Certification Report

Thales Luna K7 Cryptographic Module

Sponsor and developer: ***Thales DIS CPL Canada Inc***
20 Colonnade Road, Suite 200,
Ottawa, Ontario K2E 7M6
Canada

Evaluation facility: ***SGS Brightsight BV***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-195307-CR2**

Report version: **1**

Project number: **195307_2**

Author(s): **Denise Cater**

Date: **18 July 2022**

Number of pages: **12**

Number of appendices: **0**

Head Office:
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 Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

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 licence 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, 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.

Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since 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.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Thales Luna K7 Cryptographic Module. The developer of the Thales Luna K7 Cryptographic Module is Thales DIS CPL Canada 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 Thales Luna K7 Cryptographic Module (i.e. the TOE) is a Hardware Security Module (HSM) in the form of a PCI-E card (Thales Luna PCIe HSM). It is operated in a controlled environment and can be used either as a standalone device to be inserted in a server, or as a device embedded in a Thales Luna Network HSM.

The TOE is also suitable for use in support of electronic signature and electronic sealing operations, certificate issuance and revocation, time stamp operations, and authentication services, as identified by the (EU) No 910/2014 regulation *[EU-REG]* of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eIDAS). For that purpose, the present Security Target has been explicitly written to comply with *[PP 419221-5]*; the TOE supports Assigned Keys, External Key Storage and Key Import/Export operations as defined in the PP.

The TOE was evaluated initially by SGS Brightsight B.V. located in Delft, The Netherlands and was certified on 06 October 2020. The re-evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 18 July 2022 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

This second issue of the Certification Report is a result of a “recertification with major changes”.

The major changes are the addition of two hardware variants bringing the total number of hardware variants to seven and the addition of two firmware variants resulting in a total of three firmware variants.

The security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Thales Luna K7 Cryptographic Module, 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 Thales Luna K7 Cryptographic Module 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 the TOE 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]* (Parts I, II and III).

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. Note that the certification results apply only 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 available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Thales Luna K7 Cryptographic Module from Thales DIS CPL Canada Inc located in Ottawa, Canada.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	808-000048-002 808-000048-003 808-000073-001 808-000073-002 808-000066-001 808-000069-001 808-000070-001	n/a
Software	Firmware	7.7.0, 7.7.1, or 7.7.2
	Bootloader	1.1.1, 1.1.2 or 1.1.4

To ensure secure usage a set of guidance documents is provided, together with the Thales Luna K7 Cryptographic Module. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

- Storage and management of cryptographic keys inside containers (i.e. partitions). The TOE supports a mandatory Admin Partition and several (optional) User Partitions. For a given partition, the management and usage of the related key material is restricted to the roles assigned to that partition, therefore enforcing a strict isolation between the different partitions managed inside the TOE.
- Enforcement of per-partition authenticated user roles with varying privileges.
- Enforcement of user authentication (either token-based or password-based) and per-key authorization before allowing users to perform TSF-mediated actions as defined in *[ST]*.
- Cryptographic functions (as fully detailed in *[ST]*) including:
  - Digital signature generation and verification
  - Message digest generation
  - Message authentication code generation and verification
  - Encryption and decryption (symmetric and asymmetric)
  - Key generation
  - Key derivation
  - Generation of shared secret values
  - Cryptographic support for one time password and other non-PKI based authentication mechanisms
  - Random number generation
- Key management functions.
- Secure Trusted Channel (STC) for confidentiality and integrity protection of communication between TOE and Remote Client Applications.
- Firmware update.
- Auditing functionalities.
- Self protection mechanisms:
  - Voltage and temperature monitors and zeroization response
  - Passive shield (for K7 TOE variant) / active shield (for K7+ TOE variant).

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. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

It should be noted that user-defined ECC curves are not included in this certification. Only the curves defined in *[ST]* section 6.3 are included in the evaluation scope of this certification.

Note that EN 419221-5 Protection Profile [PP 419221-5] claims the environment for the TOE protects against loss or theft of the TOE, deters and detects physical tampering, protects against attacks based on emanations of the TOE, and protects against unauthorised software and configuration changes on the TOE and the hardware appliance in which it is contained ("OE.Env Protected operating environment").

The ST follows the PP and also claims OE.Env, thus the environment in which the TOE is used must ensure the above protection.

Any threats violating these objectives for the environment are not considered.

