PROTECT

SAFENET LUNA CA3

Product Description

The Luna CA3 is a hardware security module adhering to the PKCS #11 v2.01 standard, more commonly referred to as the Cryptographic Token Interface (Cryptoki). A HSM is typically used to generate, protect and provide secure usage of a Public Key Infrastructure Certification Authority's private key.

Evaluation Scope

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

- Cryptographic support;
- User data protection;
- Security management;
- Protection of the TOW security function; and
- Trusted path.

The following was outside the scope of the evaluation:

- Security audit; and
- PKI applications utilising this HSM.

Common Criteria Certification – Summary

The product was found to meet the requirements of the Common Criteria (CC) evaluation assurance level EAL4+.

DSD's Cryptographic Evaluation

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

PROTECT

The cryptographic primitives evaluated were all found to be correct; these were RSA, DSA, Diffie-Hellman, 3-DES, SHA-1 and MD5.

DSD's Recommendations

Although the Luna CA3 has been evaluated this doesn't mean that a PKI system using the Luna CA3 is secure. Use of the Luna CA3 must be in conjunction with an appropriately evaluated PKI application.

The Luna CA3 allows the user application to seed the pseudo random number generation (PRNG). DSD was unable to assess the quality of the PRNG internal seeding so any user of the Luna CA3 should seed the PRNG with sufficient entropy. The PRNG is responsible for supplying randomness to the key generation in the Luna CA3, and so insufficient entropy will result in weak keys.

Finally, DSD was unable to investigate the authentication mechanism of the Luna CA3 so appropriate physical security should be put in place to ensure that only authorised people are allowed access to the device. This is good practice for any CA so should not be any extra burden.

Point of Contact

For further information regarding the certification of this product, or compliance with the ISM, please contact DSD on (02) 6265 0197 or email assist@dsd.gov.au.

Australian Government Information Security Manual

The advice given in this document is in accordance with the ISM release date September 2009. Australian government agencies are reminded to check the latest release of the ISM at www.dsd.gov.au/library/infosec/ism.html to investigate if any changes have taken place.

Date of this Consumer Guide

This Consumer Guide was issued by DSD on 18 February 2010.