Certification Report

SafeNet Luna® PCI configured for use in Luna® SA 4.5.1 (RF) with Backup

Sponsor and developer:	***SafeNet Canada, Inc.*** **20 Colonnade Road, Suite 200** **Ottawa, ON** **Canada K2E 7M6**
Evaluation facility:	***Brightsight*** **Delftechpark 1** **2628 XJ Delft** **The Netherlands**
Report number:	**NSCIB-CC-12-36718-CR**
Report version:	**1**
Project number:	**NSCIB-CC-12-36718**
Authors(s):	**NLNCSA**
Date:	**July 26th 2013**
Number of pages:	**18**
Number of appendices:	**0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Head office Apeldoorn:
Boogschutterstraat 11A
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Apeldoorn:
Vissenstraat 6
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Enschede:
Josink Esweg 10
P.O. Box 337
7500 AH Enschede
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 859

TÜV Rheinland Nederland B.V. is a
registered company with the
Amsterdam Chamber of Commerce
under number 27288788
info@nl.tuv.com
www.tuv.com/nl

Certificate

Standard
Common Criteria for Information Technology Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)

Certificate number **C12-36718**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer
SafeNet Inc.

20 Colonnade Road, suite 200, K2E 7M6 Ottawa, Canada

Product and assurance level
<u>SafeNet Luna® PCI configured for use in Luna® SA 4.5.1 (RF) with Backup</u>

Assurance Package:
- EAL 4-augmented by ADV_IMP.2, ALC_FLR.2, AVA_CCA.1, AVA_MSU.3, AVA_VLA.4

Protection Profile Conformance:
- PP/0308 Cryptographic Module for CSP Signing Operations with Backup Protection Profile , version 0.28, 27th October 2003

Project number **NSCIB-CC-12-36718-CR**

Evaluation facility **Brightsight BV located in Delft, the Netherlands**

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 2.3 (ISO/IEC 18045:2005)

Common Criteria Recognition Arrangement for components up to EAL4

SOGIS
INFORMATION TECHNOLOGY SECURITY
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 2.3 for conformance to the Common Criteria for IT Security Evaluation version 2.3. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity
Date of issue : **02-08-2013**
Certificate expiry : **02-08-2023**

Registration number
RvA
PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

TÜV Rheinland Nederland B.V.
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

CONTENTS:

Foreword 4

Recognition of the certificate 5

1 Executive Summary 6

2 Certification Results 7

2.1 Identification of Target of Evaluation 7
2.2 Security Policy 7
2.3 Assumptions and Clarification of Scope 10
2.4 Architectural Information 12
2.5 Documentation 13
2.6 IT Product Testing 13
2.7 Evaluated Configuration 14
2.8 Results of the Evaluation 15
2.9 Evaluator Comments/Recommendations 16

3 Security Target 17

4 Definitions 17

5 Bibliography 18

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products.

A part of the procedure is the technical examination (evaluation) of the product according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Recognition of the certificate

The Common Criteria Recognition Arrangement and SOG-IS logos are printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Luna® PCI configured for use in the Luna® SA 4.5.1 (RF) with Backup (Luna® PCI). The developer of this product is SafeNet Canada, Inc. with corporate headquarters located in Belcamp MD, USA and Engineering office located in Ottawa, Canada. SafeNet Canada, Inc. also acted as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The Luna® PCI cryptographic module is a Hardware Security Module (HSM) in the form of a PCI card that typically resides within a custom computing or secure communications appliance. It is contained in its own secure enclosure that provides physical resistance to tampering and zeroization of plaintext key material and security parameters in the event a tamper signal is received. The boundary of the cryptographic module is defined to encompass all components inside the secure enclosure on the PCI card

The Security Target and the TOE claim conformance to the Cryptographic Module for CSP Signing Operations with Backup Protection Profile (PP/0308), version 0.28, dated 27th October 2003. This Protection Profile was registered and certified by ANSSI under the reference PP/0308.

The Luna® PCI configured for use in the Luna® SA 4.1 was originally evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on October 20th 2009, That evaluation, with certification ID NSCIB-CC-07-09219 was completed on November 2nd 2009.

