Certification Report

TESS v7.1 Platform Revision 1.0

Sponsor and developer: ***Thales DIS France SAS***
6 rue de la Verrerie
Meudon Cedex
France

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-2400099-01-CR**

Report version: **1**

Project number: NSCIB-**2400099-01**

Author(s): **Jordi Mujal**

Date: **07 February 2025**

Number of pages: **12**

Number of appendices: **0**

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, TrustCB 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 TrustCB 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 TrustCB 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, TrustCB 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

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 TESS v7.1 Platform Revision 1.0. The developer of the TESS v7.1 Platform Revision 1.0 is Thales DIS France SAS located in Meudon Cedex, France 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, as an eSE product, ensures the data is stored in a safe place and information is given to only authorized applications and people. It is a multi-applicative security device, intended to host e.g. payment, eID, access control, transport and/or loyalty applications. The CSP part of the TOE is a cryptographic service provider package, providing cryptographic services for the protection of the confidentiality and the integrity of user data, and for entity authentication.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 07 February 2025 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the TESS v7.1 Platform Revision 1.0, 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 TESS v7.1 Platform Revision 1.0 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_DVS.2 (Sufficiency of security measures) 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).

TrustCB 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 TESS v7.1 Platform Revision 1.0 from Thales DIS France SAS located in Meudon Cedex, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	S3NSN6H	Rev. 0
Software	TESS v7.1 OS	V1.19 (OS Information: **D0027115DA0113)**
	TESS v7.1 Patch	**00010000**

To ensure secure usage a set of guidance documents is provided, together with the TESS v7.1 Platform Revision 1.0. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 4.5.

2.2 Security Policy

The platform implements (at least) the following services:

- Management and control of the communication between the card and external entities
- Card basic security services as follows:
    - Checking environmental operating conditions using information provided by the IC
    - Checking life cycle consistency
    - Providing secure cryptography primitives and algorithms
    - Ensuring the security of the PIN and cryptographic key objects
    - Generating random numbers
    - Handling secure data object and backup mechanisms
    - Managing memory content
- Enforcement of the Javacard firewall mechanism
- Standard Application Programming Interfaces (APIs) such as the Javacard API (JCAPI) and the Global Platform API (GPAPI).
- Proprietary Thales API: Secure API which provides security services to applications
- Initialization of the Issuer Security Domain (ISD) and management of the card life cycle
- Creation and management of Supplementary Security Domains (SSD)
- SCP02, SCP03, SCP11, SCP80 and SCP81 support
- RSA, ECC support
- CSP, a cryptographic service provider package, providing cryptographic services for the protection of the confidentiality and the integrity of user data, and for entity authentication.

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 7.2 of the *[ST]*.

2.3.2 Clarification of scope

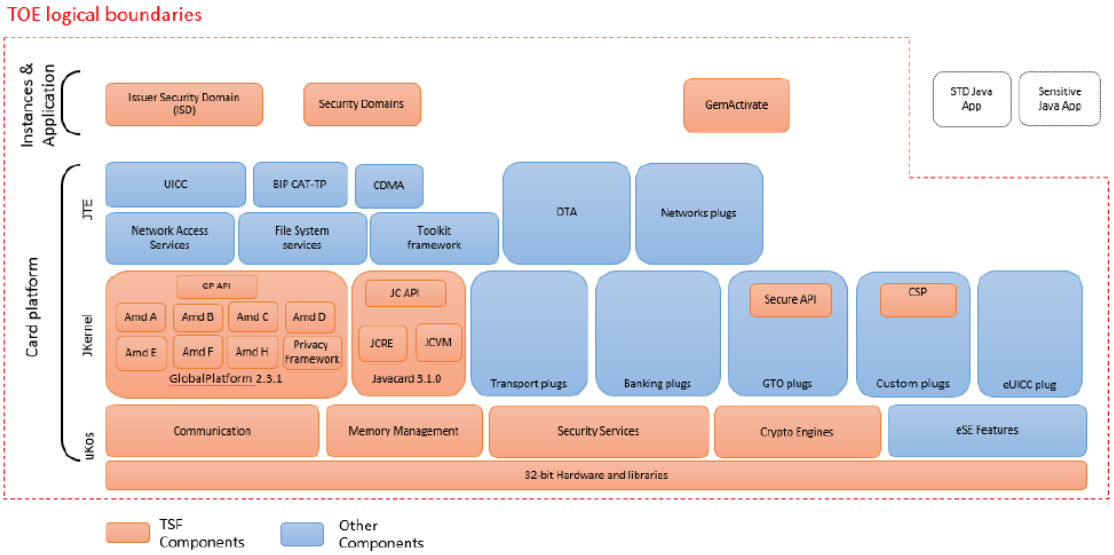
The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

There are no security claims on the following components of the platform which do not form part of the TOE security functionality:

