



Australian Government
Department of Defence

Australasian Information Security Evaluation Program

**Maintenance Report Supplementing
Certificate Report 2011/77**

**26 June 2014
Version 1.0**

Commonwealth of Australia 2014

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

Amendment Record

Version	Date	Description
1.0	26/06/2014	Final release

Table of Contents

1. Table of Contents.....	iv
2. Chapter 1 – Introduction	1
<i>1.1 Purpose.....</i>	<i>1</i>
<i>1.2 Identification.....</i>	<i>1</i>
3. Chapter 2 – IAR Summary.....	3
<i>2.1 Description of changes</i>	<i>3</i>
<i>2.2 Software changes.....</i>	<i>3</i>
<i>2.3 Hardware changes.....</i>	<i>3</i>
<i>2.4 Development environment changes</i>	<i>3</i>
<i>2.5 Documentation updated.....</i>	<i>4</i>
4. Chapter 3 - Assurance Continuity	5
<i>3.1 Assurance Continuity Result.....</i>	<i>5</i>
5. References and Abbreviations.....	6

Chapter 1 – Introduction

1.1 Purpose

This document is an addendum to the Certification Report (Ref [1]) that describes the relevant baseline evaluation of the Senetas CN Series Ethernet Encryptor, Senetas CS Series Ethernet Encryptor and CypherManager.

The purpose of this Maintenance Report is to describe the status of the assurance continuity activities undertaken by Senetas for the *Senetas CN Series Ethernet Encryptor & CS Series Ethernet Encryptor and CypherManager* against the requirements contained in the Assurance Continuity: CCRA Requirements (Ref [2]).

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

This report should be read in conjunction with:

- a) The certified TOE's Certification Report (Ref [1]).
- b) The certified TOE's Security Target v3.0 (Ref [4]) which provides a full description of the security requirements and specifications that were used as the basis of the baseline evaluation.
- c) The Maintenance Report Supplementing Certification Report 2011/77, 19 Dec 2011, Version 1.0 & Maintenance Report Supplementing Certification Report 2011/77 22 July 2013 Version 1.0. (Ref [3]).

1.2 Identification

Table 1: Identification Information

Item	Identifier
Impact Analysis Report	Impact Analysis Report for Senetas CN Series Ethernet Encryptor & CS Series Ethernet Encryptor and CypherManager
Evaluation Scheme	Australasian Information Security Evaluation Program
Maintained TOE	Senetas CN Series Ethernet Encryptor 4.4.0, Senetas CS Series Ethernet Encryptor 4.4.0 and CypherManager 7.2.0
Developer	Senetas Security Pty Ltd
Certified TOE	Senetas CN Series Ethernet Encryptor, Senetas CS Series Ethernet Encryptor and CypherManager. 4.02

Security Target	Security Target for Senetas CN Series Ethernet Encryptor Senetas CS Series Ethernet Encryptor CypherManager Version 3.0, 17th August 2011
Certificate Number	2011/77

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 of the Security Target (Ref [4]).

Chapter 2 – IAR Summary

2.1 Description of changes

The Impact Analysis Report (IAR) indicated that the following minor changes have been made to the Senetas CN Series Ethernet Encryptor, Senetas CS Series Ethernet Encryptor and CypherManager.

Table 2: Version changes

ID	Description	Certified version	Changed version
A5135B	CN1000 Ethernet 1G(SFP) AC Unit	4.0.2	4.4.0
A5141B	CN1000 Ethernet 1G(SFP_RJ45) AC Unit	4.0.2	4.4.0
A5203B	CN3000 Ethernet 10 G AC Unit	4.0.2	4.4.0
A5204B	CN3000 Ethernet 10 G DC Unit	4.0.2	4.4.0
A5175B	CYPHERNET FIBRE CHANNEL 4G AC UNIT	4.0.2	4.4.0
A5165B	CYPHERNET SONET OC-48/STM16 – SONET/SDH	4.0.2	4.4.0
A5213B	CYPHERNET SONET OC-192/STM64 – SONET/SDH	4.0.2	4.4.0
A5214B	CYPHERNET SONET OC-192/STM64 – SONET/SDH	4.0.2	4.4.0

2.2 Software changes

Version 4.4 release is for updated compliance to FIPs 140-2. Each fix was applied to make the TOE function as originally intended, no additional security functionality was added, and no existing security functionality was removed. Regression testing was applied to Version 4.4.0 of the software running on encryptors and consistent results were found by both developers and evaluators.

Types of minor updates that are not related to the TSF include:

- Key lengths changed to 2048bits
- DH changed from Group 2 to Group 14
- Addition of a local activation command.

2.3 Hardware changes

No hardware changes were made.

2.4 Development environment changes

The changes to the development environment do not have a follow on effect on any assurance components outside the development environment.

2.5 Documentation updated

The certified Security Target was 'Senetas CN Series Ethernet Encryptor, Senetas CS Series Ethernet Encryptor and CypherManager'. Version 3.0, 17th August 2011. No changes were required to this document.

The test evidence is the only evaluation evidence to change. Senetas test evidence verifying that the 4.4.0 functions correctly has been provided (Ref [5]).

Chapter 3 - Assurance Continuity

3.1 Assurance Continuity Result

After consideration of the Impact Analysis Report (IAR) provided by Senetas, Australasian Certification Authority (ACA) has determined that the proposed changes are minor. 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 Series Ethernet Encryptor, Senetas CS Series Ethernet Encryptor and CypherManager.

References and Abbreviations

A.1 References

1. Certification Report 2011/77, 5 Sept 2011, Version 1.0 Australasian Certification Authority.
2. Assurance Continuity: CCRA requirements, Common Criteria Interpretation Management Board, CCIMB-2012-06-01, Version 2.1, June 2012.
3. Maintenance Report Supplementing Certification Report 2011/77 19 Dec 2011 Version 1.0 & Maintenance Report Supplementing Certification Report 2011/77 22 July 2013 Version 1.0.
4. Security Target: Senetas CN Series Ethernet Encryptor, Senetas CS Series Ethernet Encryptor and CypherManager. Version 3.0, 17 Aug 2011.
5. Senetas Test Evidence:
 - Fibre Channel Test Plan;
 - Ethernet Encryptor Test Specification;
 - A5141B-4.4.0- Test results;
 - A5165B-4.4.0- Test results;
 - A5175B-4.4.0- Test results;
 - A5203B_A5204B- 4.4.0 Test Results; and
 - A5213B_A5214B- 4.4.0 Test Results.
6. Impact Analysis Report for Senetas CN Series Ethernet Encryptor, Senetas CS Series Ethernet Encryptor and CypherManager, version 1.3, May 2014.

A.2 Abbreviations

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