Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2008/46

6 June 2008

Version 1.0

Amendment Record

Version	Date	Description
1.0	06/06/2008	Final version – public release

Executive Summary

1 Senetas CypherNET Multi-Protocol Encryptor is the Target of Evaluation (TOE).

2 It is a high speed, standards based multi-protocol encryptor that is designed to protect the confidentiality of voice, data and video information transmitted over Synchronous Optical/Synchronous Digital Hierarchy (SONET/SDH), Asynchronous Transfer Mode (ATM), Ethernet networks and protocol independent point-to-point data networks. The TOE supports data rates of up to 10 Gigabits per second.

3 This report describes the findings of the IT security evaluation of the TOE and concludes that it meets the target assurance level of EAL 4 of the Common Criteria Standard. 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 Australia Pty Limited and was completed in April 2008.

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

a) used only in its evaluated configuration, ensuring that the assumptions concerning the TOE security environment, and organisational security policies (Ref [1]) are fulfilled; and

b) operated according to the administrator guidance document (Ref [3]).

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

6 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

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

1.2 Purpose

8 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, Senetas CypherNET Multi-Protocol Encryptor, against the requirements of the Common Criteria (CC) evaluation assurance level EAL 4; and

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

9 This report should be read in conjunction with the TOE 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

10 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 CypherNET Multi-Protocol Encryptor
Software Version	The TOE consists of two versions of CypherNET Application Software versions 1.7.0 and 1.7.5 loaded onto the applicable Encryptor Hardware model and CypherManager Software Version 6.3.0.
Security Target	Security Target for CypherNET Multi-Protocol Encryptor, Version 1.18, February 2008.
Evaluation Level	EAL 4
Evaluation Technical Report	Evaluation Technical Report for CypherNET Multi-Protocol Encryptor Version 2.0, April 2008
Criteria	CC Version 2.1, August 1999, with interpretations as of 4 September 2002.
Methodology	CEM-99/045 Version 1.0, August 1999, with interpretations as of 4 September 2002.
Conformance	CC Part 2 Conformant CC Part 3 Conformant
Sponsor	Senetas Security Pty Ltd
Developer	Senetas Security Pty Ltd
Evaluation Facility	CSC Australia Pty Limited

Chapter 2 - Target of Evaluation

2.1 Overview

11 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

12 The TOE comprises both hardware (CypherNET) and software (CypherManager) developed by Senetas Security Pty Limited. The CypherNET Multi-Protocol Encryptor uses 3DES and AES encryption to provide confidentiality of voice, data and video information transmitted over Synchronous Optical/Synchronous Digital Hierarchy (SONET/SDH), Asynchronous Transfer Mode (ATM), and Ethernet Networks and protocol independent point-to-point data networks at data rates up to 10 Gigabits per second. It also provides access control facilities using access rules for each defined SONET/SDH, ATM, Ethernet, or link connection.

13 The CypherManager client application employs the SNMP v3 protocol for secure remote management of the CypherNET Hardware devices. The TOE provides the following security features:

a) Industry standard cryptography to protect the confidentiality of network traffic transmitted across an untrusted link;

b) Internal management of cryptographic keys;

c) Secure remote management using the SNMPv3 protocol;

d) Audit;

e) Identification and Authentication of administrative users; and

f) Self protection against physical tampering of the CypherNET encryptors.

2.3 Security Policy

14 The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. The TSP is composed of several implicit and explicit policies. The TOE explicitly enforces Information Flow Control and Access Control Security Function Policies (SFPs), defined in the Security Target (Ref [1]). A summary of the Security Policies is provided below.

2.3.1 Information Flow Control Security Function Policy

15 The Information Flow Control SFP defines the flow of information based on attributes stored within the Connection Action Table (CAT). The policy enables administrators to enforce a confidentiality policy by dictating the action traffic can take through the TOE. The permissible actions are:

a) Bypass – transmit or receive traffic in clear text;

b) Encrypt – encrypted and transmitted to a peer encryptor; and

c) Discard - prevent forwarding the traffic any further.

2.3.2 Management Access Console Policy

16 The Management Access Console Policy enforces role based access on the console management interface used to administer the TOE. This policy also enforces identification and authentication over this management interface. The following user classes for identification and authentication are supported by the TOE:

a) Administrators – Administrators have complete access to the management functionality of the TOE.

b) Supervisors – Supervisors are able to view all configurations parameters, the audit log, change the system time, modify the CAT table and modify a restricted subset of configuration parameters.

c) Operators – Operators are only able to view the configuration of the TOE.