- The eUICC and Javacard Telecom Environment (JTE) functionalities.
- The CSP implements the following modes but they are out of scope of the TOE:
  - EACv1
  - Integrated mapping (DH and ECDH)
  - Generic mapping (DH)

2.4 Architectural Information

The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows:



2.5 Documentation

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

Identifier and Version
D1619041 - Operational guidance on CC platforms - TESS v7.1, v1.0, June 2024
D1620259 - Operational guidance on CC platforms for VA - TESS v7.1, v1.0, June 2024
D1619040 - Preparative guidance on CC platforms - TESS v7.1, v1.0, June 2024
D1578508 - Guidance for profile set up vs. JavaCard System Protection Profile, v1.6, July 4, 2024

GlobalPlatform Card, Composition Model Security Guidelines for Basic Applications, v2.0, November 2014
D1516176 - Guidance for Secure application development on Thales Embedded Secure Solutions, v4.1, December 16, 2024
D1344508 - Patch Loading Management for Certified Secure Elements - External Procedure, A04, March 2022
D1542793A - UpTeq Card, Applet Development Guide, February 11, 2021
D1619036 - TESSv7.1 - APDU Guide, September 3, 2024
D1619039 - TESSv7.1 - User's Guide, September 3, 2024
D1258682 - Application Verification for Certified Secure Elements - External Procedure, C03b, October 2023
Cryptographic Service Provider API, Programming Guidelines, v1.1, November 22, 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 performed extensive testing on functional specification, subsystem and SFR-enforcing module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

The underlying hardware and crypto-library test results are extendable to composite evaluations, because the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.

For ADV_IMP a thorough implementation representation review is performed on the TOE. During this attack-oriented analysis, the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this analysis will be performed according to the attack methods in *[JIL-AMS]*. An important source for assurance in this step is the technical report *[HW-ETRfC]* of the underlying platform.

All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The total test effort expended by the evaluators was 24 weeks. During that test campaign, 25% perturbation attacks, 8% retrieving keys with FA, 59% side-channel attacks, 4% software attacks, and 4% application isolation penetration tests.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[ST]*.

Part of the penetration testing was performed on an earlier revision of the TOE. The assurance gained from testing on an earlier revision has been assessed to be valid for the final TOE version, because the changes introduced were minimal and did not have an impact on the TSF.

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.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential". The TOE supports a wider range of key sizes (see *[ST]*), including those with sufficient algorithmic security level to exceed 100 bits as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities

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

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 8 Site Technical Audit Reports.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number TESS v7.1 Platform Revision 1.0.

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 TESS v7.1 Platform Revision 1.0, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_DVS.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'demonstrable' conformance to the Protection Profile *[PP-GP]*.

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

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 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. 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: none.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 “high attack potential”. To be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The TESS v7.1 Platform – Security Target, version 1.2, 07 February 2025 *[ST]* is included here by reference.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

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

API	Application Programming Interface
APDU	Application Protocol Data Unit
CSP	Cryptographic Service Provider
ECC	Elliptic Curve Cryptography
eUICC	Embedded UICC
eSE	Embedded Secure Element
IC	Integrated Circuit
IT	Information Technology
ISD	Issuer Security Domain
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
OS	Operating System
PIN	Personal Identification Number
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SCP	Secure Channel Protocol
SD	Security Domain
SSD	Supplementary Security Domain
SE	Secure Element
TOE	Target of Evaluation

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
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[ETR]	Evaluation Technical Report “TESS v7.1 Platform revision 1.0” – EAL4+, 24-RPT-863, version 5.0, 07 February 2025
[ETRfC]	Evaluation Technical Report “TESS v7.1 Platform revision 1.0” – EAL4+, 24-RPT-1556, version 3.0, 07 February 2025
[HW-CERT]	Rapport de certification ANSSI-CC-2023/46-R01 S3NSN6H (S3NSN6H_20240515), 06 December 2024
[HW-ETRfC]	Evaluation Technical Report (ETR for composition) - CAYUSE10-R1, référence LETI.CESTI.CAY10R1.COMPO.001 – V1.0, 28 August 2024
[HW-ST]	Security Target Lite of S3NSN6H, Version 2.1, 21 August 2024
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2.1, February 2024
[JIL-AMS]	Attack Methods for Smartcards and Similar Devices, Version 2.5, May 2022 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[PP-CSP]	Cryptographic Service Provider Protection Profile, V0.9.8, February 2019, registered under the reference BSI-CC-PP-0104-2019
[PP-GP]	GlobalPlatform Technology - Secure Element Protection Profile, GPC_SPE_174, Version 1.0, 17 February 2021, registered under the reference CCN-CC-PP-5/2021
[ST]	TESS v7.1 Platform – Security Target, version 1.2, 07 February 2025
[ST-lite]	TESS v7.1 Platform – Security Target, version 1.1p, 07 February 2025
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)