with Senetas CN series encryptors and can operate in both point – point and mesh configurations.

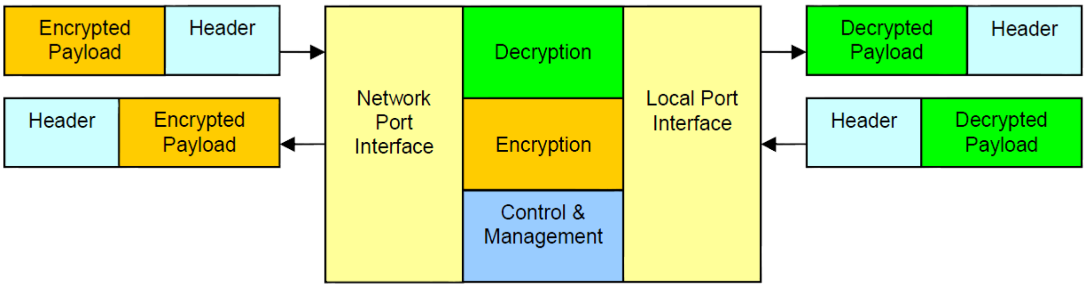

Figure 1 – Senetas Ethernet Encryptor Range block diagram

15 The encryptors provide access control and authentication between secured sites and confidentiality of transmitted information by cryptographic mechanisms (see Figure 1 – Senetas Ethernet Encryptor Range block diagram). The encryptors can be added to an existing network with complete transparency to the end user and network equipment. An example installation of a Senetas CN Ethernet encryptor is shown in Figure 2 - Ethernet Security Solution.

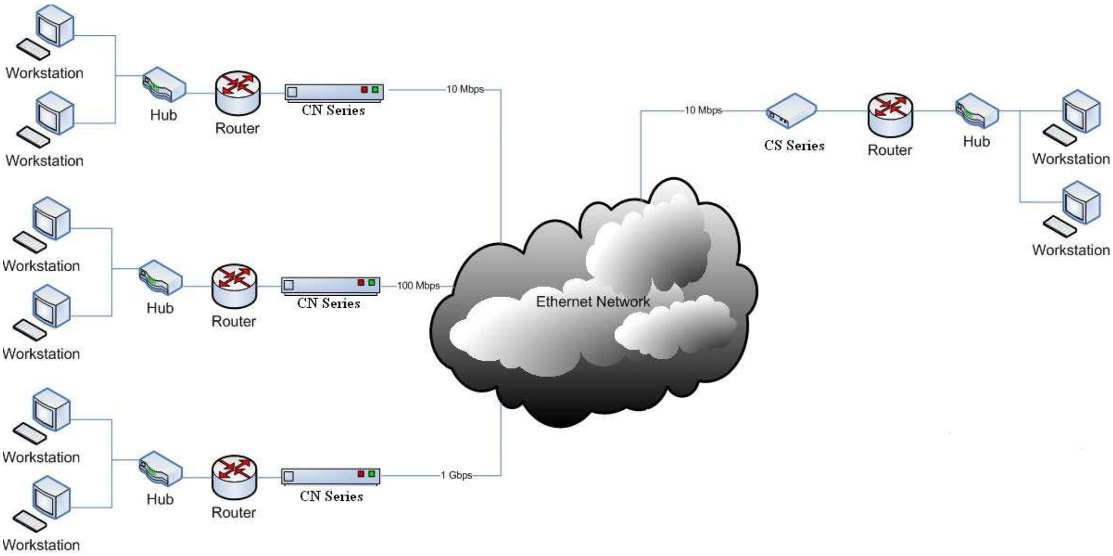

Figure 2 - Ethernet Security Solution

16 The Senetas Encryptors can be remotely managed securely by using CypherManager, a SNMPv3 compliant management station. Remote management sessions connect to the encryptor through the dedicated front panel Ethernet port or logically via the local or network interfaces. The

encryptors can also be managed locally through the RS232 console port supporting a Command Line Interface (CLI).

17 The encryptors support different types of user roles with different privileges according to a set of pre-defined roles. The three defined roles are Administrator, Supervisor and Operator. Only the Administrator has unrestricted access to the security features of the encryptor. Only Administrators can activate X.509 certificates that are required for the encryptor to commence operation.