2.3.3 Management Access SNMP Policy

17 The Management Access SNMP Policy enforces role based access on the SNMPv3 management interface used to administer the TOE. The same user classes and restrictions described in Section 2.3.2 are applicable within this policy. This policy enforces authentication to the TOE and confidentiality of management traffic via the SNMPv3 protocol.

2.3.4 Encryptor Authentication Security Function Policy.

18 The Encryptor Authentication SFP defines the process of peer encryptor mutual authentication used during the process of cryptographic tunnel establishment. This policy governs the key exchange that takes place based on X.509 certificate authentication and RSA key exchange. Each encryptor has a signed certificate from a trusted CA (in the case of the TOE CypherManager fulfils this role). These certificates provide mutual authentication for encryptors within the network.

2.3.5 Certificate Enrolment Security Function Policy

19 The Certificate Enrolment SFP defines the process of installing certificates on to an encryptor as it is commissioned. This policy requires the hashes to be validated on the encryptors to ensure the certificate installation process has not been compromised.

2.3.6 Self Protection Security Function Policy

20 The Self Protection SFP defines the processes employed by the TOE to protect it from tampering. When a network card or the case is removed from an encryptor unit the encryption key used to encrypt passwords and session encryption keys on the encryptor is erased. This erasure renders the stored session encryption keys and passwords inaccessible.

2.3.7 Self Test Security Function Policy

21 The Self Test SFP enforces self testing of TOE hardware and software when the TOE is turned on. The Self Test policy ensures the correct operation of the TOE prior to it being operable. Should the self test fail the policy dictates the TOE fail into a secure state where no traffic is passed through the device.

2.3.8 Audit Security Function Policy

22 The Audit SFP defines the events that are audited during the operation of the TOE. This policy audits all modifications to the values of TSF data, the result of self testing and any failures of self testing.

2.4 TOE Architecture

23 The TOE consists of the following major architectural subsystems:

a) **CypherManager Subsystem.** This subsystem, which connects via an internal interface to the Ethernet port on the front panel or in-band via the local and network interfaces, enables secure remote management of CypherNET using SNMPv3 commands via a graphical user interface. All SNMPv3 commands are authenticated and can be encrypted.

b) **Management Subsystem.** This subsystem provides the following functionality:

i) Creation and maintenance of the audit log;

ii) Audit trail analysis and review;

iii) Creation and maintenance of user profiles;

iv) Identification and authentication of users;

v) Remote management using SNMPv3;

vi) Local management using the RS232 console port;

vii) Creation and maintenance of the Connection Action Table (CAT);

viii) Random number generation for keys;

ix) A real time clock;

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

xi) Automatic destruction of keys and user passwords if either of the interface cards is removed.

c) **Software Cryptographic Subsystem**. This subsystem provides cryptographic support services to the management subsystem implemented in software. The software cryptographic subsystem is built using the open source openssl libraries.

d) **Low-Speed Cryptographic Subsystem** This subsystem provides low speed traffic encryption implemented in hardware, and used in the low speed Ethernet and Link encryptor products.

e) **High-Speed SONET/SDH Cryptographic Subsystem.** This subsystem provides high speed encryption implemented in hardware for SONET/SDH traffic in the SONET encryptors.

f) **High-Speed ATM Cryptographic Subsystem**. This subsystem provides high speed encryption implemented in hardware for ATM traffic in the ATM encryptors.

g) **High Speed Ethernet Cryptographic Subsystem** This subsystem provides high speed encryption implemented in hardware for ethernet traffic in the ethernet encryptors.

h) **Local and Network Interface Subsystem**. Both the network and local interface subsystems convert the physical signal received from the network and translate it into a suitable logical format for the frame/cell/bit stream/packet to be processed by the encryptor.

2.5 Clarification of Scope

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

25 Unlike other encryption devices which provide Layer 3 encryption and may contain built in replay protection, the TOE is a Layer 2 encryption device that does not provide or claim protection against the replay of legitimate traffic. The TOE is designed to provide high performance

confidentiality of data transmitted across untrusted networks. As such, the threats identified in the Security Target (Ref [1]) are considered to be a complete list of threats a consumer would expect to be countered by the TOE.