This Certification Report pertains to the results of a delta evaluation of the Luna® SA 4.1 product, specifically, the Luna® SA 4.5.1. This certification was completed on July 26th with the preparation of this certification report. Both certifications were conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the Security Target *[ST]*, that identifies assumptions made during the evaluation, the intended environment for the Luna® PCI, the security requirements and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Luna® PCI configured for use in the Luna® SA 4.5.1 (RF) with Backup are advised to verify that their own environment is consistent with the Security Target and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* for this product provide sufficient evidence that it meets the Evaluation Assurance Level 4 augmented (EAL 4+) assurance requirements for the evaluated security functionality. The assurance level is augmented with: ADV_IMP.2 (Implementation of the TSF), ALC_FLR.2 (Evaluation of flaw remediation), AVA_CCA.1 (Covert Channel Analysis), AVA_MSU.3 (Validation of analysis) and AVA_VLA.4 (Highly resistant). The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 2.3 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 2.3 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the Luna® PCI with Backup for use in the Luna® SA 4.5.1 (RF) evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Luna® PCI configured for Use in Luna® SA 4.5.1 (RF) with Backup from SafeNet Canada, Inc. located in Ottawa, Canada.

The TOE, Luna® PCI configured for use in the Luna® SA 4.5.1 (RF) with Backup, includes the following:

- the Luna® PCI cryptographic module in a PCI Card form factor (216-010031-001 [legacy part number 900691-000] and 216-010031-002 [legacy part number 900691-001] with Firmware Version 4.8.7),
- a Luna® PIN Entry Device (PED) (Local PED – Firmware Versions 2.0.2 and 2.4.0-3) and iKeys,
- API library and driver software (version 4.5.1),
- Luna® SA 4.5 / 4.5.1 Guidance Documentation (700-010478-002, Revision B).

These are the three non security relevant differences between part numbers 900691-000 and 900691-001:

1. Minor modification to PCB. Improper position of connector interferes with the addition of the PCI bracket for Luna® PCI applications.

2. Addition of tooling holes. Added two tooling holes to aid in assembly of the bottom cover to the PCB. Added plating and RoHS information onto bottom cover drawing.

3. Material contributing to de-lamination. Another material was substituted to correct the problem.

To ensure secure usage a set of guidance documents is provided together with the Luna® PCI configured for use in Luna® SA 4.5.1 with Backup. Details can be found in section 2.5 of this report.

2.2 Security Policy

The TOE provides a physically and logically protected component for the performance of cryptographic functions for:

- Ø key generation
- Ø key storage
- Ø encryption and decryption,
- Ø digital signature and verification

used by application systems that provide cryptographic support functions such as a Certificate Authority/Certification Service Provider (CA/CSP) or Time Stamp Authority (TSA). It includes processors, read-only and random-access memory, and firmware packaged in a tamper-resistant form along with Cryptographic API software that resides on the host computer.

Figure 1 shows the TOE and Figure 2 its appliance deployment configuration – as part of the Luna® SA network-attached appliance.

