Certification Report

Luna PCI-E Cryptographic Module, Firmware Version 6.10.9

Sponsor and developer:	***SafeNet Inc.*** **20 Colonnade Road, Suite 200** **K2E 7M6, Ottawa ON** **Canada**
Evaluation facility:	***Brightsight*** **Delftechpark 1** **2628 XJ Delft** **The Netherlands**
Report number:	**NSCIB-CC-179205-CR**
Report version:	**1**
Project number:	**179205**
Author(s):	**Denise Cater/Wouter Slegers**
Date:	**22 December 2017**
Number of pages:	**14**
Number of appendices:	**0**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)
Certificate number	**CC-17-179205**
	TÜV Rheinland Nederland B.V. certifies:
Certificate holder and developer	**SafeNet Inc.** **20 Colonnade Road, Suite 200, K2E 7M6, Ottawa ON, Canada**
Product and assurance level	**Luna PCI-E Cryptographic Module, Firmware Version 6.10.9** Assurance Package: ▪ EAL4 augmented with ALC_FLR.2 and AVA_VAN.5
Project number	**179205**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL2

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 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. 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.

SOGIS Mutual Recognition Agreement for components up to EAL7

Validity

Date of 1st issue : **29-12-2017**
Certificate expiry : **29-12-2022**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

C.C.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

TÜVRheinland®
Precisely Right.

CONTENTS:

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, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site 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 or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, 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 or site satisfies the security requirements stated in the (site) security target.

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

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

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-E Cryptographic Module, Firmware Version 6.10.9. The developer of the Luna PCI-E Cryptographic Module, Firmware Version 6.10.9 is SafeNet Inc. located in Ottawa, Canada and they also act 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 TOE provides a logically protected component for the performance of cryptographic functions for key generation, key storage, encryption and decryption, key wrapping, secure key transport, key establishment, digital signature generation and verification used by application systems that provide cryptographic support functions such as a Certificate Authority/Certification Service Provider (CA) or Time Stamp Authority (TSA).

Luna SA is the most common host for the Luna PCI-E Cryptographic Module and when acting as the host system, it allows clients to authenticate to the TOE to access cryptographic services. Access to TOE services is provided using supplied host software (non-TOE) that interfaces to the Crypto Module using its PCI-E interface.

The TOE Security Functionality is contained within the Luna PCI-E cryptographic module (a printed circuit board in PCI-E card format enclosed within tamper-evident metal covers). The Luna SA is outside the scope of the TOE.

The TOE has been originally evaluated by Brightsight B.V. located in Delft, The Netherlands and was certified on 29 June 2017 under certification ID CC-17-38671. The re-evaluation also took place by Brightsight B.V. and was completed on 15 December 2017 with the approval of the ETR. The re-evaluation procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*. It should be noted that the re-evaluation was for the same firmware version of the TOE as the original and one (of four) hardware version included in the scope of the TOE for the original evaluation. This re-evaluation activity was to add physical protection claims (FPT_PHP.1 and FPT_PHP.3) and to increase the vulnerability analysis from AVA_VAN.4 to AVA_VAN.5.

The security evaluation re-used the evaluation results of previously performed evaluations under certification ID CC-17-38671. A full, up to date vulnerability analysis has been made, as well as renewed testing.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Luna PCI-E Cryptographic Module, Firmware Version 6.10.9, 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-E Cryptographic Module, Firmware Version 6.10.9 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 EAL4 augmented (EAL4(+)) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Flaw Reporting Procedures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the 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.

---

[1] The Evaluation Technical Report 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 is the Luna PCI-E Cryptographic Module, Firmware Version 6.10.9 from SafeNet Inc. located in Ottawa, Canada.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	808-00015-003	n/a
Software	Luna PCI-E Cryptographic module Firmware	6.10.9

To ensure secure usage a set of guidance documents is provided together with the Luna PCI-E Cryptographic Module, Firmware Version 6.10.9. Details can be found in section 2.5 of this report.

2.2 Security Policy

The Target of Evaluation – TOE (i.e. Luna PCI-E Cryptographic Module) is a Hardware Security Module (HSM) in the form of a PCI-E card that typically resides within a custom computing or secure communications appliance that is operated in a controlled environment. The TOE features hardware key management to maintain the confidentiality and integrity of digital signature and encryption keys. Key material is generated, stored, and used exclusively within the Luna PCI-E cryptographic module to prevent compromise. The cryptographic functionality includes:

- Key generation; symmetric (TDES and AES) keys and asymmetric key pairs (RSA and ECDSA),
- Key storage,
- Encryption and decryption using both symmetric and asymmetric cryptography, and
- Digital signature generation and verification using RSA and ECDSA key pairs.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The TOE must be operated within protected physical environment that limits physical access to the TOE to authorised individuals. The TOE environment described for this TOE is consistent with that specified in *[PP]*. **It should be noted that the environment described in *[PP]* is required to prevent attackers from getting physically near the TOE.** As a result, for any TOE claiming OE.ENV from *[PP]*, attacks on the physical enclosure of the TOE, as well as attacks on any interfaces not exposed to the host computer (such as serial and USB interfaces on the device), are **out of scope of these evaluations**. The user of the TOE is reminded to operate the TOE in a physically and procedurally secure environment.