18 The encryptors provide an audit capability to support the effective management of the security features of the device. The audit capability records all management activity for security relevant events.

19 The TOE provides the following security functionality:

a) Audit - The TOE is able to generate auditable data for security relevant events;

b) Certificate Management - certificates will be maintained for the use by the product;

c) Protected Data Exchange - the confidentiality of packets sent over the untrusted network will be maintained;

d) Identification and Authentication - of administrative users who are responsible for the configuration and monitoring of the TOE;

e) Key Management - will be used in implementing security functions;

f) Information Flow Control - controlling the flow of received Ethernet frames from external hosts;

g) Role-Based Access Control - restriction of users to different configuration interfaces based on the role they are assigned;

h) Secure Remote Management - remote administration by Cypher-Manager allows for secure management and configuration of the TOE; and

i) Self Protection - the TOE will protect against unauthorised access to the physical security of the TOE.

2.3 Security Policy

The Security Target (Ref [1]) contains no explicit security policy models for the TOE.

2.4 TOE Architecture

20 The TOE is comprised of several major subsystems. The major subsystems defined within the TOE Design Specification are as follows:

2.4.1 Management Console Subsystem

21 The Management Console subsystem provides a Graphical User Interface (GUI) for remote management of encryptors. The Management Console subsystem utilises encrypted SNMPv3 communications over either an out-of-band management interface or in-band via the local and network interfaces. The required software is described in the Assumption "A.CypherManager".

2.4.2 Management Subsystem

22 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 profiles;

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 Action Table (CAT);

h) Random number generation for keys;

i) A real time clock;

j) 3-way messaging function;

k) Multicast/VLAN operation;

l) Running of self-tests during start-up; and

m) Automatic destruction of keys and user passwords if either of the interface cards are removed.

2.4.3 Local and Network Interface Subsystems

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

2.4.4 FPGA Crypto Subsystem

24 The CN Series Ethernet 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 purely in hardware.

2.5 Clarification of Scope

25 The evaluators consider the application of the TOE in its intended environment and security functionality provided by the TOE to be clearly defined within the Security Target (Ref [1]). As a point of clarification; unlike other encryption devices which provide Layer 3 encryption and may contain built in replay protection, the Encryptors are Layer 2 encryption devices that do not provide or claim protection against replay of legitimate traffic. The Encryptors are simply designed to provide high performance confidentiality of data transmitted across un-trusted networks.

26 Additionally, while the encryptors provide VLAN encryption capabilities, they rely solely on the underlying infrastructure in the environment (i.e. switches and routers) to correctly enforce VLAN separation. As such, you should consider the threats identified in the Security Target (Ref [1]) to be a complete list of threats a consumer would expect to be countered by the TOE.

2.5.1 Evaluated Functionality

27 The TOE provides the following evaluated security functionality:

a) Ethernet Processing;

b) Audit;

c) Certificate Management;

d) Data Exchange;

e) Identification;

f) Key Management;

g) Information Flow Control;

h) Role Based Access;

i) Secure Remote Management; and

j) Self Protection.

2.5.2 Non-evaluated Functionality

28 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

29 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 the configuration meets the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

30 The following encryptor application software versions and CypherManager versions apply to this evaluation:

Description	Version
CN Series Ethernet Application Software	4.0.2
CS Series Application Software	2.0.2
CypherManager	6.6.0

31 The Developer's Architectural Design identifies the following components of the TOE:

2.6.1.1 Senetas CN Series Models

ID	Description
A5137B	CN1000 Ethernet 100M (SFP+RJ45) AC Unit
A5139B	CN1000 Ethernet 10M (SFP+RJ45) AC Unit
A5141B	CN1000 Ethernet 1G (SFP+RJ45) AC Unit
A5135B	CN1000 Ethernet 1G (SFP) AC Unit
A5203B	CN3000 Ethernet 10G AC Unit
A5204B	CN3000 Ethernet 10G DC Unit

2.6.1.2 Senetas CS Series Models

ID	Description
A4201B	CypherStream Ethernet 10M AC Unit
A4203B	CypherStream Ethernet 100M AC Unit

2.6.2 Delivery procedures

32 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated version. They should then receive the correct hardware and software.

