SENETAS CN/CS SERIES ETHERNET ENCRYPTOR

PROTECT

Product Description

The Senetas CN Series Encryptor is a standards-based multi-protocol encryptor designed to secure the confidentiality of data transmitted over networks at data rates up to 10 Gbps.

The Senetas CS Series Encryptor is a software based (non FPGA) store and forward packet processing Ethernet encryptor designed to secure the confidentiality of data transmitted over networks at data rates up to 100 Mbps.

Both the CN and CS Encryptors act as "bumps-in-the-wire" – encryption of data sent between Encryptors is transparent to the end user and any connected network equipment.

CypherManager 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 CypherManager application is used to manage both CN and CS 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 EAL4+, maintenance July 2013 and June 2014.

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).

PROTECT

Only one instance of CypherManager 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.

Network Devices MUST NOT be used 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; 2014)

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 CypherManager 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

For further information regarding the certification, cryptographic evaluation or compliance with the Information Security Manual please contact ASD on 1300 CYBER1 (1300 292 371) or email asd.assist@defence.gov.au.

ISM 2014

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/index.htm

Consumer Guide

This Consumer Guide was reissued by ASD during June 2014.