Certificate Report

Version 1.0

20 November 2020

CSA_CC_19003

for
Thales Luna K7 Cryptographic Module

From

Thales

This page is left blank intentionally

Foreword

Singapore is a Common Criteria Certificate Authorizing Nation, under the Common Criteria Recognition Arrangement (CCRA). The current list of signatory nations and approved certification schemes can be found at the CCRA portal:

https://www.commoncriteriaportal.org

The Singapore Common Criteria Scheme (SCCS) is established for the info-communications technology (ICT) industry to evaluate and certify their IT products against the requirements of the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 (ISO/IEC 15408) and Common Methodology for Information Technology Security Evaluation (CEM) Version 3.1 (ISO/IEC 18045) in Singapore.

The SCCS is owned and managed by the Certification Body (CB) under the ambit of Cyber Security Agency of Singapore (CSA).

The SCCS certification signifies that the target of evaluation (TOE) under evaluation has been assessed and found to provide the specified IT security assurance. However, certification does not guarantee absolute security and should always be read with the particular set of threats sought to be addressed and assumptions made in the process of evaluation.

This certification is not an endorsement of the product.

Amendment Record

Version	Date	Changes
1.0	Nov 2020	Released

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

Executive Summary

This report is intended to assist the end-user of the product in determining the suitability of the product in their deployed environment.

The Target of Evaluation (TOE) is the Thales Luna K7 Cryptographic Module and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS). The TOE comprises of the following components:

Identifier	Version
Hardware	808-000048-002
	808-000073-001
	808-000066-001
	808-000069-001
	808-000070-001
Bootloader	1.1.1, 1.1.2, or 1.1.4
Firmware	7.7.0

Table 1 - TOE components identifier

The list of guidance documents to use with the product in its certified configuration is as follows.

Name and version	Version
007-013968-001, Thales Luna K7(+) Cryptographic Module, Common Criteria User Guidance – Part1: Preparative Procedures	Revision E
007-000465-001, Thales Luna K7(+) Cryptographic Module, Common Criteria User Guidance – Part2: Operational Guidance (General)	Revision F
007-000466-001, Thales Luna K7(+) Cryptographic Module, Common Criteria User Guidance – Part3: eIDAS Guidance	Revision E
007-000467-001, Thales Luna K7(+) Cryptographic Module, Common Criteria User Guidance – Part4: TOE Integration for use in Composite Evaluation	Revision D

Table 2 - List of guidance documents

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 can fulfil general purpose HSM use cases, where assured cryptographic services alongside generation and management of cryptographic keys is required. The TOE is also suitable for use by Trust Service Providers (TSP) supporting 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 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eIDAS).

The evaluation of the TOE has been carried out by Brightsight B.V., an approved CC test laboratory, at the assurance level CC EAL 4 augmented with AVA_VAN.5 (Advanced Methodical Vulnerability Analysis) and completed on 6 November 2020.

The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality
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 PIN or PW-based) and per-key authorization before allowing users to perform TSF-mediated actions as defined in [ST].
Cryptographic functions covering: ▪ 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).

Table 3: TOE Security Functionalities

Please refer to the Security Target [1] for more information.

The assets to be protected by the TOE has been defined. Based on these assets, the TOE Security Problem Definition has been defined in terms of Assumptions, Threats and Organisation Policies. These are outlined in Chapter 4 of the Security Target [1]

This Certification covers the configurations of the TOE as outlined in Chapter 5.3 of this report.

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate applies only to the specific version and release of the IT product in its evaluated configuration. This certificate is not an endorsement of the IT product by SCCS, and no warranty of the IT product by SCCS, is either expressed or implied.

Table of Contents

1 Certification

1.1 Procedure

The certification body conducts the certification procedure according to the following criteria:

- Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 [2] [3] [4];
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 5 [5]; and
- SCCS scheme publications [6] [7] [8]

1.2 Recognition Agreements

The international arrangement on the mutual recognition of certificates based on the Common Criteria Recognition Arrangement had been ratified on 2 July 2014. The arrangement covers certificates with claims of compliance against collaborative protection profiles (cPPs) or evaluation assurance levels (EALs) 1 through 2 and ALC_FLR. Hence, the certification for this TOE is covered partially by the CCRA for the components up to EAL2.

The Common Criteria Recognition Arrangement mark printed on the certificate indicates that this certification is recognised under the terms of this agreement by all signatory nations listed on the CC web portal (https://www.commoncriteriaportal.org).

