TNO CERTIFICATION

Date
November 2nd, 2009

Reference
NSCIB-CC-07-09219-CR

Subject

Project number
09219

NSCIB-CC-07-09219

Certification Report

Luna® PCI Configured for Use in Luna SA 4.1 with Backup

TNO CERTIFICATION

TNO CERTIFICATION
HEREBY DECLARES THAT EVALUATION
HAS DEMONSTRATED THAT THE PRODUCT

Luna® PCI Configured for Use in Luna SA 4.1with Backup,
Assurance Package: EAL 4-augmented by ADV_IMP.2,
ALC_FLR.2, AVA_CCA.1, AVA_MSU.3, AVA_VLA.4

Product and version

FROM

SafeNet, Inc. Ottawa, Canada

Sponsor's name and address

COMPLIES WITH THE

Common Criteria for Information Technology Security
Evaluation (CC), Version 2.3

Certification guidelines or standards

AS DEMONSTRATED BY / EVALUATION PERFORMED BY

Brightsight BV, located in Delft, the Netherlands

Testing Laboratory

APPLYING THE

Common Methodology for Information Technology Security
Evaluation (CEM), Version 2.3

NSCIB-CC-07-09219-CR

Certification Report number

THE CERTIFICATE HAS BEEN ISSUED ON

November 12, 2009

1st Issue Date

November 12, 2019

Expiry Date

ISSUED IN: Apeldoorn, the Netherlands

DIRECTOR TNO CERTIFICATION

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 TNO Certification or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TNO Certification or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

CERTIFICATE NUMBER C07-09219

ACCREDITED BY THE COUNCIL FOR ACCREDITATION

Table of contents

Document Information

Date of issue	2nd November 2009
Author	R. Hunter
Version of report	1
Certification ID	NSCIB-CC-07-09219
Sponsor and Developer	SafeNet, Inc.
Evaluation Lab	Brightsight BV
TOE name	Luna® PCI Configured for Use in Luna SA 4.1 with Backup
TOE reference name	Luna® PCI
Report title	Certification Report
Report reference name	NSCIB-CC-07-09219-CR

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 the NSCIB, TNO Certification has the task of issuing certificates for IT security products.

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) is compliant with the requirements of both the international Common Criteria Recognition Arrangement (CCRA) and the European SOG-IS Mutual Recognition Agreement (SOG-IS).

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 in the Netherlands are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TNO Certification 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 TNO Certification 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, TNO Certification 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.

This evaluation contains the components ADV_IMP.2, ALC_FLR.2, AVA_CCA.1, AVA_MSU.3 and AVA_VLA.4 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition, the EAL4-components of these assurance families are relevant.

The European Recognition Agreement approved by the SOG-IS in April 1999 provides mutual recognition of ITSEC and Common Criteria certificates for all evaluation levels (E6, resp. EAL7). This agreement was originally signed by Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom.

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 4.1 with Backup (Luna® PCI). The developer of this product is SafeNet, Inc. with corporate headquarters located in Belcamp MD, USA and Engineering office located in Ottawa, Canada. SafeNet, Inc. also acts 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 ST 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 Security IC Platform Protection Profile. This protection profile was registered and certified by DCSSI under the reference PP/0308.

The Luna® PCI configured for use in the Luna SA 4.1 with Backup was evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on October 20th 2009, The certification procedure was conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security [NSCIB]. The certification was completed on November 2nd 2009 with the preparation of this Certification Report.

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 configured for use in the Luna SA 4.1 with Backup, 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 4.1 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][1] 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].

TNO Certification, as the NSCIB Certification Body, declares that the Luna® PCI configured for use in the Luna SA 4.1 with Backup evaluation meets all the conditions of the Arrangement on the 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.

---

[1] The evaluation technical report is a NSCIB document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4+ evaluation is the Luna® PCI Configured for Use in Luna SA 4.1 with Backup from SafeNet, Inc. located in Ottawa, Canada.