2.5.1 Evaluated Functionality

26 The TOE provides the following evaluated security functionality:

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.

2.5.2 Unevaluated Functionality

27 Potential users of the TOE are advised that some functions and services may not have 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 the Australian Government Information and Communications Technology Security Manual (ACSI 33) (Ref [2]) for policy relating to using an evaluated product in an unevaluated configuration. New Zealand Government users should consult the New Zealand Information and Communications Technology Security Manual (NZSIT 400 Series) (Ref [12]).

28 Potential users of the TOE should note that the use of the USB port which provides the capability to backup and restore configuration data, as well as upgrade the TOE, is outside the scope of this evaluation. While a PIN code is required to access this functionality, there is no capability to authenticate the administrator conducting this task. Therefore, it is recommended that these functions be conducted via the network interface which is fully audited and within scope of the evaluation.

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 these defined evaluated configurations. Australian Government users should refer to ACSI 33 (Ref [2]) to ensure that configurations meet the minimum Australian Government policy requirements. New Zealand Government users should refer to NZSIT 400 Series (Ref [12]).

30 The TOE consists of two versions of CypherNET application software (Versions 1.7.0 and 1.7.5) loaded onto the applicable encryptor hardware models as shown below, and a single version of CypherManager software (Version 6.3.0) which is applicable to all models.

31 The TOE also consists of the following hardware models categorised into SONET, ATM, LINK and Ethernet devices, and listed along with the applicable CypherNET application software version:

- **SONET – CypherNET Application Software 1.7.0**

  A2141B001 - CYPHERNET SONET OC3/OC12/OC48 AC Unit
  A2142B001 - CYPHERNET SONET OC3/OC12/OC48 DC Unit
  A2201B001 - CYPHERNET SONET OC192 DC Unit

- **ATM – CypherNET Application Software 1.7.0**

  A2111B001 - CYPHERNET ATM E1 AC Unit
  A2113B001 - CYPHERNET ATM E1/T1 AC Unit
  A2115B001 - CYPHERNET ATM E3/T3 AC Unit
  A2121B001 - CYPHERNET ATM OC3 Single Mode 15KM AC Unit
  A2123B001 - CYPHERNET ATM OC3 Single Mode 40KM AC Unit
  A2125B001 - CYPHERNET ATM OC3 Multi-Mode 2KM AC Unit
  A2127B001 - CYPHERNET ATM OC3 Single Mode 15KM & Single Mode 40KM AC Unit
  A2129B001 - CYPHERNET ATM OC3 Multi-Mode 2KM & Single Mode 15KM AC Unit
  A2109B001 - CYPHERNET ATM OC3 Multi-Mode 2KM & Single Mode 40KM AC Unit
  A2117B001 - CYPHERNET ATM OC12 Single Mode 15KM AC Unit
  A2119B001 - CYPHERNET ATM OC12 Single Mode 40KM AC Unit

