Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Maintenance Report Supplementing Certificate Report 2014/89

31 March 2015
Version 0.1

Amendment Record

Version	Date	Description
0.1	31/03/2015	Internal 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). 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.

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 2.6.0 and Senetas CM Management Application 7.4.0
Developer	Senetas Security Pty Ltd
Certified TOE	Senetas CN Series Encryptor Range 2.4.0 and Senetas CM Management Application 7.3.0
Security Target	Security Target for Senetas CN Series Encryptor Range & Senetas CM Management Application, version 1.0, 5 August 2014
Certificate Number	2014/89

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
A6040B	CN6040 1G ETHERNET + 1/2/4G Fibre Channel (SFP+ RJ45) AC UNIT	2.4.0	2.6.0
A6041B	CN6040 1G ETHERNET + 1/2/4G Fibre Channel (SFP+ RJ45) DC UNIT	2.4.0	2.6.0
A6042B	CN6040 1G ETHERNET + 1/2/4G Fibre Channel (SFP+ RJ45) AC/DC UNIT	2.4.0	2.6.0
A6100B	CN6010 10G Ethernet (XFP) AC UNIT	2.4.0	2.6.0
A6101B	CN6010 10G Ethernet (XFP) DC UNIT	2.4.0	2.6.0
A6102B	CN6010 10G Ethernet (XFP) AC/DC UNIT	2.4.0	2.6.0
A6010B	CN6010 1G Ethernet (SFP + RJ45) AC UNIT	2.4.0	2.6.0
A6011B	CN6010 1G Ethernet (SFP + RJ45) DC UNIT	2.4.0	2.6.0
A6012B	CN6010 1G Ethernet (SFP + RJ45) AC/DC UNIT	2.4.0	2.6.0
A4010B	CN4010 1G Ethernet UNIT	2.4.0	2.6.0
CM7	CM Management Application software	7.3.0	7.4.0

2.2 Software changes

(a) ECDH and ECDSA for secure message exchange

This change was an extension to Senetas PKI Infrastructure support to include ECDSA/ECDH (suite B) algorithms. In addition to RSA2048 certificates, the Encryptors now support P-256/P-384/P-521 FIPS approved curves. This change is confirmed to the embedded software only, and has no impact on the FPGA design.

Elliptic Curve Diffie Hellman (ECDH) and Elliptic Curve Digital Signature (ECDSA) algorithms have been added as an extension of the existing X.509 PKI framework (that was previously evaluated in the 2.4.0 submission) as an option to secure key exchanges between Encryptors (X.509 certificate public key and digital signature algorithms). This feature has been added to comply with the NIST suite-B algorithms and to provide perfect forward secrecy. Users can now set the key exchange algorithm to RSA2048 or EC256, EC384 or EC521 via the CSR Type field in CM7.

Note: ECDH/ECDSA are only supported on Ethernet Encryptors.

(b) GCM on 10Gbe

This change relates to the port of the previously certified 16 GCM to Senetas 10G Ethernet design. This is primarily an FPGA code base change for the 10G build. Some minor software changes were made to support switching modes as per the 1G operation.

GCM provides authenticated encryption by calculating a Galois Message Authentication Code (GMAC) over a portion of a frame and appends the GMAC to the frame. This is a 10GbE extension of the existing 1GbE GCM implementation previously submitted in version 2.4.0. It is based on and fully compatible with the previous 1GbE design. When GCM mode is enabled the entire L2 frame will be authenticated by default. Optionally, only the encrypted payload can be selected to be authenticated to cater for network scenarios that require header modification by the network. This is selectable via the policy – a command or CM7 under the Policy settings. If the authentication failure rate exceeds a certain threshold, the connection is restarted. By default this threshold is disabled to prevent denial of service attacks. Alternatively the connection can be stopped. Frames that fail authentication are re-transmitted with an invalid FCS.

The CM7 Management Application software was updated to support the above software changes.

2.3 Hardware changes

No hardware changes were made.

2.4 Development environment changes

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

2.5 Documentation updated

The test evidence and the Security Target are the only evaluation documents to change (description given in the table below). The TOE design, Guidance and Functional specification are not impacted by the changes in the SFRs.

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	Yes, SFRs updated to include the new algorithms.
Functional Specification	N	No changes have occurred to functional Specification.
TOE Design	N	No changes occurred.

Test Plans	Y	Test evidence has been updated to include Specific Test plans and results.

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 SFRs defined below are updated in the ST to include the new algorithms. See the updated Security Target: *Security Target for Senetas CN Series Encryptor Range & Senetas CM Management Application, version 1.1, 1 December 2014* (Ref [6]).

- FCS_CKM.1.1.C to support for ECDH & ECDSA.
- FCS_CKM.2.1.A to add of ECDH & ECDSA to X.509 certificates.
- FCS_COP.1.1.B to provide more Encryptors with support to GCM, an algorithm that was previously evaluated.

All changes are to the previously certified Senetas CN Series Encryptor Range (v.2.4.0) & Senetas CM management Application (v7.3.0) 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 V2.6.0 and CM v7.4.0 with consistent results found by the vendor.

Senetas test evidence that verifies the functions impacted by the SFR changes in v2.6.0 and CM v7.4.0 are implemented correctly have been provided (Ref [4]).

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 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. A6040B_A6041B_A6042B-FC-2.6.0 Test results
        ii. A6100B_A610B_A6102B-2.6.0- Test results
        iii. A4010B-2.6.0- Test results
        iv. A6010B_A6011B_A6012B-2.6.0-Test Results
        v. A6040B_A6041B_A6024B-Eth. 2.6.0 Test Results
5. Senetas CN Series Encryptor Range 2.6.0 & Senetas CM Management Application IAR v1.2
6. Security Target for Senetas CN Series Encryptor Range & Senetas CM Management Application, version 1.1, 1 December 2014

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
CSR	Client-side rendering
EAL	Evaluation Assurance Level
FCS	Frame check sequence
GCM	Galois Counter Mode
IAR	Impact Analysis Report
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function