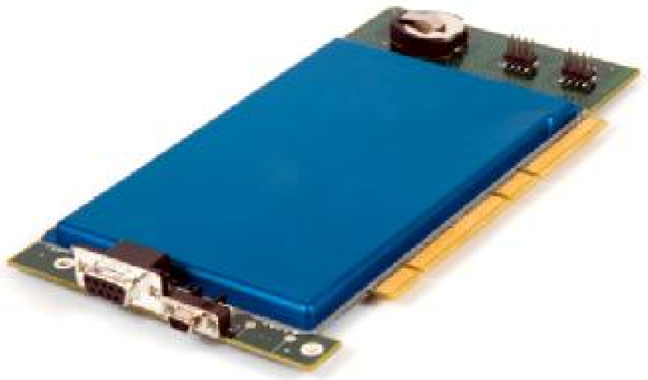

Figure 1. Luna® PCI Cryptographic Module

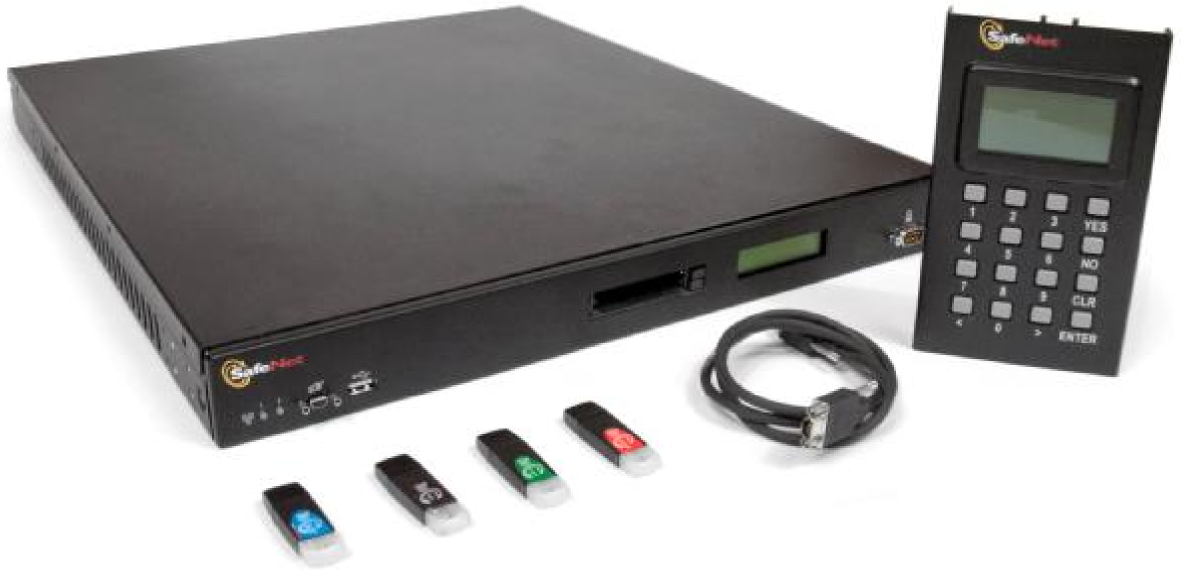

Figure 2 Luna® SA with PED and iKeys

The boundary of the TOE encompasses the following:

1. The Luna® PCI cryptographic module – a printed circuit board in PCI card format enclosed within tamper-resistant metal covers. The printed circuit board hosts volatile and non-volatile memory, a microprocessor, with its associated firmware, data, control and key transfer signal paths, an FPGA that provides an entropy selection function for the on-board random bit generator, input/output controller, power management and a local oscillator.
2. The Luna® PIN Entry Device, which is housed in a separate physical enclosure and, through a physically and electrically separate data port connection to the module, provides a trusted path for the communication of critical security parameters (authentication data and plaintext cryptographic parameters) to and from the module.
3. iKeys, which are USB token devices used to securely store authentication data and other critical security parameters for entry through the Luna® PIN Entry Device.
4. PKCS #11 client library and driver software provides the programming and communications interface normally used to access the cryptographic module.
5. User and Administrative Guidance documentation for the TOE is provided on CD-ROM along with client PKCS #11 software.

The TSF boundary is the Luna® PCI cryptographic module.

The following authenticated roles are supported by the TOE:

- Security Officer (SO) – authorized to install and configure the TOE, set and maintain security policies, and create and delete users (Crypto Officer and Crypto User roles). The TOE can have only one SO.
- Crypto Officer – authorized to create, use, destroy and backup/restore cryptographic objects.
- Crypto User – authorized to use cryptographic objects (e.g., sign, encrypt/decrypt).

The major functions supported by the TOE are outlined below:

Random Number Generation

- FIPS 140-2 validated Deterministic Random Bit Generator (Pseudo-random Number Generator) seeded by internal Hardware Non-deterministic Random Bit Generator. Based on ANSI X9.31, Appendix A section 2.4

Generate Public/Private Key Pairs

- RSA 1024, 2048, 4096 bits key pairs in accordance with ANSI X9.31
- DSA 1024 bits key pairs in accordance with FIPS PUB 186-2
- ECDSA in accordance with FIPS PUB 186-2 and ANSI X9.62

Generate Secret (Symmetric) Keys

- TDES 112, 168 bits in accordance with FIPS PUB 46-3 and ANSI X9.52
- AES 128, 192, 256 bits in accordance with FIPS PUB 197

Secure Key Material Storage and Access

- Key material stored in hardware and strongly encrypted
- Access to private keys and symmetric keys is provided via key handles only

Compute Digital Signatures and Verify Digital Signatures

- RSA 1024 bits, 2048 bits, 4096 bits (PKCS #1 V1.5, PKCS #1 PSS, ANSI X9.31) with SHA-1
- RSA 1024 bits, 2048 bits, 4096 bits (PKCS #1 V1.5, PKCS #1 PSS) with SHA-256, 384, 512
- DSA 1024 bits (FIPS PUB 186-2) with SHA-1
- ECDSA (FIPS PUB 186-2 Appendix 6 recommended curves) with SHA-1