This report pertains to the TOE, the Luna® PCI configured for use in the Luna SA 4.1 with Backup, which comprises the following main components:

- Ø The Luna® PCI cryptographic module in a PCI Card form factor (900691-000 with Firmware Version 4.6.1)
- Ø a Luna® PIN Entry Device (PED) (Firmware Version 2.0.2) and iKeys
- Ø API library and driver software (version 4.1)
- Ø Luna SA 4.1 Guidance Documentation (900506-037, Revision B)

To ensure secure usage, guidance documentation as described above is provided on a CD-ROM. 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:

Ø   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.

Ø   Crypto Officer – authorized to create, use, destroy and backup/restore cryptographic objects.

Ø   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
Ø   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
Ø   RSA 1024, 2048, 4096 bits key pairs in accordance with ANSI X9.31

Ø   DSA 1024 bits key pairs in accordance with FIPS PUB 186-2

Ø   ECDSA in accordance with FIPS PUB 186-2 and ANSI X9.62

Generate Secret (Symmetric) Keys

Ø   TDES 112, 168 bits in accordance with FIPS PUB 46-3 and ANSI X9.52

Ø   AES 128, 192, 256 bits in accordance with FIPS PUB 197

Secure Key Material Storage and Access

Ø   Key material stored in hardware and strongly encrypted

Ø   Access to private keys and symmetric keys is provided via key handles only

Compute Digital Signatures and Verify Digital Signatures
Ø   RSA 1024 bits, 2048 bits, 4096 bits (PKCS #1 V1.5, PKCS #1 PSS, ANSI X9.31) with SHA-1

Ø RSA 1024 bits, 2048 bits, 4096 bits (PKCS #1 V1.5, PKCS #1 PSS) with SHA-256, 384, 512

Ø DSA 1024 bits (FIPS PUB 186-2) with SHA-1

Ø ECDSA (FIPS PUB 186-2 Appendix 6 recommended curves) with SHA-1

Encrypt / Decrypt Data

Ø RSA 1024, 2048 and 4096 bits in accordance with PKCS #1 V1.5 and OAEP

Ø TDES (ECB and CBC mode) 112 and 168 bits in accordance with FIPS PUB 46-3

Ø AES (ECB and CBC mode) 128 and 256 bits in accordance with FIPS PUB 197

Import (Unwrap) Private Keys

Ø 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

Ø TDES, AES with TDES and AES in ECB mode

Ø 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:

Ø User authentication,

Ø Access control for the creation and destruction of keys,

Ø Access control for security administration functions,

Ø Access control for usage of keys with cryptographic functions,

Ø 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 assumptions about the environmental 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.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:

- Ø the central processing unit
- Ø a coprocessor for accelerating cryptographic operations
- Ø a physical random number generator
- Ø storage devices used to store the CSP-SCD or the DTBS-representation
- Ø 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 4.6.1.

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.

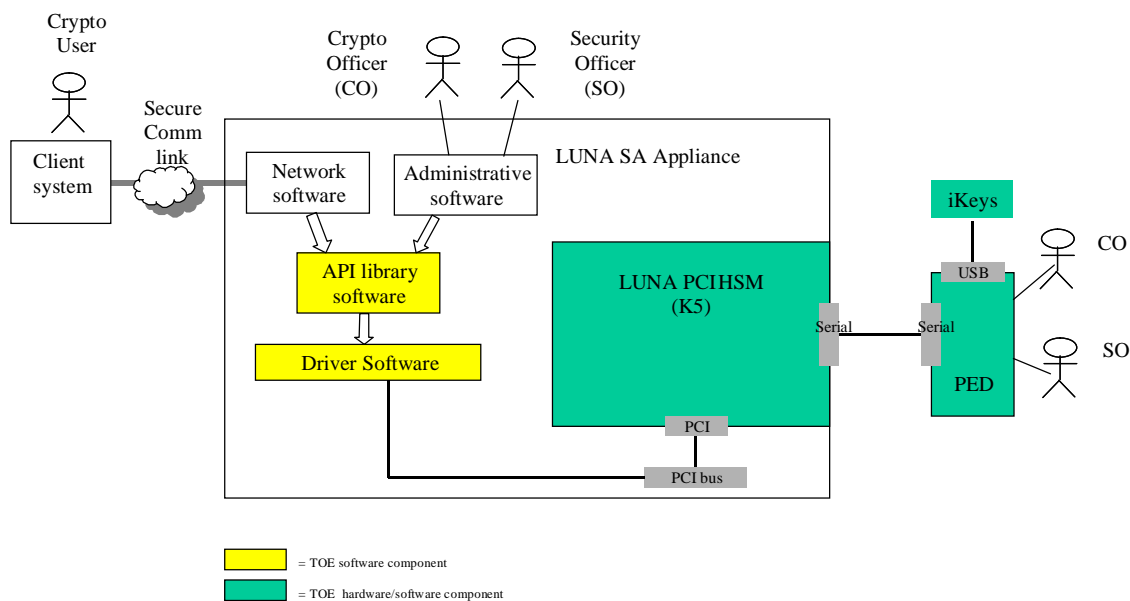See Figure 3 for an impression of the TOE in its operational environment.