2.6.2.1 Senetas Hardware

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

34 After placing an order, Senetas will issue an Order Acknowledgement Form listing the assigned user order number, the model number(s), serial number(s) 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.

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

2.6.2.2 Senetas Software

36 Before shipping any software upgrades, a Software Upgrade Notice will be sent to the user. The software upgrade notice 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.

37 Before shipment of the software, a Shipment Identification Number label is attached to the software media, the software media is sealed in an envelope and a tamper proof seal is attached across the flap of the envelope.

38 Upon delivery, the customer must verify the information in the Shipment Identification label matches the Software Upgrade Notice. 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 Verifying the Evaluated Product

39 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 (Ref [1]).

40 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 encryptors CLI.

2.6.4 Product Installation

41 Installation, generation and start up of the TOE, such that the TOE is in the evaluated configuration is detailed in the corresponding user guidance

documentation (ref [3]). These documents provide comprehensive installation and configuration instructions and identify considerations for the initiation of traffic flow in specific configurations. The documents are delivered to the customer along with the TOE during the standard shipment process.

2.6.5 Documentation

42 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is provided with the TOE:

a) Senetas Encryption Product Manual, Release 140, December 2010 (Ref [3]).

43 The Senetas Encryption Product Manual (Ref [3]) describes the processes and other relevant information for the secure installation and operation of the Encryptors. Additionally this document describes the usage assumptions and details the technical information regarding the TOE's use.

2.6.6 Secure Usage

44 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.

45 Section 3.1: 'Assumptions' in the Security Target (Ref [1]) provides a full description of the assumptions. Assumptions are made in the following areas:

a) Physical security;

b) Configuration;

c) Administrators;

d) Restricted access to private key; and

e) Installation.

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

a) All encryption services including, confidentiality, authentication, key generation and key management, must conform to standards specified in FIPS PUB 140-2 and the ISM.

b) Traffic flow is controlled on the basis of the information in the Ethernet frame and the action specified in the Connection Action Table. Any Ethernet frame for which there is no CAT entry, is discarded. By default, all Ethernet frames are discarded. The P.INFOFLOW OSP ensures that the correct protective action of bypass, discard or encrypt is applied to any given Ethernet frame received by the TOE.

c) 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 OSP ensures that administration of the TOE is performed in accordance with the concept of least privilege.

Chapter 3 - Evaluation

3.1 Overview

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

3.2 Evaluation Procedures

48 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation (Refs [4], [5], [6]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) (Ref [7]). The evaluation was also carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [8] & [11]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [12]) were also upheld.

3.3 Functional Testing

49 To gain confidence that the developer's 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. Independent evaluator testing was conducted at CSC's AISEF Laboratory at 217 Northbourne Avenue, Turner ACT.

50 The evaluators conducted independent and penetration testing between the 23rd May 2011 and the 17th of August 2011. The test cases were developed in accordance with the National Association of Testing Authorities (NATA) requirements defined in section 5.4 of ISO/IEC 17025. In terms of selecting the hardware and software sample to undergo independent evaluator testing the evaluators considered the following factors in selecting the test sample.

a) The TOE hardware consists of both AC and DC variations. The examination of the TOE; and

b) The design demonstrated that there is no difference between AC and DC encryptor models in terms of the TSF and its implementation;

51 The following table identifies the hardware platforms and software versions selected for independent testing based on the factors identified

above. As such the evaluators tested the following models to cover a significant sample of defined security functionality:

ID	Description	Version
A5141B	CN1000 Ethernet 1G (SFP+RJ45) AC Unit (CN1000)	4.0.2
A4203B	CypherStream Ethernet 100M AC Unit (CS100)	2.0.2
A4201B	CypherStream Ethernet 10M AC Unit (CS10)	2.0.2
N/A	CypherManager	6.6.0

52 As a result of the factors described above the test sample in relation to hardware models allowed the number of models tested to be minimised to three of a possible eight available. Given the similarities in implementation across models, the evaluators consider that this is a reasonable sample of TOE models.

53 In terms of the sample of developer tests to be repeated by the evaluators the evaluators examined the test plans produced by the developer and noted the following factors in selecting the developer sample to repeat

a) The configurations used by the evaluators were identical to that of the developers; and

b) The aims and objectives of each evaluators test matched the aims and objectives of each developer test.