Encrypt / Decrypt Data

- RSA 1024, 2048 and 4096 bits in accordance with PKCS #1 V1.5 and OAEP
- TDES (ECB and CBC mode) 112 and 168 bits in accordance with FIPS PUB 46-3
- AES (ECB and CBC mode) 128 and 256 bits in accordance with FIPS PUB 197

Import (Unwrap) Private Keys

- RSA 1024, 2048 and 4096 bit private keys in PKCS #8 format with TDES and AES in CBC mode

Export (Wrap) and Import (Unwrap) Secret Keys

- TDES, AES with TDES and AES in ECB mode
- TDES, AES with RSA 1024, 2048 and 4096 bits in accordance with PKCS #1 V1.5

The TOE provides the following security services to support the protection of key material and cryptographic services:

- User authentication,
- Access control for the creation and destruction of keys,
- Access control for security administration functions,
- Access control for usage of keys with cryptographic functions,
- Self-test of the TOE.

For more information about the security policy that the TOE implements, please refer to *[ST]* Chapter 2.

2.3 Assumptions and Clarification of Scope

2.3.1 Usage assumptions

The following assumptions about the usage aspects defined by the Security Target have to be

met (for the detailed and precise definition of the assumptions refer to the *[ST]*, chapter 3.2):

A.Correct_DTBS Correct DTBS Content Data

The DTBS-representation submitted to the TOE is assumed to be correct. This requires that the DTBS (e.g. the certificate content data) has been generated and formatted correctly and maintains this correctness until it is passed to the TOE.

A.User_Authentication Authentication of Users

The client application software is assumed to be operating as the TOE user on behalf of a human user and interacts directly, including authenticating, as the user of the TOE. Individual human users authorised to access the TOE cryptographic services may not be known to the TOE itself. The TOE environment performs identification and authentication for the individual users and allows successfully authenticated users to use the client application as their agent for the cryptographic services.

A.Admin Trustworthy TOE Administration

When in operation, it is assumed that there will be a competent authority assigned to manage the TOE and the security of the information that it contains and who can be trusted not to deliberately abuse their privileges so as to undermine security.

A.User_Management User Management

The TOE will not, in general, be aware of the identities of end-users authorised for the TOE services. It is assumed that the management of the individual user assignments for the 3 TOE roles is done in the environment in a trustworthy fashion according to a well-defined policy.

2.3.2 Environmental assumptions

The following assumption about the environmental aspects defined by the Security Target has to be met (for the detailed and precise definition of the assumption refer to the *[ST]*, chapter 3.2):

A.Audit_Support *CSP audit review*

The CSP reviews the audit trail generated and exported by the TOE. The client application receives and stores the audit trail of the TOE for review by the System auditor of the CSP according to the audit procedure of the CSP.

A.Data_Store *Storage and Handling of TOE data*

The TOE environment ensures the confidentiality, integrity and availability of their security relevant data for TOE initialisation, start-up and operation if stored or handled outside the TOE. The TOE environment ensures the availability of the backup data. Examples of these data are verification authentication data, cryptographic key material and documentation of TOE configuration data.

A.Controlled_Access *Physical Security Controls*

When in operation and when stored as a backup, the TOE is assumed to be located within a controlled access facility providing physical security that is adequate to prevent physical access by unauthorized persons.

A.Human_Interface *Interface with Human Users*

The client application will provide an appropriate interface and communication path between human users and the TOE because the TOE does not have a human interface for authentication and management services. The TOE environment transmits identification, authentication and management data of TOE users correctly and in a confidential way to the TOE.

A.Legitimate_FW_Update *Legitimate Firmware Update Signed by the Vendor*

It is assumed that legitimate firmware update packages are digitally signed by the vendor using a private key whose use is restricted to this purpose and that the digital signature is verifiable by an instance of the TOE.

2.3.3 Clarification of scope

The threats listed below are not (entirely) averted by the TOE. Additional support from the operating environment of the TOE is necessary (for detailed information about the threats and how the environment may cover them refer to the *[ST]*, especially chapter 3.3.1 and chapter 8).

T.Data_Manipul Manipulating Data outside of the TOE

User data that is transmitted to the TOE from the client application may be manipulated within the TOE environment before it is passed to the TOE. This may result in the effect that the TOE signs data without the approval of the user under whose control the data is submitted to the TOE. When performed within the client application such manipulations may not be detectable by the TOE itself and therefore this threat needs to be countered within the TOE environment.