Figure 3 The TOE in its operational environment

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

2.5 Documentation

The following electronic documentation is provided as part of the product in the form of a CD-ROM by the developer to the customer:

Identifier	Version
Luna SA 4.1 Guidance Documentation	900506-037, 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

Developer Testing
The developer employed four basic techniques:
- Ø Running scripts on the client system, together these scripts test all PKCS#11 related client functionality in the K5 TSF;
- Ø Exercising CLI commands on the Luna SA, together these tests test the administrative functions of the TSF also including software upgrade, backup and recovery;
- Ø Luna SA CLI commands in combination with changing hardware conditions, these tests test the physical self protection and failure handling;
- Ø Testing the quality of the cryptographic algorithms and the PRNG according to FIPS 140-2 certification.

The functional tests performed by the developer cover all TSF security functions.

Evaluator testing

The functional testing by the evaluator was been performed using a developer test configuration conformant to the *[ST]*. This system had been tested in a network environment also containing other SafeNet, Inc. HSM products and a variety of client systems. The total testing strategy covered installation testing (according to the user guidance), regression testing, administrative testing, vulnerability testing including IP testing, system upgrade testing and specific feature testing. The TOE was tested in its end user configuration ready for user commands (meaning firmware version 4.6.1 is successfully loaded).

The evaluator identified four techniques to simulate the TSF security functions:
- Ø Regression testing using scripts that generate commands to the TSF, these scripts test the commands with varying parameters;
- Ø Procedures for administrative TSF functions using CLI commands;
- Ø Combinations of the two above;
- Ø Testing the cryptographic algorithms and the PRNG according to FIPS 140-2 procedures.

2.6.2 Test Configuration

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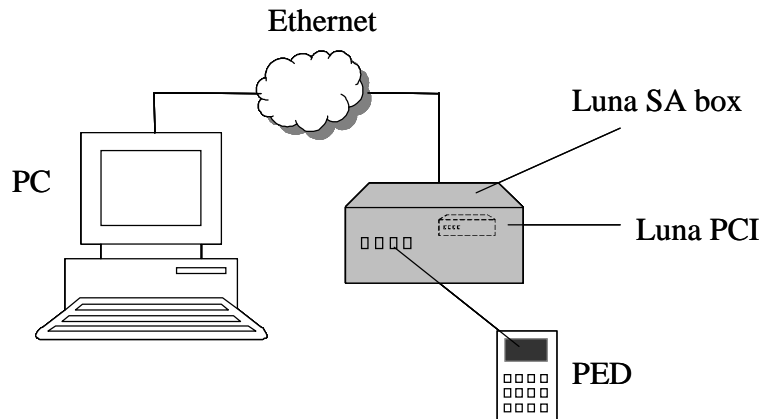

Figure 4 Schematic presentation of the test configuration

The core of the test configuration is a Luna SA with a K5 Luna PCI inside and a Luna® PIN Entry Device 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 4) 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, Inc.	Model GRK-07-0100
		SN: 0950071
		Part 808-00001-001
Luna PCI	SafeNet, Inc.	Luna K5
		Model VBD-03-0100
Luna PED	SafeNet, Inc.	MODEL: PED-03-0101 SN:0202045
iKeys	SafeNet, Inc.	USB memory sticks
Personal computer		PC 2.0 GHz, Window2000

2.6.3 Independent Penetration Testing

From analysing the TOE resistance using design information an attack potential analysis rating assurance on protection could be decided for a number of attack scenarios. For some attack scenarios penetration testing was expected to be extremely difficult and for those scenarios additional detailed design information was requested from the developer (code details) for further detailed analysis. For a number of attack scenarios it was decided to conduct practical testing.