2.4 Architectural Information

The Thales Luna K7 Cryptographic Module (i.e. the TOE) is a standalone PCI-E card in the form of 'Thales Luna PCIe HSM' or as an embedded module inside the 'Thales Network HSM'. The TOE can fulfil general purpose HSM use cases, where assured cryptographic services alongside generation and management of cryptographic keys are required. The TOE also supports the option for further customization of the HSM for a given integration through the ability to load 3rd party developed code (non-TOE) in the form of Functional Modules (FM) onto the HSM.

Local client applications reside in the same hardware appliance as the TOE, e.g. in the case of the TOE being a PCI-E card inside a server, local client applications are the applications running within the same server boundary and using the TOE's services through the PCI-E bus. Another example of local client application is an embedded application running inside the physical boundary of the TOE and using the Luna FM API. Note that the secure environment is considered sufficient to provide the authentication, confidentiality and integrity protection needed for communication between the TOE and local applications.

External client applications communicate remotely with the TOE through a network connection and over a secure channel identified as Secure Trusted Channel (STC) which provides authentication of its end-points and protection of confidentiality and integrity of data sent over the channel.

The high level logical architecture of the TOE can be depicted as follows:

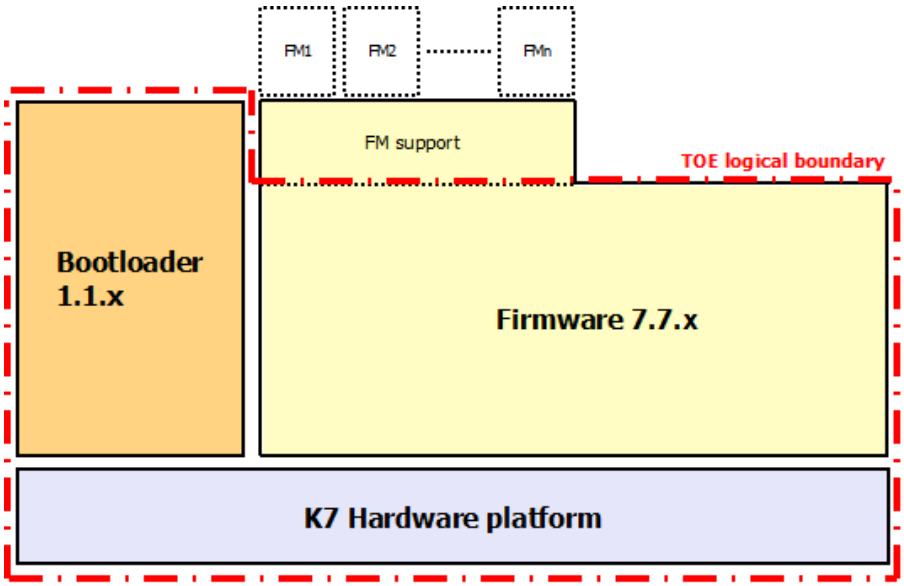

Figure 1 Thales Luna K7 Cryptographic Module, TOE logical boundary

2.5 Documentation

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

Identifier	Version
007-013968-001, Thales Luna K7(+) Cryptographic Module, Common Criteria User Guidance – Part1: Preparative Procedures	Revision H, 06 May 2022.
007-000465-001, Thales Luna K7(+) Cryptographic Module, Common Criteria User Guidance – Part2: Operational Guidance (General)	Revision I, 06 May 2022.
007-000466-001, Thales Luna K7(+) Cryptographic Module, Common Criteria User Guidance – Part3: eIDAS Guidance	Revision H, 06 May 2022.
007-000467-001, Thales Luna K7(+) Cryptographic Module, Common Criteria User Guidance – Part4: TOE Integration for use in Composite Evaluation	Revision G, 06 May 2022.

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 developer has performed extensive testing on functional specification and module-to-module interaction level. Several proprietary automated test suites are used, supported by execution of cryptographic test suites (such as known answer tests) and to demonstrate FPT_PHP.1 and FPT_PHP.3 requirements from [PP 419221-5] (and hence compliance with ISO/IEC 19790:2012 Security Level 3) physical hardware tests were also performed.

The underlying hardware are extendable to composite evaluations, providing the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators in the baseline evaluation and this re-evaluation, the developer test environment was used. The evaluators repeated the developer tests, as well as executing additional test cases designed by the evaluator. During the baseline evaluation this also includedtesting of random number generation in accordance with [AIS31].