A2107B001 - CYPHERNET ATM OC12 Single Mode 15KM & Single Mode 40KM AC Unit

A2112B001 - CYPHERNET ATM E1 DC Unit

A2114B001 - CYPHERNET ATM E1/T1 DC Unit

A2116B001 - CYPHERNET ATM E3/T3 DC Unit

A2122B001 - CYPHERNET ATM OC3 Single Mode 15KM DC Unit

A2124B001 - CYPHERNET ATM OC3 Single Mode 40KM DC Unit

A2126B001 - CYPHERNET ATM OC3 Multi-Mode 2KM DC Unit

A2128B001 - CYPHERNET ATM OC3 Single Mode 15KM & Single Mode 40KM DC Unit

A2130B001 - CYPHERNET ATM OC3 Multi-Mode 2KM & Single Mode 15KM DC Unit

A2110B001 - CYPHERNET ATM OC3 Multi-Mode 2KM & Single Mode 40KM DC Unit

A2118B001 - CYPHERNET ATM OC12 Single Mode 15KM DC Unit

A2120B001 - CYPHERNET ATM OC12 Single Mode 40KM DC Unit

A2108B001 - CYPHERNET ATM OC12 Single Mode 15KM & Single Mode 40KM DC Unit

- **LINK – CypherNET Application Software 1.7.0**

  A2131B001 - CYPHERNET LINK E1 AC Unit

  A2133B001 - CYPHERNET LINK X.21/V.11 AC Unit

  A2132B001 - CYPHERNET LINK E1 DC Unit

  A2134B001 - CYPHERNET LINK X.21/V.11 DC Unit

- **ETHERNET – CypherNET Application Software 1.7.5**

  A2101B002 - CYPHERNET ETHERNET 1G AC Unit

  A2103B001 - CYPHERNET 10/100 BASE-TX AC Unit

  A2102B002 - CYPHERNET ETHERNET 1G DC Unit

  A2104B001 - CYPHERNET 10/100 BASE-TX DC 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 product. They will receive an order acknowledgement. This order acknowledgement details the process that should be undertaken by the end user to ensure they receive the TOE in a secure fashion, free from tampering or masquerading.

33 The order acknowledgement states the end user should:

a) Take note of the expected date of delivery;

b) Confirm the tamper proof seals remain sealed; and

c) Ensure the serial numbers on the acknowledgement match those on the received item. The consumer is able to verify that they have received the evaluated product by checking the model number on either the underside of the encryptor unit, the LCD display panel on the front of the unit or by logging into the unit.

34 If during delivery of the TOE there is any deviation in the above procedure, it is recommended that the customer contact the vendor for further advice.

2.6.3 Determining the Evaluated Configuration

35 The evaluated configuration may be confirmed by logging into the TOE and confirming the version numbers.

2.6.4 Documentation

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

a) Senetas CypherNET Product Manual version 1.4[3].

37 The CypherNET Product manual describes the processes and other relevant information for the secure installation and operation of the Senetas CypherNET Multi-Protocol Encryptor. Additionally, this document describes the usage assumptions and details the technical information regarding the TOE's use.

2.6.5 Secure Usage

38 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.

39 The TOE is intended for use by organisations that need to provide confidentiality of information transmitted over SONET/SDH, ATM, Ethernet and protocol independent networks, and access control to prevent unauthorised connection to the protected network. The following is a summary of the assumptions for the operating environment of the TOE:

a) CypherManager is located within controlled access facilities, which will aid in preventing unauthorised users from attempting to compromise the security functions of the TOE. For example, unauthorised physical access to the CA private key used to sign X.509 certificates.

b) CypherNET is located in a secure area at the boundary of the site to be protected to ensure that the unit is not physically bypassed. It is assumed that CypherNET is installed on the boundary of the protected and unprotected network to ensure confidentiality of transmitted information.

c) The administrators are competent to manage the TOE, and can be trusted not to abuse their privileges or undermine security.

d) Appropriate audit logs are maintained and regularly examined. Without capturing security relevant events or performing regular examination of audit records, a compromise of security may go undetected.

e) A password used to protect the private key of the CypherManager remote management station is restricted to Administrators.

40 In addition, the following organisational security policies must be created:

a) All encryption services including confidentiality, authentication, key generation and key management, must conform to standards specified in FIPS PUB 140-2 and ACSI33.

b) Traffic flow is controlled on the basis of the information in the SONET/SDH header, ATM cell header or Ethernet frame and the action specified in the Connection Action Table. Any SONET/SDH payloads, ATM cells, Ethernet frame or bit stream for which there is no CAT entry, are discarded. By default, all SONET/SDH payloads, ATM cells, Ethernet frames or bit streams are discarded.

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).

Chapter 3 - Evaluation

3.1 Overview

41 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

42 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] and [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] and [9]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [10]) were also upheld.

3.3 Functional Testing

43 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 included developer test plans and results, as well as developer coverage and depth analysis. 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.

44 In addition, a number of independent tests were conducted by the evaluators. These included:

a) Console interface user roles,

b) SNMP interface user roles,

c) Ethernet encryption,

d) Tamper detection mechanism,

e) Audit log generation,

f) Discard traffic,

g) Secure remote management,

h) Cryptographic validation,

i) Unsuccessful Login Lockout,

j) Unattended Session Logout,

k) Self testing,

l) Reliable time source,

m) Failure with Secure State,

n) SONET Encryption,

o) Upgrade privilege, and

p) Software Cryptographic Operation.

3.4 Penetration Testing

45 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 its intended environment. This analysis included a search for possible vulnerability sources in publicly available information such as:

a) Milw0rm - http://www.milw0rm.com;

b) Security Focus - http://www.securityfocus.com;

c) Secunia - http://www.secunia.com; and

d) Packetstorm Security - http://www.packetstormsecurity.org.