When analysing the user guidance the evaluator remarked that network attacks could be a serious threat to the TOE. From analysing ATE evidence it was found that SafeNet, Inc. conducts extensive network penetrations tests. Because of its importance to the security of the TOE the evaluator decided to also perform network penetration test in addition to the logical attacks described earlier.

The following penetration testing was conducted:
- Ø EMA testing for listening to the Luna® PCI cryptographic module using EMA signals
- Ø Penetrate the Luna® PIN Entry Device for tapping of PED communication
- Ø Logical testing
- Ø Network penetration testing

2.6.4 Testing Results

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

The evaluator concludes that all independent tests conducted confirm the expected behaviour of the TOE. The evaluators have found no exploitable vulnerabilities for the TOE in its intended environment. No residual vulnerabilities were identified.

2.7 Evaluated Configuration

The TOE, as it has been evaluated, in its appliance deployment configuration (as part of the Luna® SA network-attached appliance) was set up and configured using the guidance documents referred to in section 2.5 of this report.

2.8 Results of the Evaluation

The evaluation lab documented its evaluation results in the *[ETR]*[2] which references several Intermediate Reports. The verdict of each claimed assurance requirement is given in the following table:

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

---

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

During this evaluation, the following versions of documents were used:
- Ø Common Criteria for Information Technology Security Evaluation, Parts I, II and III, version 2.3
- Ø Common Methodology for Information Technology Security Evaluation, version 2.3
- Ø Final Interpretation for RI # 69 – Informal Security Policy Model.

Because under CC2.3 the CEM stops at EAL4 an agreed methodology was needed for EAL4+. The work item descriptions in the BSI document AIS34 (see *[AIS34]*) have been used as common agreed basis between the scheme and evaluation lab for the work items related to the claimed EAL4 augmentations.

Based on the above evaluation results the evaluation lab concluded that the Luna® PCI Configured for Use in Luna SA 4.1 with Backup to be **CC Part 2 extended**, **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, AVA_VLA.4** as required by the **Cryptographic Module for CSP Signing Operations with Backup Protection Profile (PP/0308), version 0.28, dated 27th October 2003**. The minimum SOF-level is: **High**.

This implies that the product satisfies the security technical requirements specified in the Luna® PCI Configured for Use In Luna® SA 4.1 With Backup Security Target, Revision level 11, dated September 17th 2009.

2.9 Evaluator Comments/Recommendations

From the analysis of the assurance obtained from the hardware and software design analysis and from the validation testing and the penetration testing it is concluded that the TOE is sufficiently protected against attacks with attack potential high, provided that necessary security measures in the non-IT environment are effectively in place. The evaluators have found no exploitable vulnerabilities for the TOE in its intended environment.

3 Security Target

The Security Target, "Luna® PCI Configured for Use In Luna® SA 4.1 With Backup Security Target", Revision level 11, dated September 17th 2009, unique ID CR-2386 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:

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BSI	Bundesamt für Sicherheit in der Informationstechnik
CSP	Certification-Service-provider
CSP-SCD	CSP signature creation data
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
ITSEF	IT Security Evaluation Facility
NSCIB	Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging
PCI	Peripheral Component Interconnect
PKCS	Public Key Cryptography Standard
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
TDES	Triple DES
TNO	Netherlands Organization for Applied Scientific Research

5 Bibliography

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

[AIS34]   AIS34 Evaluation methodology for CC Assurances Classes for EAL5+ , version 2, 24/10/2008.

[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, Evaluation Methodology, Version 2.3, August 2005

[ETR]   09-RPT-036 v2.0 Evaluation Technical Report Luna® PCI, October 12th 2009.

[NSCIB]   Netherlands Schema for Certification in the Area of IT Security, Version 1.2, 9 December 2004.

[PP]   CWA-14167-2 version 0.28, dated 27th October 2003 Cryptographic Module for CSP Signing Operations with Backup Protection Profile (PP/0308).

[ST]   Luna® PCI Configured for Use In Luna® SA 4.1 With Backup Security Target, Revision level 11, dated September 17th.