SQ-PHOENIX MULTIFUNCTION ENCRYPTOR VERSION 2.7

Product Description

The SQ-Phoenix Multifunction Encryptor Version 2.7 is an in-line encryptor for voice and fax communications over analogue transmission networks . It is designed to protect the confidentiality of sensitive information during transmission.

Scope of Evaluation

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

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the Security Functions.

Potential users of the SQ-Phoenix product are advised that the following set of functions and services were not evaluated as part of the evaluation:

- All key management configurations other than Net Mode;
- Encryption using cryptographic algorithms other than AES 128;
- Operation without dedicated cryptographic circuitry;
- Secure file transfers over the secure voice link; and
- Ancillary support equipment.

Common Criteria Certification Summary

The product has met the requirement of the Common Criteria (CC) evaluation assurance to level EAL 2.

DSD's Cryptographic Evaluation

Because the product employs cryptography, DSD performed a cryptographic evaluation on the product in addition to the Common Criteria certification.

DSD's Recommendations

For Australian Government users it is recommended that the product be configured as per the Target of Evaluation (TOE) for this certification. In addition, DSD makes the following recommendations:

- The device must be configured to use the DSD Approved Cryptographic Algorithm AES with a keysize of 128 bits
- Users should verify that AES is installed on each device by establishing a secure voice connection to another unit which is known to have AES installed
- Users must implement an appropriate secure key exchange infrastructure.

This product has been evaluated to EAL 2, and as such, in accordance with ACSI 33, it can be used to transmit:

- IN-CONFIDENCE data over UNCLASSIFIED networks;
- RESTRICTED data over UNCLASSIFIED networks;
- PROTECTED data over UNCLASSIFIED networks; and
- HIGHLY PROTECTED data over IN-CONFIDENCE networks.

Point of Contact

For further information regarding the certification, cryptographic evaluation or compliance with ACSI 33, please contact DSD on (02) 62650197 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 periodically check the latest release of ACSI 33 at www.dsd.gov.au/library/infosec/acsi33.html.

Date of this Consumer Guide

This Consumer Guide was issued by DSD on 31 January 2008.