2 Validity of the Certification Result

This Certification Report only applies to the version of the TOE as indicated. The Certificate is valid till **19 November 2025**[1].

In cases of changes to the certified version of the TOE, the validity may be extended to new versions and releases provided the TOE sponsor applies for Assurance Continuity (i.e. re-certification or maintenance) of the revised TOE, in accordance with the requirements of the Singapore Common Criteria Scheme (SCCS).

The owner of the Certificate is obliged:

- When advertising the Certificate or the fact of the product's certification, to refer to and provide the Certification Report, the Security Target and user guidance documentation herein to any customer of the product for the application and usage of the certified product;
- To inform the SCCS immediately about vulnerabilities of the product that have been identified by the developer or any third party; and
- To inform the SCCS immediately in the case that relevant security changes in the evaluated life cycle has occurred or the confidentiality of documentation and information related to the TOE or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is no longer valid.

[1] Certificate validity could be extended by means of assurance continuity. Certificate could also be revoked under the conditions specified in SCCS Publication 3 [8]. Potential users should check the SCCS website (www.csa.gov.sg/programmes/csa-cc-product-list) for the up-to-date status regarding the certificate's validity.

3 Identification

The Target of Evaluation (TOE) is: Thales Luna K7 Cryptographic Module

The following table identifies the TOE deliverables.

Identifier	Version
Hardware	808-000048-002
	808-000073-001
	808-000066-001
	808-000069-001
	808-000070-001
Bootloader	1.1.1, 1.1.2, or 1.1.4
Firmware	7.7.0

Figure 1 - TOE Deliverables

The guide for receipt and acceptance of the above-mentioned TOE are described in the set of guidance documents.

Name and version	Version
007-013968-001, Thales Luna K7(+) Cryptographic Module, Common Criteria User Guidance – Part1: Preparative Procedures	Revision E
007-000465-001, Thales Luna K7(+) Cryptographic Module, Common Criteria User Guidance – Part2: Operational Guidance (General)	Revision F
007-000466-001, Thales Luna K7(+) Cryptographic Module, Common Criteria User Guidance – Part3: eIDAS Guidance	Revision E
007-000467-001, Thales Luna K7(+) Cryptographic Module, Common Criteria User Guidance – Part4: TOE Integration for use in Composite Evaluation	Revision D

Table 4 - Guidance Document (part of TOE deliverables)

Additional identification information relevant to this Certification procedure as follows:

TOE	Thales Luna K7 Cryptographic Module
Security Target	Thales Luna K7 Cryptographic Module Security Target, 002-010985-001, Rev J, 25 September 2020
Developer	Thales
Sponsor	Thales
Evaluation Facility	Brightsight B.V.
Completion Date of Evaluation	6 November 2020
Certification Body	Cyber Security Agency of Singapore (CSA)
Certificate ID	CSA_CC_19003
Certificate Validity	5 years from date of issuance

Table 5: Additional Identification Information

4 Security Policy

The TOE's Security Policy is expressed by the set of Security Functional Requirements listed and implemented by the TOE.

The TOE implements policies pertaining to security functional class "User Data Protection".

Specific details concerning the above mentioned security policy can be found in Chapter 5 of the Security Target [9].

5 Assumptions and Scope of Evaluation

5.1 Assumptions

The assumptions defined in the Security Target [9] and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE environment and are listed in the tables below:

Environmental Assumptions	Description
OE.ExternalData Protection of data outside TOE control	Where copies of data protected by the TOE are managed outside of the TOE, client applications and other entities shall provide appropriate protection for that data to a level required by the application context and the risks in the deployment environment. This includes protection of data that is exported from, or imported to, the TOE (such as audit data and encrypted keys). In particular, any backups of the TOE and its data shall be maintained in a way that ensures appropriate controls over making backups, storing backup data, and using backup data to restore an operational TOE. The number of sets of backup data shall not exceed the minimum needed to ensure continuity of the TSP service. The ability to restore a TOE to an operational state from backup data shall require at least dual person control (i.e. the participation and approval of more than one authenticated administrator).
OE.Env Protected operating environment	The TOE shall operate in a protected environment that limits physical access to the TOE to authorized Administrators. The TOE software and hardware environment (including client applications) shall be installed and maintained by Administrators in a secure state that mitigates against the specific risks applicable to the deployment environment, including (where applicable): ▪ Protection against loss or theft of the TOE or any of its externally stored assets