T.Insecure_Init Insecure Initialisation of the TOE

Unauthorised CSP personnel or authorised CSP personnel without using adequate organisational controls may initialise the TOE with insecure system data, management data or user data.

An attacker may manipulate the backup data to initialise the TOE insecurely by the restore procedure.

T.Insecure_Oper Insecure Operation of the TOE

The TOE may be operated in an insecure way not detectable by the TOE itself. This includes the use and operation of the TOE within another environment than the intended one (e. g. the TOE may be connected to a hostile system).

T.Malfunction Malfunction of TOE

Internal malfunction of TOE functions may result in the modification of DTBS-representation, misuse of TOE services, disclosure or distortion of CSP-SCD or denial of service for authorized users. This includes the destruction of the TOE as well as hardware failures which prevent the TOE from performing its services. This includes also the destruction of the TOE by deliberate action or environmental failure. Technical failure may result in a insecure operational state violating the integrity and availability of the TOE services. The correct operation of the TOE also depends on the correct operation of critical hardware components. A failure of such a critical hardware component could result in the disclosure or distortion of the CSP-SCD, the modification of DTBS-representation or the ability to misuse services of the TOE. Critical components might be:

- the central processing unit
- a coprocessor for accelerating cryptographic operations
- a physical random number generator
- storage devices used to store the CSP-SCD or the DTBS-representation
- physical I/O device drivers

2.4 Architectural Information

In this chapter the architecture of the TOE is described. The Luna® PCI HSM is contained on a printed circuit board in PCI card format with a PCI bus interface enclosed within two blue coloured metal covers. This hardware form factor is officially identified with Hardware Version VBD-03-0100, but mostly referenced by the name "K5". The printed circuit board hosts a microprocessor that runs the Luna® PCI firmware with version 4.8.7.

The function of the Luna® PIN Entry Device is to communicate authentication data and PINs to and from the Luna® PCI. The iKeys are USB memory devices containing authentication data.

The Luna® PCI has been designed such that users only have access to their 'own' key material stored in 'partitions'. These partitions function as 'private virtual HSMs' for users. Logical access to key material and cryptographic services is provided indirectly through the API Library software on the Luna® SA host computer.

See Figure 3 for an impression of the TOE in its operational environment.

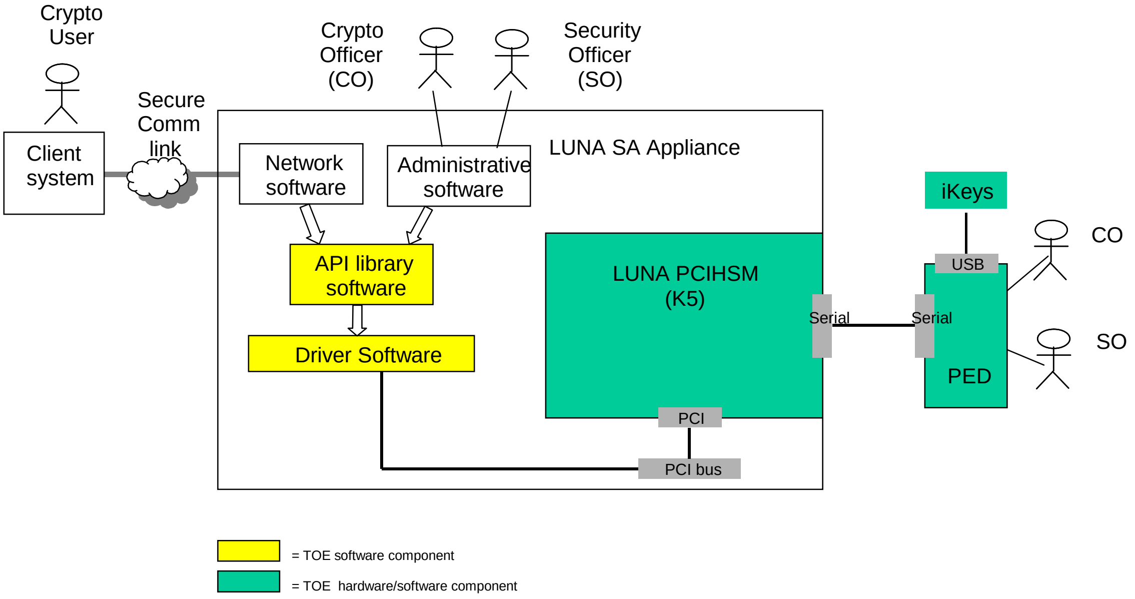

Figure 3 The TOE in its operational environment

All security functionality of the TOE is located in the Luna® PCI HSM. As such the Luna® PCI HSM can be regarded as the TSF.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
Luna SA guidance documentation on CD ROM	700-010478-002, Revision B