The TOE environment must protect the user data in the red area of the IT system and controls the exchange data between the red and black area of the IT system according to the IT security policy.

2.4 Architectural Information

The TOE subsystems, depicted in Figure 1 below, are summarised in the following table.

Subsystem	Description
Hardware subsystem	PowerPC 440EPx Processor (CPU), with SafeXcel-3120 Security Processor w/ 64MBytes private Flash Memory and SafeXcel-1746 Accelerator Bridge for (PCI <-> PCIe) and a FPGA supports the Bus Logic nvRAM in the RTC 64 MBytes Flash Memory and 256 MBytes SDRAM Memory Voltage and temperature are monitored Entire K6 cryptographic module security boundary is covered in opaque, thermally conductive potting material and has removal switches
Bootloader Subsystem	The boot loader is responsible for ensuring the integrity of the underlying platform memory and for ensuring the integrity of the main firmware load. The boot loader loads all other embedded subsystems onto the cryptographic module. The bootloader is built from a separate make file.
Linux Subsystem	The Luna PCI-E cryptographic module includes Linux Kernel version 2.6.28 at its core. The HSM/PCI-e is a single application on top of the Linux system.
Main Subsystem	This subsystem is responsible for: Providing an entry point for the process that provides all HSM services by starting an infinite loop function in the communication subsystem. Initializing and zeroing the HSM, Setting the cryptographic module policy values, Applying capability and policy updates, Initiating firmware updates and rollbacks, Maintaining the firmware version number, the communication protocol number, and the amount of global storage available across the HSM.
Communication Subsystem	This subsystem contains the main loop for receiving commands and dispatching to other subsystems.
Session Manager Subsystem	This subsystem maintains information on active sessions alongside authentication status for each of the sessions.
User Subsystem	This subsystem maintains user management and user authentication services for the cryptographic module.
Rule subsystem	This subsystem maintains capabilities and policies.
Param Subsystem	This subsystem is interface for other subsystems to the Rule subsystem.
Key Management subsystem	This subsystem provides security-enforcing functions. It processes all commands that involve the generation, wrapping/unwrapping and derivation of keys. Key destruction is performed within the Object Handler subsystem.
Cryptographic Operations Subsystem	This subsystem is responsible for cryptographic operations on the Luna HSM.

Subsystem	Description
Master Tamper Key (MTK) Subsystem	This subsystem handles the MTK recovery.
Object Handler Subsystem	This subsystem maintains all data structures.
Memory Management Subsystem	This subsystem manages the allocation of memory.