	▪ Inspections to deter and detect tampering (including attempts to access side-channels, or to access connections between physically separate parts of the TOE, or parts of the hardware appliance) ▪ Protection against the possibility of attacks based on emanations from the TOE (e.g. electromagnetic emanations) according to risks assessed for the operating environment ▪ Protection against unauthorized software and configuration changes on the TOE and the hardware appliance ▪ Protection to an equivalent level of all instances of the TOE holding the same assets (e.g. where a key is present as a backup in more than one instance of the TOE).
OE.DataContext Appropriate use of TOE functions	Any client application using the cryptographic functions of the TOE shall ensure that the correct data are supplied in a secure manner (including any relevant requirements for authenticity, integrity and confidentiality). For example, when creating a digital signature over a DTBS the client application shall ensure that the correct (authentic, unmodified) DTBS/R is supplied to the TOE, and shall correctly and securely manage the signature received from the TOE; and when certifying a public key the client application shall ensure that necessary checks are made to prove possession of the corresponding private key. The client application may make use of appropriate secure channels provided by the TOE to support these security requirements. Where required by the risks in the operational environment a suitable entity (possibly the client application) shall perform a check of the signature returned from the TOE, to confirm that it relates to the correct DTBS. Client applications shall be responsible for any required logging of the uses made of the TOE services, such as signing (or sealing) events. Similar requirements shall apply in local use cases where no client application need be involved, but in which the TOE and its user data (such as keys used for signatures) need to be configured in ways that will support the need for security requirements such as sole control of signing keys. Appropriate procedures shall be defined for the initial creation of data and continuing operation of the TOE according to the specific risks applicable to the deployment environment and the ways in which the TOE is used.

OE.Uauth Authentication of application user	Any client application using the cryptographic services of the TOE shall correctly and securely gather identification and authentication/authorization data from its users and securely transfer it to the TOE (protecting the confidentiality of the authentication/authorization data as required) when required to authorize the use of TOE assets and services.
OE.AuditSupport Audit data review	The audit trail generated by the TOE will be collected, maintained and reviewed by a System Auditor according to a defined audit procedure for the TSP.
OE.AppSupport Application security support	Procedures to ensure the ongoing security of client applications and their data shall be defined and followed in the environment, and reflected in use of the appropriate TOE cryptographic functions and parameters, and appropriate management and administration actions on the TOE. This includes, for example, any relevant policies on algorithms, key generation methods, key lengths, key access, key import/export, key usage limitations, key activation, cryptoperiods and key renewal, and key/certificate revocation.

Table 6: Environmental Assumptions

Details can be found in section 4.2 of the Security Target [1].

5.2 Clarification of Scope

The TOE physical boundary is the SafeNet Luna K7 PCI-E card with passive (K7) and active (K7+) shielding. The TOE is intended to be operated in a protected operating environment (OE.Env) 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.

Secure channel may exist between the TOE with external and local client applications but these are not covered within the scope of evaluation.

The scope of evaluation is limited to the claims made in the Security Target [1].

5.3 Evaluated Configuration

The Thales Luna K7 is a hardware security module in the form of a PCI-E card that 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 can fulfil general purpose HSM use cases, where assured cryptographic services alongside generation and management of cryptographic keys is required and is also suitable for use by Trust Service Providers (TSP) supporting electronic signature and electronic sealing operations, certificate issuance and revocation, time stamp operations, and authentication services,

Note that the TOE is not aware of the context in which a cryptographic function is used. Any such context is therefore the responsibility of client applications used by the trust service provider or operator, and these client applications need to use the cryptographic functions in an appropriate way. In general, this will be achieved by suitable configuration of the TOE and its stored data.

