Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Maintenance Report Supplementing Certificate Report 2014/89

14 March 2018
Version 1.0

Amendment Record

Version	Date	Description
1.0	14/03/2018	External release

Table of Contents

1. **Table of Contents....................iv**

2. **Chapter 1 – Introduction....................1**

1.1 Purpose....................1

1.2 Identification....................1

3. **Chapter 2 – IAR Summary....................3**

2.1 Description of changes....................3

2.2 Software changes....................3

2.3 Hardware changes....................4

2.4 Regression Testing....................4

2.5 Development environment changes....................5

2.6 Documentation updated....................5

4. **Chapter 3 - Assurance Continuity....................6**

3.1 Assurance Continuity Result....................6

5. **References and Abbreviations....................7**

A.1 References....................7

A.2 Abbreviations....................7

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 Encryptor Range and Senetas CM Management Application.

The purpose of this Maintenance Report is to describe the status of the assurance continuity activities undertaken by Senetas for the *Senetas CN Series Encryptor Range and Senetas CM Management Application* 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)(Ref [5]). 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 v1.0 (Ref [3]) which provides a full description of the security requirements and specifications that were used as the basis of the baseline evaluation.
c) The updated TOE's Security Target v1.2 (Ref [6]) which provides a full description of the security requirements and specifications that were used as the basis of the maintenance report.

1.2 Identification

Table 1: Identification Information

Item	Identifier
Impact Analysis Report	Impact Analysis Report for Senetas CN Series Encryptor 2.6.3, Version 2.0, March 2018
Changed TOE	The Senetas CN Series Encryptor Range
Certified TOE	Certification Report 2014/89 CN Series Models CN6040 1G ETHERNET + 1/2/4G Fibre Channel (SFP+RJ45) AC UNIT CN6040 1G ETHERNET + 1/2/4G Fibre Channel (SFP+RJ45) DC UNIT CN6040 1G ETHERNET + 1/2/4G Fibre Channel (SFP+RJ45) AC/DC UNIT CN6100 10G ETHERNET (XFP) AC UNIT CN6100 10G ETHERNET (XFP) DC UNIT CN6100 10G ETHERNET (XFP) AC/DC UNIT CN6010 1G ETHERNET (SFP+RJ45) AC UNIT CN6010 1G ETHERNET (SFP+RJ45) DC UNIT

	CN6010 1G ETHERNET (SFP+RJ45) AC/DC UNIT CN4010 1G ETHERNET UNIT
Original Security Target	Security Target for Senetas CN Series Encryptor Range & Senetas CM Management Application, 5 August 2014 Version 1.0
Updated Security Target	Security Target for Senetas CN Series Encryptor Range & Senetas CM Management Application, Version 1.2, 29 November 2017
Evaluation Level	EAL 2+
Evaluation Technical Report	Evaluation Technical Report for Senetas CN Encryptor Range, Version 1.0, 12th Aug 2014
Certification Report	AISEP Certification Report, Certificate Number: 2014/89, 18 August 2014, Version 1.0
Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4,
Methodology	CCMB-2017-04-004, April 2017
Conformance	CC Part 2 conformant CC Part 3 augmented with ALC_FLR.2 (Flaw reporting procedures)
Sponsor	Senetas Security Pty Ltd 312 Kings Way, South Melbourne, VIC 3205, Australia.
Developer	Senetas Security Pty Ltd
Evaluation Facility	DXC 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 of the Security Target (Ref [3]).

Chapter 2 – IAR Summary

2.1 Description of changes

The Impact Analysis Report (IAR) indicated a number of changes made to the certified TOE. These are described in section 2.2.

The TOE's certified and changed versions are listed in table below.

Table 2: Version changes

ID	Description	Certified version	Changed version
A6100B	CN6100 10G Ethernet (XFP) AC UNIT	2.6.0	2.6.3
A6101B	CN6100 10G Ethernet (XFP) DC UNIT	2.6.0	2.6.3
A6102B	CN6100 10G Ethernet (XFP) DC UNIT	2.6.0	2.6.3
A6102B	CN6100 10G Ethernet (XFP) DC UNIT	2.6.0	2.6.3
A6102B	CN6010 1G Ethernet (SFP + RJ45) DC UNIT	2.6.0	2.6.3
A6102B	CN6010 1G Ethernet (SFP + RJ45) AC/DC UNIT	2.6.0	2.6.3