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer’s testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The testing by the developer exercised all modules as described in the low level design documentation and all internal interfaces of the TOE. The developer employed four basic techniques:

1. Running scripts on the client system, together these scripts test all PKCS#11 related client functionality in the K5 TSF;
2. Exercising CLI commands on the Luna® SA, together these tests test the administrative functions of the TSF also including software upgrade, backup and recovery.
3. Luna® SA CLI commands in combination with changing hardware conditions, these tests test the physical self-protection and failure handling.
4. Testing the quality of the cryptographic algorithms and the PRNG according to FIPS140-2 certification.

The evaluator independent testing consisted of:

1. Sample testing (4:ATE_IND:2-8) to validate the developer testing by running regression test scripts on the evaluator test configuration. These test scripts were mainly focused on cryptographic functions used by CUs from client systems.
2. Independent tests (4:ATE_IND:2-4) by defining and running interactive tests on the evaluator test configuration using a command line interface on the Luna® SA. These tests were mainly focused on SO and CO responsibilities.

2.6.2 Independent Penetration Testing

Following the Developer Vulnerability Analysis, the following penetration testing effort was made.

1. The evaluators assessed all possible vulnerabilities found during evaluation of the classes. This resulted in a shortlist with a number of possible vulnerabilities to be tested.
2. The evaluators made an analysis of the TOE in its intended environment to check whether the developer vulnerability analysis has assessed all information.
3. In addition the evaluator conducted a brainstorm and concluded from this brainstorm a list of possible vulnerabilities. From these vulnerabilities a list of possible attack scenarios was concluded and from these attack scenarios the evaluator analyzed the level protection using design information. The CEM rating method for attack potential was used for decisions on sufficient trust for TOE protection.

For a number of attack scenarios the evaluator decided that practical testing was needed.

2.6.3 Test Configuration

The test set up for the evaluator independent testing consisted of the following configuration:

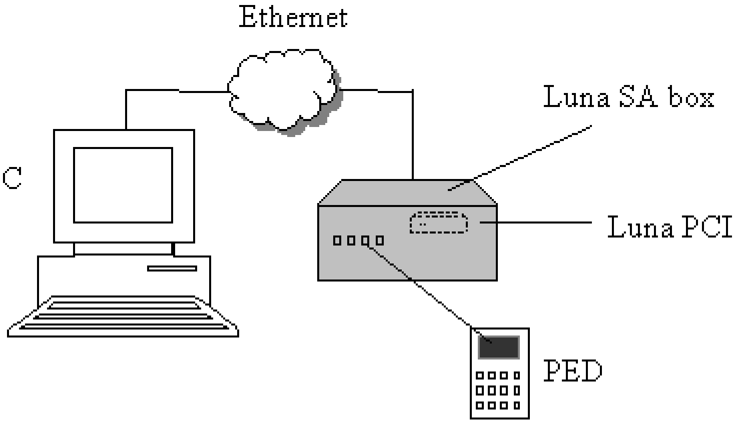

Figure 1 Schematic presentation of the test configuration

The core of the test configuration is a Luna® SA with a K5 Luna® PCI inside and a PED connected to the SA. These components comprise the TOE according to the *[ST]*. The PC runs a terminal emulator to control the SA administrative software in the Luna® (see Figure 1) and the PC also contains test applications to test the client functionality in the Luna® PCI.