46 Given the nature of the product and the absence of similar products, the evaluators also focused their efforts on the technologies employed by the TOE. The evaluators considered it unlikely they would find public domain exploits or vulnerabilities to specifically exploit this product. The search described above confirmed this hypothesis. As an alternative the evaluators concentrated on the underlying network protocols and open source software used in the TOE.

47 Following the evaluator's search for vulnerabilities it was determined that the Ethernet products were most susceptible to vulnerabilities exploitable by an attacker at an EAL 4 attack potential. This is due to the following factors:

a) Ethernet is the most common network technology people have access to;

b) An abundance of public domain tools and literature is readily available in relation to exploiting ethernet networks; and

c) Lack of public domain information regarding exploiting protocols such as ATM and SONET/SDH, and where an exploit was identified it required significant time and effort to exploit and was therefore considered out of scope for an EAL 4 evaluation.

48 The evaluators focused their efforts on the 1G Ethernet Encryptors configured in multipoint mode undertaking penetration tests in the following categories:

a) Flow control policy;

b) ARP cache poisoning and man in the middle attacks;

c) Exploitation of MAC address learning and malformed traffic;

d) Public domain exploits against network services;

e) Etherleak testing and traffic replay; and

f) The TOE's system pending table.

49 The analysis conducted by evaluators and the subsequent testing indicated that the TOE will resist an attacker with a low attack potential. This is consistent with the requirements of the EAL 4 assurance level.

Chapter 4 - Certification

4.1 Overview

50 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

51 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [11]), the Australasian Certification Authority certifies the evaluation of Senetas CypherNET Multi-Protocol Encryptor performed by the Australasian Information Security Evaluation Facility, CSC Australia.

52 CSC Australia has found that Senetas CypherNET Multi-Protocol Encryptor - Product 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.

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

4.3 Assurance Level Information

54 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.

55 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.

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

4.4 Recommendations

57 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 ACSI 33 (Ref [2]) and New Zealand Government users should consult the NZSIT 400 Series (Ref [12]).

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

a) used only in its evaluated configuration, ensuring that the assumptions concerning the TOE security environment, and organisational security policies (Ref [1]) are fulfilled; and

b) operated according to the administrator guidance document (Ref [3]).

Annex A - References and Abbreviations

A.1 References

[1] Security Target for Senetas CypherNET Multi-Protocol Encryptor Version 1.18

[2] Australian Government Information and Communications Technology Security Manual (ACSI 33), September 2007, Defence Signals Directorate, (available at www.dsd.gov.au/library/infosec/acsi33.html)

[3] Senetas CypherNET Product Manual version 1.4, February 2008

[4] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 2.1, August 1999, CCIMB-99-031, incorporated with interpretations as of 4 September 2002

[5] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements (CC), Version 2.1, August 1999, CCIMB-99-032, incorporated with interpretations as of 4 September 2002

[6] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (CC), Version 2.1, August 1999, CCIMB-99-033, incorporated with interpretations as of 4 September 2002

[7] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology (CEM), Version 1.0, August 1999, CEM-99/045, Incorporated with interpretations as of 2003-12-31

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

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

[10] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000 (available at www.dsd.gov.au/library/pdfdocs/CCDocumentation/ccra.pdf)

[11] Senetas CypherNET Multi-Protocol Encryptor Evaluation Technical Report, Version 2.0, 21 April 2008 (Commercial-in-Confidence)

[12] New Zealand Information and Communications Technology Security Manual (NZSIT 400 Series), February 2008, Government Communications Security Bureau (available at www.gcsb.govt.nz/newsroom/nzsits.html)

A.2 Abbreviations

ACA	Australasian Certification Authority
AES	Advanced Encryption Standard
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
CA	Certificate Authority
CAT	Connection Action Table
CC	Common Criteria
CEM	Common Evaluation Methodology
DES	Data Encryption Standard
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
GCSB	Government Communications Security Bureau
MAC	Media Access Control
RSA	Rivest Shamir Adleman
SFP	Security Function Policy
SNMP	Simple Network Management Protocol
SONET/SDH	Synchronous Optical/Synchronous Digital Hierarchy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
USB	Universal Serial Bus
3DES	Triple Data Encryption Standard