2.6.2 Independent penetration testing

The AVA_VAN.5 assurance class requires the evaluator to conduct a methodical vulnerability analysis based on publicly available source of information and based on structured examination of the evidence while performing other evaluation activities (ASE, ADV, AGD, ALC & ATE).

Given the restrictions imposed by the PP (which prevents any physical attack and any side channel attack that requires physical proximity to the TOE), the evaluator focused on vulnerabilities related to logical design/architectural flaws in the TOE implementation that would lead intended users to abuse the TOE.

With the exception of one test case, all penetration tests were logical test cases. Considering that physical access to the TOE is prevented by the protected environment, hardware attacks to the TOE, as well as any attack that requires side channel techniques based on power/EM emanation, were excluded from the test plan. The devised test cases focus on fuzzing over externally visible commands, abuse of policy settings and timing measurements when performing cryptographic operations.

A total of 12 weeks of effort were applied to the execution of the penetration test cases during the baseline evaluation. The evaluators performed an analysis the penetration testing results obtained during the baseline evaluation and confirmed that the results are still valid as there have been no developments in tooling or techniques for the logical tests since the tests were executed in the baseline evaluation.

2.6.3 Test configuration

[ST] lists seven part numbers for TOE variants. The evaluators assessed the differences and concluded that they were not security impacting.

During the baseline evaluation most evaluator independent functional tests were performed on a variant of each of the K7 and K7+. All evaluator penetration tests were performed on a K7 variant with a selection also performed on a K7+ variant. The PED used to demonstrate PED authentication was not one of those listed in the ST, but the evaluator assessed the differences and determined they would not impact the TOE behaviour.

During this re-evaluation, all tests were performed on Luna K7 TOE. The HW 808-000048-003 version, FW 7.7.2 version, and Bootloader 1.1.4 version used for independent tests are in line with *[ST]*. No modification was needed, except for one test which required a slightly modified variant of the firmware.

2.6.4 Test 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.

For composite evaluations, please consult the *[ETRfC]* for details.

2.7 Reused Evaluation Results

This is a re-certification. Documentary and test evaluation results of the earlier version of the TOE have been reused, but vulnerability analysis has been renewed.

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE (including data centre sites), by use of four Site Technical Audit Reuse reports.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Thales Luna K7 Cryptographic Module and associated version numbers as detailed in *Identification of Target of Evaluation*.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents. To support composite evaluations according to *[COMP]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that must be considered when this TOE is used as platform in a composite evaluation.

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

Based on the above evaluation results the evaluation lab concluded the Thales Luna K7 Cryptographic Module, 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]*.

The Security Target claims 'strict' conformance to the Protection Profile *[PP 419221-5]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. Certain aspects of the TOE's security funcçctionality, 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. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must 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. For the evolution of attack methods and techniques to be covered, the customer 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 cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: **User-defined ECC curves**.

3 Security Target

The Thales Luna K7 Cryptographic Module - Security Target, 002-010985-001, Rev M, 06 May 2022 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information Technology
FM	Functional Modules
HSM	Hardware Security Module
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
RNG	Random Number Generator
STC	Secure Trusted Channel
TOE	Target of Evaluation
TSP	Trusted Service Provider

5 Bibliography

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

[AIS31] AIS31, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 2.1, 02 December 2011

[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

[ETR] Evaluation Technical Report Thales Luna K7/K7+ – EAL4+, 22-RPT-159, Version 4.0, 18 July 2022

[ETRfC] Evaluation Technical Report for Composition Thales Luna K7/K7+ – EAL4+, 22-RPT-721, Version 3.0, 18 July 2022

[EU-REG] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[JIL-AAPHD] Application of Attack Potential to Hardware Devices with Security Boxes, Version 3.0, July 2020

[JIL-AMHD] Attack Methods for Hardware Devices with Security Boxes, Version 3.0, February 2020 (sensitive with controlled distribution)

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019

[PP 419221-5] EN 419 221-5:2018, Protection Profiles for TSP Cryptographic Modules – Part 5 Cryptographic Module for Trust Services, v1.0, registered under the reference ANSSI-CC-PP-2016/05-M01, 18 May 2020

[ST] Thales Luna K7 Cryptographic Module - Security Target, 002-010985-001, Rev M, 06 May 2022

(This is the end of this report.)