SEPTEMBER 2014

Senetas CN Series Encryptor Range & Senetas CM Management Application

Product Description

Senetas CN Series Encryptors are standards-based multi-protocol encryptors designed to secure the confidentiality of data transmitted over networks at data rates up to 10 Gbps.

Senetas CN Series Encryptors act as a "bump-in-the-wire" – encryption of data sent between Encryptors is transparent to the end user and any connected network equipment.

The Senetas CM management application is a Graphical User Interface (GUI) software package that runs on a Windows platform. It acts as a Certification Authority (CA) for signing of X.509 certificates. The CM application is used to manage CN Series Encryptors.

Evaluation Scope

The scope of the ASD Cryptographic Evaluation (ACE) included the following functionality:

- Authentication
- Data confidentiality
- Data integrity

Common Criteria Certification – Summary

The product was found to meet the requirements of the Common Criteria (CC) evaluation assurance level EAL2+ augmented with ALC_FLR.2.

ASD Findings and Recommendations

ASD performed a cryptographic evaluation on the product in addition to the Common Criteria evaluation.

As the product has successfully completed an ACE, it can be used to downgrade the requirements of PROTECTED data in transit to those of UNCLASSIFIED, in accordance with the Australian Government Information Security Manual (ISM).

Only one instance of CM MUST be used to configure all Encryptors in the same network.

Encryptors MUST be configured and managed either locally through the local interface or from the trusted network side.

Encryptors MUST NOT be configured or managed from the untrusted network side.

Agencies MUST NOT use Encryptors to manage VLANs for both classified networks and unclassified networks or non-classified networks and unclassified networks. (reference: Australian Government Information Security Manual, Control: 1138; Revision: 2; Updated: Feb-14)

Any compromised Encryptor MUST be promptly removed from the network, physically recalled and new certificates generated. A compromised Encryptor MUST result in a rekey of the entire network.

Encryptors and the workstation running CM take on the classification of the network they are connected to and MUST be treated as such.

Recommendations given in this Consumer Guide take precedence over those in the ISM where there is a conflict.

Contact Details

Australian government customers with questions regarding this advice should contact ASD Advice and Assistance at asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

ISM

The advice given in this document is in accordance with the Information Security Manual 2014. Australian government agencies are reminded to periodically check the latest release date of the ISM at www.asd.gov.au/infosec/ism/

Consumer Guide

This Consumer Guide was issued by ASD during September 2014.

(U) **LEGAL WARNING**: ALL DOCUMENTS ORIGINATING WITH OR RECEIVED FROM DSD, ALSO KNOWN AS ASD, ARE EXEMPT UNDER SECTION 7(2A) OF THE *FREEDOM OF INFORMATION (FOI) ACT 1982*. THIS EXEMPTION EXTENDS TO DOCUMENTS THAT CONTAIN SUMMARIES OF A DSD, ALSO KNOWN AS ASD, DOCUMENT OR EXTRACTS FROM SUCH A DOCUMENT. DSD, ALSO KNOWN AS ASD, MUST BE CONSULTED PRIOR TO THE RELEASE OF ANY SUCH INFORMATION UNDER AN FOI REQUEST.