DSD'S CONSUMER GUIDE

SENETAS CYPHERNET MULTI-PROTOCOL ENCRYPTOR

Product Description

The Senetas Cyphernet Multiprotocol encryptor is a hardware product that provides layer two encryption of SONET/SDH, ATM, Ethernet protocols and protocol-independent point-to-point data networks. Encryption can be done using triple-DES or AES, and peer authentication is conducted via the use of X.509 certificate authentication and RSA key exchange.

Evaluated Version

This consumer guide refers only to version 1.7 of the application software.

Scope of the Common Criteria Certification

The scope of the Common Criteria (CC) evaluation included the following functionality:

- Security Audit;
- Cryptographic support;
- User data protection;
- Identification and Authentication;
- Security Management;
- Protection of the TOE Security Functions;
- TOE Access, and
- Trusted Path/Channels.

If an Australian government agency is considering using the product then they need to be aware that the following functionality was not included as part of the evaluation:

- Use of the USB port which enables backup and restore functions.

Refer to the Senetas Cyphernet certification report for the product's evaluated configuration and for recommendations regarding Australian and New Zealand Government users.

Common Criteria Certification Summary

The product has met the requirements of the Common Criteria evaluation assurance level to EAL 4.

Summary of DSD's Findings

Because the product employs cryptography, DSD performed a cryptographic evaluation on the product in addition to the Common Criteria certification. The encryptor uses AES and triple-DES encryption with X.509 certificate authentication and RSA key exchange. This cryptography was found to be satisfactory for EAL4.

Users should refer to the certification report for information on the assumptions for the operating environment of the TOE, along with further information on scope and evaluated configuration.

The product has been evaluated to EAL 4. In accordance with ACSI 33 Chapter 9, the product can therefore be used for the transit of encrypted information of classification:

- IN-CONFIDENCE over an UNCLASSIFIED network;
- RESTRICTED over UNCLASSIFIED, PROTECTED or HIGHLY PROTECTED networks;
- PROTECTED over UNCLASSIFIED or IN-CONFIDENCE networks; and
- HIGHLY PROTECTED over UNCLASSIFIED, IN-CONFIDENCE or PROTECTED networks.

Point of Contact

For further information regarding the Cyphernet Multiprotocol encryptor's certification, cryptographic evaluation or compliance with ACSI 33 please contact DSD on (02) 6265 0197 or email assist@dsd.gov.au.

ACSI 33

The advice given in this document is in accordance with ACSI 33 release date September 2007. Australian government agencies are reminded to check the latest release of ACSI 33 at http://www.dsd.gov.au/library/infosec/acsi33.html to investigate if any changes have taken place.

Date of this Consumer Guide

This Consumer Guide was issued by DSD on 18 July 2008.