The table below shows the specifics of the test configuration:

Device	Manufacturer	Model
Luna® SA	SafeNet	Model GRK-12-0100 SN: 318591 Part 808-000043-001 REV E Software version 4.5.1
Luna® PCI	SafeNet	Model VBD-03-0100 SN: 313023 Part 216-010031-002 [legacy part number 900691-001] Firmware version 4.8.7
Luna® PED	SafeNet	MODEL: PED-03-0101 Firmware Version 2.4.0-3
iKeys	SafeNet	USB memory sticks
Personal computer		PC 2.0 GHz, Window2000

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer’s tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its ST and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number SafeNet Luna® PCI configured for use in Luna® SA 4.5.1 (RF) with Backup.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[1] which references several Intermediate Reports and other evaluator documents. The verdict of each claimed assurance requirement is given in the following tables:

Security Target		**Pass**
Configuration management		**Pass**
Partial CM automation	ACM_AUT.1	Pass
Generation support and acceptance procedures	ACM_CAP.4	Pass
Problem tracking CM coverage	ACM_SCP.2	Pass
Delivery and operation		**Pass**
Detection of modification	ADO_DEL.2	Pass
Installation, generation, and start-up procedures	ADO_IGS.1	Pass
Development		**Pass**
Fully defined external interfaces	ADV_FSP.2	Pass
Security enforcing high-level design	ADV_HLD.2	Pass
Descriptive low-level design	ADV_LLD.1	Pass
Implementation of the TSF	ADV_IMP.2	Pass
Informal correspondence demonstration	ADV_RCR.1	Pass
Informal TOE security policy model	ADV_SPM.1	Pass
Guidance documents		**Pass**
Administrator guidance	AGD_ADM.1	Pass
User guidance	AGD_USR.1	Pass
Life cycle support		**Pass**
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
Well-defined development tools	ALC_TAT.1	Pass
Evaluation of flaw remediation	ALC_FLR.2	Pass
Tests		**Pass**
Analysis of coverage	ATE_COV.2	Pass
Testing: high-level design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing – sample	ATE_IND.2	Pass
Vulnerability assessment		**Pass**
Validation of analysis	AVA_MSU.3	Pass
Strength of TOE security function evaluation	AVA_SOF.1	Pass
Covert Channel Analysis	AVA_CCA.1	Pass
Independent vulnerability analysis	AVA_VLA.4	Pass

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator and is not releasable for public review.

Based on the above evaluation results the evaluation lab concluded the SafeNet Luna® PCI configured for use in Luna® SA 4.5.1 (RF) with Backup, to be **CC Part 2 extended and CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented by ADV_IMP.2, ALC_FLR.2, AVA_CCA.1, AVA_MSU.3 and AVA_VLA.4**. This implies that the product satisfies the security technical requirements specified in the Luna® PCI configured for use in Luna® SA 4.5.1 (RF) with Backup Security Target, Revision 5, July 24th 2013.

The Security Target claims demonstrable conformance to the Cryptographic Module for CSP Signing Operations with Backup Protection Profile, version 0.28, dated 27th October 2003, registered and certified by ANSSI under the reference PP/0308.

2.9 Evaluator Comments/Recommendations

2.9.1 Obligations and hints for the developer

None.

2.9.2 Recommendations and hints for the customer

The customer must/shall follow the provided guidance documentation, in particular:

Ø The requirements placed by the TOE on its operational environment.

Ø Within the scope of the certified configuration, only local PED administration is allowed. The TOE is no longer in a certified configuration if remote RED functionality has been enabled.

3 Security Target

The Luna® PCI configured for use in Luna® SA 4.5.1 (RF) with Backup Security Target, Revision Level 5 is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

API	Application Programming Interface
CA/CSP	Certificate Authority/Certification Service Provider
CO	Crypto Officer (user role of the TOE)
CU	Crypto User (user role of the TOE)
HSM	Hardware Security Module
IT	Information Technology
ITSEF	IT Security Evaluation Facility
NSCIB	Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging
PED	PIN Entry Device
PIN	Personal Identification Number
P/N	Part Number
PP	Protection Profile
SA	Secure Appliance (host computer PC for the TOE)
SO	Security Officer (user role of the TOE)
TOE	Target of Evaluation
TSA	Time Stamp Authority

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, version 2.3, August 2005.
[CEM]	Common Methodology for Information Technology Security Evaluation, version 2.3, August 2005.
[ETR]	Brightsight, Evaluation Technical Report Luna® PCI, EAL4+, Version 2.0, July 24th 2013.
[NSCIB]	Nederlands Schema for Certification in the Area of IT Security, Version 2.0, 1 July 2011.
[PP]	CWA 14167-2 version 0.28 dated 27 October 2003 Cryptographic Module for CSP Signing Operations with Backup (CMCSOB) Protection Profile (PP).
[ST]	Luna® PCI configured for use in Luna® SA 4.5.1 (RF) with Backup Security Target, Revision 5, July 24th 2013

(This is the end of this report).