5.4 Non-Evaluated Functionalities

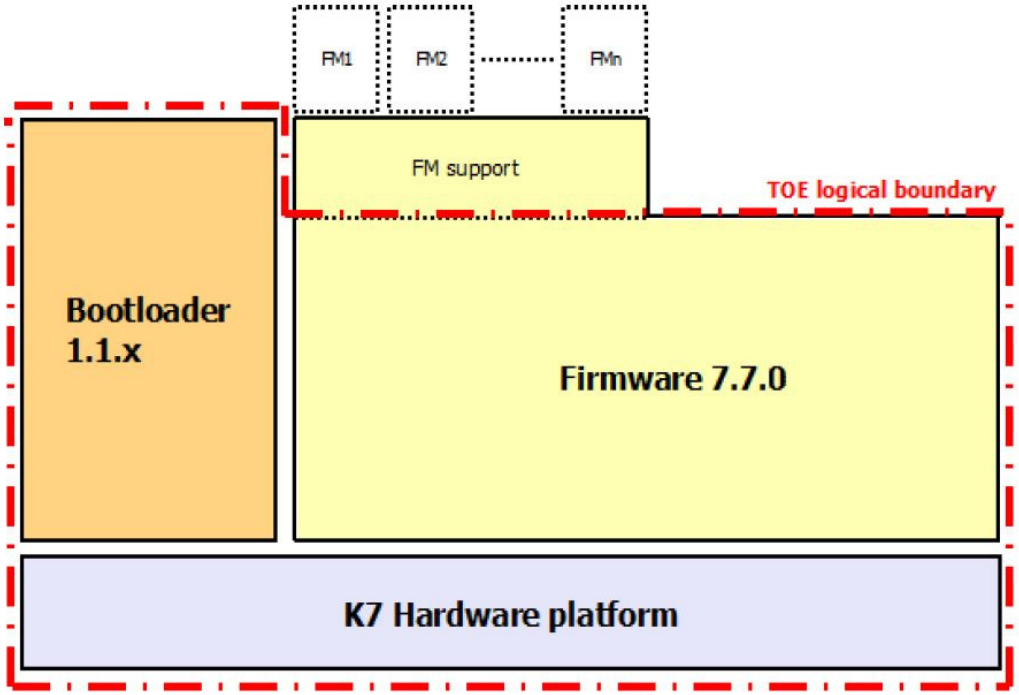
There are no non-evaluated functionalities within the scope as clarified in section 5.2.

5.5 Non-TOE Components

The TOE does not require additional components for its operation.

6 Architecture Design Information

As described in the Security Target *[1]*, the high-level logical architecture of the TOE can be depicted as follows:



7 Documentation

The evaluated documentation as listed in Table 4 - Guidance Document (part of TOE deliverables) is being provided with the product to the customer. These documentations contains the required information for secure usage of the TOE in accordance with the Security Target.

8 IT Product Testing

8.1 Developer Testing (ATE_FUN)

8.1.1 Test Approach and Depth

The developer performed functional testing covering all TSFIs and module-to-module interactions. Several proprietary automated test suites were used, along with cryptographic tests suites such as known-answer tests and physical hardware tests to fulfil FPT_PHP.1 and FPT_PHP.3 requirements and thus compliance to ISO/IEC 19790:2012 Security Level 3.

8.1.2 Test Configuration

The TOE used for testing is configured according to the TOE guidance document [10] [11] [12] [13].

8.1.3 Test Results

The test results provided by the developer covered all operational functions as

described in the Security Target [1].

All test results from all tested environment showed that the expected test results are identical to the actual test results.

8.2 Evaluator Testing (ATE_IND)

8.2.1 Test Approach and Depth

The automated test cases in the developer's test plan were repeated on K7 and K7+. These includes tests that confirm the correct execution of electronic signature/seal operation against known data to be signed as part of the PP's requirement.

The evaluator's strategy for devising independent tests was based on the following:

- Tests that expand on partially tested features of the TOE
- Tests that provide an alternate approach with respect to the testing strategy presented by the developer
- Tests that expand on the policy enforcement concept
- Test that address otherwise untested functionalities
- Tests that are mandated by the PP
- Tests that are mandated by the AIS31 standard

8.2.2 Test Configuration

A detailed test description was provided in the ATE document. The evaluator used the developer's test environment at the developer's premises to perform independent testing. Prior to running tests, the evaluator performed identification of the test environment and verification of the TOE.

8.2.3 Test Results

The developer's test reproduced were verified by the evaluator to conform to the expected results from the test plan.

8.3 Penetration Testing (AVA_VAN)

8.3.1 Test Approach and Depth

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 previous evaluation activities (ASE, ADV, AGD, 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 design/architectural flaws that would lead intended users to abuse the TOE. For this reason, the evaluator needed to find a methodical approach to scout the TOE implementation

searching for such design/architectural flaws.