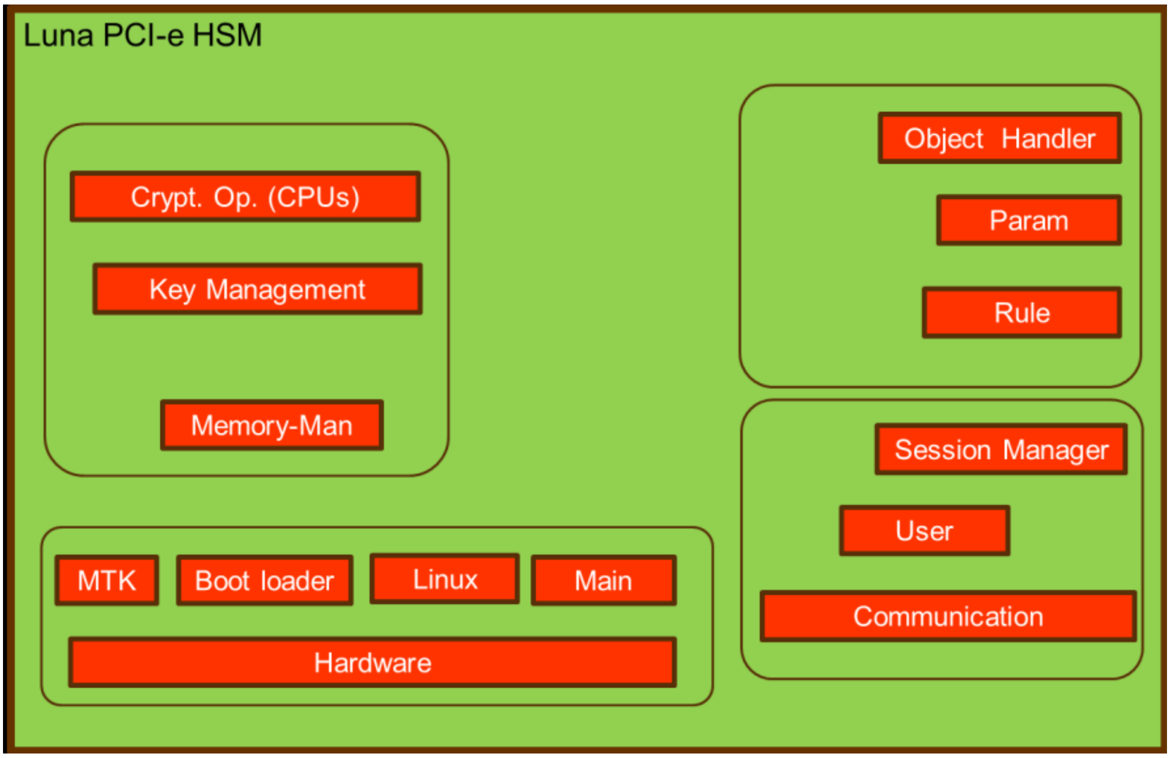

Figure 1 TOE subsystems

2.5 Documentation

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

Identifier	Version
Guidance Documentation: CR-4119, Luna PCI-E Cryptographic Module, Common Criteria User Guidance	7.0

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

As reported for the original evaluation in [CR], the developer created a testing environment that tested all logical TOE interfaces. This includes all typical deployment scenarios, all crypto functionality and the less common functionality. Additionally, security mechanisms providing the following functionality were tested:

- Zeroisation,
- internal object integrity protection,

- PCI-E bus read/write supervision to protect against attempts from the host to maliciously access sensitive internal TOE memory regions.

During the original evaluation, the evaluator repeated and confirmed the results of all automated tests presented by the vendor, as well as some manual tests that could not be exercised from external interfaces; including those for zeroisation, internal object integrity protection and PCI-E bus read/write supervision. The evaluator also devised and executed an additional twenty (20) independent functional tests to further demonstrate the behaviour of the major TOE functionalities such as User authentication, Crypto rule enforcement, Access control rule enforcement, Key Attributes and Mechanisms, Configuration, and Cloning.

For some of the functional tests a small code change was added to the TOE firmware to support a trigger signal. The evaluator reviewed this change and concluded that the extra code only starts and stops the trigger, but do not influence the functional behaviour of the TOE. Therefore, it was concluded the change did not impact the test results of the functional tests.

For the re-evaluation, which considered the addition of an AVA_VAN.5 claim and physical protection SFRs (FPT_PHP), the developer provided the additional test reports covering the following:

- Hardware tamper tests,
- Physical security tests,
- Software testing related to potential bugs that were found as a result of code review and static analysis.

During the re-evaluation activities the evaluator repeated the hardware tamper tests, as well as three (3) additional independent functional tests that arose from the further analysis performed by the evaluator for AVA_VAN.5.

2.6.2 Independent Penetration Testing

As reported for the original evaluation in [CR], the evaluator independent penetration tests were devised after performing a methodical vulnerability analysis. To identify possible vulnerabilities for further analysis, the evaluator performed the following activities:

- SFR design analysis: SFR implementation details were examined in the SFR design analysis. During this examination several possible vulnerabilities were collected.
- Additional security analysis: Once the implementations of the SFRs were understood, some coverage checks were performed on SFR relevant aspects, resulting in collection of several possible vulnerabilities.
- CWE vulnerability focus: Using inspiration from the CWE weaknesses collection, the evaluator collected a list of security questions and related answers. This approach ensured that the evaluator was forced to think in terms of vulnerabilities from all different angles and improved completeness in the vulnerability analysis. Also during this examination several possible vulnerabilities were collected.
- Public vulnerability search: Also during this search several possible vulnerabilities were collected.

Having collected possible vulnerabilities, the evaluator then analysed each possible vulnerability in turn, either producing a satisfactory analysis to show the possible vulnerability is not applicable to the TOE, or it was examined further as a potential vulnerability. For each potential vulnerability an attack description and attack rating was produced, additional code review was performed, and/or additional functional/penetration test cases were devised. From this analysis a total of eight (8) penetration tests were devised and executed in the original evaluation, comprised of 5 logical tests, 1 fuzzing test and 2 side channel tests (timing and emissions).

During the re-evaluation activities the evaluator performed an extended public domain search for vulnerabilities as well as additional source code analysis. This gave rise to execution of one (1) additional penetration test to investigate emissions.

