PROTECT

SAFENET LUNA PCI CONFIGURED FOR USE IN THE LUNA SA 4.1 WITH TRUSTED PATH AUTHENTICATION

Product Description

The SafeNet Luna SA is a network attached Hardware Security Module for the performance of cryptographic functions for key generation and storage, encryption and decryption, and digital signature computation and verification. It is available in two model families: Password Authentication and Trusted Path Authentication. DSD has evaluated the Trusted Path Authentication version.

The product consists of:

- The Luna PCI cryptographic module, which is a printed circuit board in PCI format within a tamper-resistant housing;
- The Luna Pin Entry Device (PED), which is enclosed in a separate enclosure and connected to the module via a data port;
- iKeys, which are USB token devices used to store authentication data for entry through the PED;
- PKCS #11 client library and driver software; and
- Tokens for backing up cryptographic objects on the HSM.

Common Criteria Certification Summary

The product was found to meet the requirements of the Common Criteria (CC) evaluation assurance level EAL 4+.

Evaluation Scope

The scope of the DSD evaluation included the following functionality:

- Trusted path authentication;
- Generation of cryptographic keys; and
- Secure storage of key material.

PROTECT

DSD's Findings and Recommendations

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

DSD is satisfied with the strength of function provided by the SafeNet Luna SA at the RESTRICTED or PROTECTED level, with the provision that users implement the following security policies and practices:

- Users must ensure they only use DSD Approved Cryptographic Algorithms. This can be partially enforced by setting the "Allow non-FIPS algorithms" to "Off".
- DSA moduli must be 1024 bits.
- Diffie-Hellman moduli must be at least 1024 bits.
- AES and 3DES should be used only in CBC mode, not ECB mode.
- When using Elliptic Curve Algorithms, only NIST approved curves should be used. Details of these curves can be found in Appendix D of FIPS PUB 186-3 Digital Signature Standard, June 2009, available from http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf.
- The iKeys should be used with PINs of at least 12 digits in length, and appropriate physical security measures should be in place to protect the iKeys.
- Partition Activation should only be used when strictly necessary.
- The "SO/HSM Admin can reset User PIN" policy should be "on". The "Ignore failed challenge responses" should not be set, and the number of failed login attempts trigger set to some (finite) number at the ITSA's discretion.

Point of contact

For further information regarding the certification, cryptographic evaluation or compliance with the Information Security Manual for the SafeNet Luna SA, please contact DSD on (02) 6265 0197 or email assist@dsd.gov.au.

ISM 2010

The advice given in this document is in accordance with the Information Security Manual release date November 2010. Australian government agencies are reminded to periodically check the latest release date of the ISM at http://www.dsd.gov.au/library/infosec/ism.html.

Date of this Consumer Guide

This consumer guide was issued on 13 December 2010.