Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Maintenance Report

Supplementing Certification Report 2011/77

19 Dec 2011

Version 1.0

Amendment Record

Version	Date	Description
0.1	05/12/2011	Internal release.
1.0	19/12/2011	Public release.

Table of Contents

Chapter 1 - Introduction

1.1 Purpose

1 This document in an addendum to the Certification Report (Ref [1]) that describes the relevant baseline evaluation of the Sentas Encryptor range.

2 The purpose of this Maintenance Report is to describe the status of assurance continuity activities undertaken by Senetas for the CypherNet Multi-Protocol Encryptor and the CypherNet Fibre Channel Encryptor against the requirements contained in Assurance Continuity: CCRA Requirements (Ref [4]).

3 Senetas provided information about their assurance continuity activities in the form of an Impact Analysis Report (IAR). The IARs (Ref [5] and [6]) lists the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes.

4 This report should be read in conjunction with

a) The certified TOE's Certification Report (Ref [1]).

b) The certified TOE's Security Target (Ref [7]) which provides a full description of the security requirements and specifications that were used as the basis of the baseline evaluation.

5 Both of the Maintained TOEs, the Senetas CypherNet Multi-Protocol Encryptor and the Senetas CypherNet Fibre Channel Encryptor have been evaluated separately in the past by the AISEP. The Certification report for these products (Ref [2] and [3]) should also be read.

1.2 Identification

6 Table 1 provides identification details for the maintained TOEs and the certified TOE.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
Maintained TOE	Senetas CN SONET OC-3/12/48/192 Senetas CN Fibre Channel Encryptor CypherNET Application Software version 4.0.2
Developer	Senetas Security Pty Ltd
Certified TOE	Senetas CypherNET Multi-Protocol Encryptor

	CyherNET SONET OC-3/12/48/192, ATM and Link CypherNET Fibre Channel Encryptor CypherNET Application Software version 2.0.0
Security Target	Ref [7]
Evaluation Level	EAL 4+
Certificate Number	2011/77

Chapter 2 - IAR Summary

2.1 Description of Changes

7 The Impact Analysis Report (IAR) indicated that the following minor changes have been made to the Senetas CN SONET OC-3/12/48/192:

a) **Hardware changes**

Since the certified TOE, there has been an update to power supplies in the CN SONET OC192 Encryptors.

The CN SONET OC192 Encryptor model A5211B now has two new designators (A5213B and A5214B) with following changes:

The A5213B model supports dual, hot-swappable **AC power supplies** as opposed to previous DC only standard power supplies in A5221B model.

The A5214B model supports dual, hot-swappable **DC power supplies** as opposed to previous DC only standard power supplies in A5221B model.

The new hot-swappable power supplies were included in the certified evaluated Ethernet Encryptor (CN3000 – with dual redundant hot swappable AC or DC power supplies). The same swappable power supply is used in the SONET Encryptor. The power supply is not responsible for any security functions.

b) **Model Identification changes**

The new CN SONET OC192 Encryptor uses updated model numbers due to changes in power supply as described above. The original certified model numbers and new model numbers are listed in the Table 3 below.

The Model ID changes are as follows:
Model A5221B has two new designators i.e. Model A5213B and Model A5214B.

c) **Software changes**

Version 2.0.0 of the SONET Encryptor software has now changed to version 4.0.2 as indicated in tables 2 and 3. The release of the 4.0.2 software represents minor non-security impacting updates to kernel header files (device drivers).

Device drivers updates were required due to the refactoring of the Motorola Power PC MPC8280 CPU architecture support of the CN1000 and CN3000 platforms. No re-design of the TOE was necessary as indicated in the developer evidence section of the IAR.

These updates to specific kernel files are already included in the Certified TOE evaluated code and the evaluated code base operates the SONET Encryptors.

Note: The software version is changing directly from version 2.0.0 to version 4.0.2 to ensure consistency with the reseller/OEM versioning system.

Table 2 – CN SONET OC3, OC12 and OC48 Encryptors

Certified ID	Model ID	Description	Certified software version	Changed version
A2141B	A5161B	CYPHERNET SONET OC-3/STM1 – SONET/SDH	2.0.0	4.0.2
A2141B	A5163B	CYPHERNET SONET OC-12/STM4 – SONET/SDH	2.0.0	4.0.2
A2141B	A5165B	CYPHERNET SONET OC-48/STM16 – SONET/SDH	2.0.0	4.0.2

Table 3 – CN SONET OC192 Encryptors

Certified ID	Model ID	Changed Model ID	Description	Previous Certified Version	Changed Version
A2201B001	A5211B	A5213B	CYPHERNET SONET OC-192/STM64 – SONET/SDH AC unit	2.0.0	4.0.2
A2201B001	A5211B	A5214B	CYPHERNET SONET OC-192/STM64 – SONET/SDH DC unit	2.0.0	4.0.2

8 The Impact Analysis Report (IAR) indicated that the software change described above for the SONET Encryptor is the only minor change that has occurred to the Senetas CN Fibre Channel Encryptor.

9 In summary, the CN SONET OC192 Encryptor has updated the hot-swappable power supplies and as such the model numbers were also updated.

10 Both the CN SONET OC-3/12/48/192 Encryptors and the CN Fibre Channel Encryptor software have been updated from version 2.0.0 to version 4.0.2 due to a device driver update. Software version 4.0.2 was evaluated as part of the certified TOE.

2.2 Documentation Updated

11 The affected developer evidence was:

- Common CypherNet library code;
- Test plans, results and explanatory notes for 4.0.2 Encryptor software.

Chapter 3 - Assurance Continuity

3.1 Assurance Continuity Result

12 After consideration of the Impact Analysis Report (IAR) provided by Senetas Security Pty Ltd, Australasian Certification Authority (ACA) has determined that the proposed changes are minor.

13 The ACA agrees that the resultant change in the TOE can be classified as minor and that certificate maintenance is the correct path to continuity of assurance. The ACA agrees that the original assurance result is maintained for Senetas CN SONET OC-3/12/48/192 Encryptor and CN Fibre Channel Encryptor running software version 4.0.2.

References and Abbreviations

A.1 References

[1] Certification Report 2011/77, Australasian Certification Authority.

[2] Certification Report 2009/62, Australasian Certification Authority.

[3] Certification Report 2008/46, Australasian Certification Authority.

[4] Assurance Continuity: CCRA requirements, Common Criteria Interpretation Management Board, CCIMB-2004-02-009, Version 1.0, February 2004.

[5] Impact Analysis Report for Senetas CN Series Multi-Protocol Encryptor, Version 2.2, November 2011.

[6] Impact Analysis Report for Senetas CN Fibre Channel Encryptor, Version 2.2, November 2011.

[7] Security Target for Senetas CN/CS Series Ethernet Encryptor, Version 3.0, August 2011.

A.2 Abbreviations

ACA	Australasian Certification Authority
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
IAR	Impact Analysis Report
TOE	Target of Evaluation