2.6.3 Test Configuration

For the original evaluation, the developer provided the evaluator with the TOE (hardware 808-00015-001[2] and firmware 6.10.9), code and tools necessary to recreate the test environments used for developer testing. For execution of some test cases it was necessary for a development board to be used and/or modified bootloader firmware and trigger code. The evaluators assessed the differences between the TOE and development hardware/firmware, and determined that the differences did not have an impact on the behaviour being demonstrated. These test environments were used for repeating developer testing and also for independent functional and penetration testing performed by the evaluator. See the *[ETR]* for details.

For the re-evaluation activities the evaluators used TOE hardware 808-00015-003, with firmware version 6.10.9.

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.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e. from the current best cryptanalytic attacks published, has been taken into account.

2.7 Re-used evaluation results

Although no further TOE development has taken place since the original evaluation (CC-38671) and the TOE version is unchanged, at the request of the sponsor this is a new certification with heavy re-use of the previous certification (CC-38671). Documentary evaluation results of the earlier version of the TOE have been re-used, but vulnerability analysis and penetration testing has been renewed as well as increasing the vulnerability analysis from AVA_VAN.4 to AVA_VAN.5.

No sites have been visited as part of this re-evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Luna PCI-E Cryptographic Module, Firmware Version 6.10.9, together with the PCI-E hardware identifier as detailed in Section 2.1.

The TOE can be delivered either as a standalone PCIe card or embedded in a Luna SA appliance. The delivery methods are identified in [ST] and are detailed in the Guidance Documentation (Section 2.5).

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[3] which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the Luna PCI-E Cryptographic Module, Firmware Version 6.10.9, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_FLR.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

---

[2] The single version of TOE hardware was used in testing, and the evaluators produced an equivalency rationale to demonstrate the behaviour demonstrated for this hardware variant was representative of the other 3 TOE hardware variants.

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

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. Please note that the documents contain relevant details with respect to the resistance against certain attacks.

The SO is responsible for configuring the HSM in its CC compliant mode of operation, by enabling or disabling the appropriate Module Policy settings as specified in the user guidance. In particular it is important that FIPS mode is enabled and the partition policy "21: Enable High Availability Recovery" is disabled. Also if the partition policy "11: Enable Changing Key Attributes" is disabled then the partition policies "0: Allow Private Key Cloning, "1: Allow Private Key Wrapping", "4: Allow Secret Key Cloning" and "5: Allow Secret Key Wrapping" must be disabled as well.

As noted in the user guidance, it is important that the following operations are performed using the local PED during initial setup and during administration of roles:

- All SO login operations e.g. during role or partition creation and initial configuration;
- Initialisation of CO and CU roles where PED keys are written including presentation of the challenge secret via the PED.
- Reset of the CO or CU challenge secrets to an HSM generated random value where the value is presented to the end user via the PED display.

The customer must ensure that only the serial cable provided with the TOE (as part of the Luna SA appliance delivery) is used when presenting PIN/password and Token using a device connected directly to the TOE. This is a specialised cable that incorporates features not uniformly present in all COTS serial cables, which minimise the risk of radiated emission during operation of a connected device.

The TOE environment described for this TOE is consistent with that specified in *[PP]*. **It should be noted that the environment described in *[PP]* is required to prevent attackers from getting physically near the TOE.** As a result, for any TOE claiming OE.ENV from *[PP]*, attacks on the physical enclosure of the TOE, as well as attacks on any interfaces not exposed to the host computer (such as serial and USB interfaces on the device), are **out of scope of these evaluations**. The user of the TOE is reminded to operate the TOE in a physically and procedurally secure environment.

In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the implemented cryptographic algorithms was not rated in the course of this evaluation. To fend off attackers with high attack potential appropriate cryptographic algorithms with adequate key lengths must be used (references can be found in national and international documents and standards).

3 Security Target

The Security Target Luna PCI-E Cryptographic Module, Rev 23, 05 December 2017 *[ST]* 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:

CO	Crypto Officer
CU	Crypto User
HA	High Availability
HSM	Hardware Security Module
IT	Information Technology
ITSEF	IT Security Evaluation Facility
NSCIB	Netherlands scheme for certification in the area of IT security
PED	PIN Entry Device
PP	Protection Profile
SO	Security Officer
TOE	Target of Evaluation

TÜVRheinland®
Precisely Right.

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 3.1 Revision 5, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.

[CERT] Certification Report Luna PCI-E Cryptographic Module, Firmware version 6.10.9, version 1, 29 June 2017

[ETR] Evaluation Technical Report Luna PCI-E Cryptographic Module EAL4+, RPT-16-673, Version 3.0, 15 December 2017.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.4, 27 September 2017.

[PP] Protection profiles for TSP Cryptographic Modules – Part 5, Cryptographic Modules for Trust Services, prEN 419221-5, version 1.0, 02 May 2017

[ST] Security Target Luna PCI-E Cryptographic Module, Rev 23, 05 December 2017.

(This is the end of this report).