2.2 Software changes

a) IP Command line interface change

Support for front panel Auxiliary port configuration. These changes added additional four entries for configuration of auxiliary port IPv4/IPv6 addressing and mode. Possible modes supported are bridge/isolated or disabled. However, these changes do not impact any of the SFRs.

b) Added SNMPv3 trap configuration CLI command

The SNMPv3 traps were previously only configurable via SNMPv3, but with the new 2.6.3 software, the CLI interface is able to configure snmptraps. These changes do not affect any of the SFRs.

c) Modified remote syslog configuration

As a result of the auxiliary port modifications, extra control has been added to ensure remote syslog server to specify whether that entry is assigned to the front main LAN port, or the front panel auxiliary port. This change does not impact any of the SFRs.

d) Inter process message queue changes

When the auxiliary Ethernet port is configured in isolated mode, processes accessing that port must exist within the isolated network namespace. Inter process messages queues must duplicate internal messages to reach the intended process/namespace. These changes allow for SNMP daemon to distribute traps/configuration messages to each network namespace. This change does not impact any of the SFRs.

e) Flash file system bugfix

ECC (error correction) driver code did not correctly detect memory device errors for the flash file system. A patch was written to set the relevant statistic in the event of a memory operations error. The statistics are used by the flash filesystem to detect and manage flash file system problems.
These changes fix the linux device driver code for flash file system. ECC now correctly checked, logged and corrected on error. This change does not impact any of the SFRs.

f) SNMP User Account lockout

The CLI has built in user account re-try lockout whereas SNMP did not before this release. The change was made to bring SNMP in-line with the CLI. The changes were added to allow the user to set the maximum number of retries for logging via SNMP and the account lockout time. This change impacts FIA_AFL.1, as it now allows remote admin users via SNMPv3 to be locked out.

g) Repeated character test for user account passwords

This change was added to allow the user to set the maximum number of repeated characters allowed in a user account password. This serves to add password complexity. This however, does not impact any of the requirements.

Note: The CM7 management software remained unchanged at version 7.4.0.

2.3 Hardware changes

No hardware changes were made.

2.4 Regression Testing

All changes are to the previously certified Senetas CN Series Encryptor Range (v.2.6.0) & Senetas CM management Application (v7.3.0) as described in “Section 2.1 Description of changes” are minimal and did require changes to design descriptions.

The regression tests were applied to TOE v2.6.3 with consistent results found by both the developer and the evaluators.

2.5 Development environment changes

The developer did not report any changes to the development environment.

2.6 Documentation updated

The Test Plan and Security Target have changed based on the updates (description given in the table below). The TOE design, Guidance and Functional specification are not impacted by the changes in the SFRs. The updated ST (Ref [6]) reflects a change to FIA_AFL.1 and no other SFRs.

Senetas test evidence verifies that the functions impacted by the SFR changes are implemented correctly in v2.6.3.

The following list of deliverables indicates if the document has changed followed by a description of the actual changes.

Deliverable	**Has it changed (Y/N)**	**Description of change**
Security Target	Y	Changes were documented in a new ST. These changes include an update to the requirements, and the TSS to reflect how the TOE addresses the update to the requirements.
Functional Specification	N	No changes have occurred to functional Specification.
TOE Design	N	No changes occurred.
Test Plans	Y	Test plan evidence provided.

The certified Security Target was *Security Target for Senetas CN Series Encryptor Range & Senetas CM Management Application, version 1.0, 5 August* 2014 (Ref [3]).

The updated Security Target was *Security Target for Senetas CN Series Encryptor Range & Senetas CM Management Application, Version 1.2, 29 November 2017*(Ref [6])

Based upon all of the above evidence and rationale the overall impact is considered to be **Minor.**

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 Encryptor Range and the Senetas CM7 Management Application software (Ref [5]).

References and Abbreviations

A.1 References

1. Certification Report 2014/89, 18 Aug 2014 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. Security Target for Senetas CN Series Encryptor Range & Senetas CM Management Application, 5 August 2014 Version 1.0
4. Senetas Test Evidence:
    a. Fibre Channel Test Plan
    b. Ethernet-Encryptor –Test-Specification. Test related to the changed TOE are:
        i. A6100B_A6101B_A6102B-2.6.3-Test-Results
        ii. A6010B_A6011B_A6012B-2.6.3-Test-Results
5. Senetas CN Series Encryptor Range 2.6.0 & Senetas CM Management Application IAR v2.0
6. Security Target for Senetas CN Series Encryptor Range & Senetas CM Management Application, Version 1.2, 29 November 2017

A.2 Abbreviations

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