Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Maintenance Report Supplementing Certificate Report 2017/113

09 March 2018
Version 1.0

Amendment Record

Version	Date	Description
1.0	08/03/2018	External release

Table of Contents

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 (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 (Ref [6]).

1.2 Identification

Table 1: Identification Information

Item	Identifier
Impact Analysis Report	Impact Analysis Report for Senetas CN Series Encryptor Range and Senetas CM Management Application, version 1.1
Evaluation Scheme	Australasian Information Security Evaluation Program
Maintained TOE	Senetas CN Series Encryptor Range 3.0.2 and Senetas CM Management Application 7.6.1
Developer	Senetas Security Pty Ltd
Certified TOE	Senetas CN Series Encryptor Range 3.0.1 and Senetas CM Management Application 7.6.1
Security Target	Security Target for Senetas CN Series Encryptor Range & Senetas CM Management Application, version 2.3, 29 November 2017
Updated Security	Security Target for Senetas CN Series Encryptor

Target	Range & Senetas CM Management Application, version 2.4, 8 March 2018
Certificate Number	2017/113

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
A4010B	CN4010 1G ETHERNET (RJ45) UNIT	3.0.1	3.0.2
A4020B	CN4020 1G ETHERNET (SFP) UNIT	3.0.1	3.0.2
A6010B	CN6010 1G ETHERNET (SFP+RJ45) AC UNIT	3.0.1	3.0.2
A6011B	CN6010 1G ETHERNET (SFP+RJ45) DC UNIT	3.0.1	3.0.2
A6012B	CN6010 1G ETHERNET (SFP+RJ45) AC/DC UNIT	3.0.1	3.0.2
A6040B	CN6040 1G ETHERNET + 1/2/4G Fibre Channel (SFP+RJ45) AC UNIT	3.0.1	3.0.2
A6041B	CN6040 1G ETHERNET + 1/2/4G Fibre Channel (SFP+RJ45) DC UNIT	3.0.1	3.0.2
A6042B	CN6040 1G ETHERNET + 1/2/4G Fibre Channel (SFP+RJ45) AC/DC UNIT	3.0.1	3.0.2
A6100B	CN6100 10G ETHERNET (XFP) AC UNIT	3.0.1	3.0.2
A6101B	CN6100 10G ETHERNET (XFP) DC UNIT	3.0.1	3.0.2
A6102B	CN6100 10G ETHERNET (XFP) AC/DC UNIT	3.0.1	3.0.2
A6140B	CN6140 1/10G ETHERNET (SFP+) AC UNIT	3.0.1	3.0.2
A6141B	CN6140 1/10G ETHERNET (SFP+) DC UNIT	3.0.1	3.0.2
A6142B	CN6140 1/10G ETHERNET (SFP+) AC/DC UNIT	3.0.1	3.0.2
A8003-10	CN8000 MULTI-SLOT 1/10G ETHERNET + 4/8G Fibre Channel (SFP+) AC UNIT	3.0.1	3.0.2
A9100B	CN9100 100G ETHERNET (CFP4) AC UNIT	3.0.1	3.0.2
A9101B	CN9100 100G ETHERNET (CFP4) DC UNIT	3.0.1	3.0.2
A9102B	CN9100 100G ETHERNET (CFP4) AC/DC UNIT	3.0.1	3.0.2
A9120B	CN9120 100G ETHERNET (QSFP28) AC UNIT	3.0.1	3.0.2
A9121B	CN9120 100G ETHERNET (QSFP28) DC UNIT	3.0.1	3.0.2
A9122B	CN9120 100G ETHERNET (QSFP28) AC/DC UNIT	3.0.1	3.0.2

2.2 Software changes

a) Fix support for ColorZ QSFP transceivers

On the CN 9120 the Colorz transceiver page was incorrectly specified as 20 decimal places instead of 20 hexadecimal. This fix does not impact the SFR.

b) Fix thermal daemon shutdown

The thermal management daemon was shutting down prematurely, and thus the TOE was changed to set a maximum loop count to prevent the shutdown. This fix does not impact any SFRs.

c) Thermal daemon and Menu daemon not automatically restarting

The thermal daemon (thermald) and menu (User Interface) management daemon (menud) were not automatically restarting on Zynq (ARM) based platforms. To ensure they are automatically restarted on Zynq based platforms, a startup script for menud was created. This fix did not impact any SFRs.

d) CN6140 sometimes rebooting when SFP transceiver extracted

An SFP transceiver was extracted when non-existent mdio registers were being accessed causing a kernel oops and the system would reboot. Thus the TOE was updated to stop accessing non-existent registers on the CN6140, preventing reboots. This does not impact any SFRs.

e) CN6140 Front Panel displays FW version as NA

The firmware version on the CN6140 LCD was displaying “NA”, thus the TOE added a switch for B6141 (CN6140 main board) to obtain firmware version. This does not impact the TOE SFRs as the TOE version is obtained via CLI and GUI.

f) Update inventory command’s network interface software version field

The CLI inventory command is missing B6141 reference (on CN6140 main board), and thus a switch for B6141 to inventory command was added to obtain software version for network interface. This is specific to the CN6140 model and does not impact any of the SFRs.

g) Link alarms not being reported on certain models

During the processing of link alarms the type of LEDs the unit has was being checked and certain models were incorrectly reporting “no LEDs” and the function was terminating before the alarm was fully processed. Tests were added for new models to correctly determine LED family. This change does not impact any of the SFRs.

h) Zynq based systems could fail to boot

The upgrade process was not leaving enough spare FLASH memory blocks to allow the boot process to always run successfully. Thus the root file system allocation was updated to ensure the boot process will always have enough blocks to run successfully. This update does not impact any of the SFRs.

i) Clear stats of the QSFP Transceiver on the CN9120

There was no mechanism for clearing stats on QSFP transceivers that support page 20. The TOE was updated to clear page 20 transceiver stats, on model CN 9120 which does not impact any of the SFRs.

j) Update FPGA Transceiver settings on the CN6140

The Ethernet links on the CN6140, were not always coming up correctly, and thus the need to update the FPGA transceiver settings. This however, does not impact any of the SFRs.

Note: The CM7 management software remained unchanged at version 7.6.1.

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.3.0.1) & Senetas CM management Application (v7.6.1) as described in 'Section 2.1: Description of changes' are minimal and did not require changes to design descriptions.

The regression tests were applied to TOE v3.0.2 and CM v7.6.1 with consistent results found by the vendor.

2.5 Development environment changes

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

2.6 Documentation updated

The test Plan has been updated include testing of changes outlined in Section 2. The ST has been updated to reflect the change in TOE version.

The TOE design, Guidance and Functional specification are not impacted by the changes.

Senetas test evidence verifies that the functions impacted by the changes are implemented correctly in v3.0.2.

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 new ST. However, changes are only specific to the new software version, as none of the changes as defined above impact SFRs.
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 2.3, 29 November 2017 (Ref [3]).*
The updated Security Target is *Security Target for Senetas CN Series Encryptor Range & Senetas CM Management Application, version 2.4, 08 March 2018 (Ref [6]).*

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.

References and Abbreviations

A.1 References

1. Certification Report 2017/113, 13 Dec 2017 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, 29 November 2017 Version 2.3
4. Senetas Test Evidence:
    a. 3.0.2-Test-plan_v1.0
    b. 3.0.2-Test report
5. Senetas CN Series Encryptor Range 3.0.2 & Senetas CM Management Application IAR v3.0
6. Security Target for Senetas CN Series Encryptor Range & Senetas CM Management Application, version 2.4, 08 March 2018

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