The evaluator's strategy for performing vulnerability analysis was based on the following:

1. Identification of areas of concern using open source publicly maintained weakness enumeration database. Areas of concerns includes Accessibility, Cryptography, Secure Channel etc.
2. Iteratively, for each SFR, the evaluator formulates security relevant questions for each identified area of concern which are then translated into TOE specific possible vulnerabilities.
3. The evaluator then justifies whether a possible vulnerability is removed or sufficiently mitigated by the TOE implementation/environment/functional testing evidence. For instance, in response to vulnerabilities identifying usage of weak cryptographic algorithms, the developer modified the ST claim and guidance documentation to exclude usage of TDES and SHA-1.
4. Residue Potential vulnerabilities are then addressed in the context of penetration tests and further code review.

The approach chosen by the evaluator is commensurate with the assurance component chosen (AVA_VAN.5) treating the resistance of the TOE to an attack with the High attack potential.

The evaluator found no exploitable vulnerability in the TOE when operated in the evaluated configuration. No residual risks were identified.

9 Results of the Evaluation

The Evaluation Technical Report (ETR) was provided by the CCTL in accordance with the CC, CEM and requirements of the SCCS. As a result of the evaluation, the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 augmented by ALC_FLR.2 and AVA_VAN.5 assurance package

This implies that the TOE satisfies the security requirements specified in the Security Target [1].

10 Obligations and recommendations for the usage of the TOE

The documents as outlined in Table 2 - List of guidance documents contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition, all aspects of Assumptions, Threats and OSPs as outlined in the Security Target [1] that are not covered by the TOE shall be fulfilled by the operational environment of the TOE.

Potential user of the product shall consider the results of the certification within his/her system risk management process. As attack methods and techniques evolve over time, he/she should define the period of time whereby a re-assessment of the TOE is required and convey such request to the sponsor of the certificate.

No additional recommendation was provided by the evaluators.

11 Acronyms

CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CCTL	Common Criteria Test Laboratory
CSA	Cyber Security Agency of Singapore
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SAR	Security Assurance Requirement
SCCS	Singapore Common Criteria Scheme
SFR	Security Functional Requirement
TOE	Target of Evaluation
TSF	TOE Security Functionality

12 Bibliography

[1] Thales, “Thales Luna K7 Cryptographic Module Security Target, 002-010985-001, Rev J,” 2020.

[2] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [Document Number CCMB-2017-04-001]. Version 3.1 Revision 5,” 2017.

[3] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components [Document Number CCMB-2017-04-002], Version 3.1 Revision 5,” 2017.

[4] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components [Document Number CCMB-2018-04-003] Version 3.1 Revision 5,” 2017.

[5] Common Criteria Maintenance Board (CCMB), “Common Methodology for Information Technology Security Evaluation - Evaluation Methodology [Document Number CCMB-2017-04-004], Version 3.1 Revision 5,” 2017.

[6] Cyber Security Agency of Singapore (CSA), “SCCS Publication 1 - Overview of SCCS, Version 5.0,” 2018.

[7] Cyber Security Agency of Singapore (CSA), “SCCS Publication 2 - Requirements for CCTL, Version 5.0,” 2018.

[8] Cyber Security Agency of Singapore (CSA), “SCCS Publication 3 - Evaluation and Certification, Version 5.0,” 2018.

[9] Brightsight B.V., “Evaluation Technical Report Thales Luna K7/K7+ EAL 4+, 19-RPT-515 Version 6.0,” 5 October 2020.

[10] “007-013968-001, Thales Luna K7(+) Cryptographic Module, Common Criteria User Guidance – Part1: Preparative Procedures, Revision E, 25th September 2020”.

[11] “007-000465-001, Thales Luna K7(+) Cryptographic Module, Common Criteria User Guidance – Part2: Operational Guidance (General), Revision F, 25th September 2020.”.

[12] “007-000466-001, Thales Luna K7(+) Cryptographic Module, Common Criteria User Guidance – Part3: eIDAS Guidance, Revision E, 25th September 2020”.

[13] “007-000467-001, Thales Luna K7(+) Cryptographic Module, Common Criteria User Guidance – Part4: TOE Integration for use in Composite Evaluation, Revision D, 25th September 2020”.

[14] EN 419 221-5:2018 version 1.0, “Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trusted Services, v1.0, registered under the reference ANSSI-CC-PP-2016/05-M01,” 18 May 2020.

[15] Brightsight B.V., , “Evaluation Technical Report for Composition Thales Luna K7/K7+ EAL 4+, 20-RPT-983, v3.0,” 5 October 2020.

----------End of Report ----------