3.4 Penetration Testing

54 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. This analysis included a search for possible vulnerability sources in publicly available information such as:

- Milw0rm - http://www.milw0rm.com
- Security Focus - http://www.securityfocus.com
- Secunia - http://www.secunia.com
- Packetstorm Security - http://www.packetstormsecurity.org.

55 Given the nature of the product and the absence of similar products, the evaluators considered it unlikely public domain exploits or vulnerabilities specifically targeting the product would be identified. The evaluators confirmed this hypothesis via the search identified above and therefore focused their efforts on the technologies employed by the TOE, including the underlying network protocols and open source software used in the TOE.

56 The analysis conducted by the evaluators and the subsequent testing indicated that the TOE will resist an attacker with an attacker potential consistent with the requirements of an EAL 4+ ALC_FLR.2 assurance level.

Chapter 4 - Certification

4.1 Overview

57 This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen and recommendations made by the certifiers.

4.2 Certification Result

58 After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref [13]), the Australasian Certification Authority certifies the evaluation of Senetas Ethernet Encryptor Range performed by the Australasian Information Security Evaluation Facility, CSC.

59 CSC has found that Senetas Ethernet Encryptor Range upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL 4+ ALC_FLR.2.

60 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Assurance Level Information

61 EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE and a subset of the implementation, to understand the security behaviour. Assurance is additionally gained though an informal model of the TOE security policy.

62 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for obvious vulnerabilities and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

63 EAL4 also provides assurance though the use of development environment controls and additional TOE configuration management including automation and evidence of secure delivery procedures.

64 ALC_FLR.2 is the flaw remediation procedures documents the procedures used to track all security flaws from the initial detection through to the resolution of the flaw.

65 The flaw remediation procedures provide a mechanism for ensuring each flaw contains a description in terms of its nature and effect and resolution

status. The procedures also ensure a corrective action is provided for each identified security flaw. Resolution actions include documentation releases, patch releases and maintenance releases.

4.4 Recommendations

66 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.

67 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:

a) The TOE is used only in its evaluated configurations;

b) The encryptors are located within controlled access facilities, to aid in preventing unauthorised users from attempting to compromise the security functions of the TOE;

c) Encryptors should be located on the border of the trusted and untrusted network and configured to encrypt, discard and bypass traffic based on information contained in the Connections Action Table (CAT);

d) While the encryptors provide VLAN encryption capabilities, they rely solely on the underlying infrastructure in the environment (i.e. switches and routers) to correctly enforce VLAN separation. It is therefore necessary the need to ensure that switches and other network infrastructure be configured securely to protect against VLAN hopping attacks.

e) One or more administrators, together with any 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; and

f) The appropriate audit logs are maintained and regularly examined.

Annex A - References and Abbreviations

A.1 References

[1] Senetas CN Series Ethernet Encryptor, Senetas CS Series Ethernet Encryptor, CypherManager, CypherNet-Security-Target, Version 3.0, August 2011.

[2] Australian Government Information Security Manual (ISM), November 2010, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] Senetas Encryption Product Manual, Release 140, December 2010.

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, version 3.1 Revision 3, July 2009, CCMB-2009-07-001.

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, version 3.1 Revision 3, July 2009, CCMB-2009-07-002.

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, version 3.1 Revision 3, July 2009, CCMB-2009-07-003.

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

[8] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.1, 29 September 2006, Defence Signals Directorate.

[9] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.1, 29 September 2006, Defence Signals Directorate.

[10] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.1, 29 September 2006, Defence Signals Directorate.

[11] AISEP Publication No. 4 – Sponsor and Consumer Guidance, AP 4. Version 3.1, 29 September 2006, Defence Signals Directorate.

[12] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000

[13] Senetas Ethernet Encryptor Range Evaluation Technical Report, CSC-EFC-T0069-ETR, Version 1.0, 19 August 2011.

A.2 Abbreviations

AC	Alternating Current
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CAT	Connections Action Table
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
DC	Direct Current
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
GCSB	Government Communications Security Bureau
GUI	Graphical User Interface
ISM	Information Security Manual
LAN	Local Area Manager
NATA	National Association of Testing Authorities
OSP	Organisational Security Policy
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SMNPv3	Simple Network Manager Protocol version 3
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
VLAN	Virtual Local Area Network
WAN	Wide Area Manager