EUCC Certification Report

TESS v6.1 Platform, version 1.0

Sponsor and developer:	***Thales DIS France SAS*** **6 rue de la Verrerie** **92197 Meudon** **France**
Evaluation facility:	***SGS Brightsight*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**EUCC-3110-2026-2500171-01 Certification Report**
Report version:	**1**
Project number:	**EUCC-2500171-01**
Author(s):	**Jordi Mujal, TrustCB B.V.** **contact: eucc@trustcb.com**
Date:	**25 September 2026**
Number of pages:	**17**
Number of appendices:	**0**

Reproduction of this report is authorised only if reproduced in its entirety.

® TrustCB is a registered trademark. Any use or application requires prior approval by TrustCB

CONTENTS

Foreword 3

International recognition of the certificate 4

1 Executive Summary 5

2 ICT Product details 6

2.1 Identification of the ICT Product 6
2.2 Contact information related to the evaluation of the ICT Product 6
2.3 Security services and policies 6
2.3.1 Security services 6
2.3.2 Vulnerability management 7
2.3.3 Assurance Continuity policies 7
2.3.4 Lifecycle management processes and production facilities 7
2.3.5 Patch management process 7
2.4 Assumptions and Clarification of Scope 7
2.4.1 Assumptions 7
2.4.2 Clarification of scope 8
2.5 Architectural Information 8
2.6 Supplementary Cybersecurity Information 9

3 Evaluation summary 10

3.1 Identification of used assurance components 10
3.2 EUCC State of the Art documents and Protection Profiles 10
3.3 ICT Product testing 10
3.3.1 Testing approach and depth 10
3.3.2 Independent penetration testing 10
3.3.3 Test configuration 10
3.3.4 Test results 11
3.4 ICT Product evaluation 11
3.4.1 Reused evaluation results 11
3.4.2 Evaluated configuration 11
3.4.3 Assessment against each assurance requirement 11
3.5 Results of the evaluation 13
3.6 Certificate information and scheme label 14
3.7 Comments and Recommendations 14

4 Security Target 15

5 Glossary 15

6 Bibliography 16

Foreword

The Common Criteria-based European Cybersecurity Certification Scheme (EUCC) is a certification scheme created under the Cybersecurity Act (CSA), Regulation (EU) 2019/881 of 17 April 2019.

The EUCC is described by Commission Implementing Regulation (EU) 2024/482 of 31 January 2024, laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

The Dutch implementation of the CSA is regulated in Dutch law in the 'Uitvoeringswet cyberbeveiligingsverordening' (UITVW). In this law the role of NCCA is assigned to the Dutch Authority for Digital Infrastructure (RDI), which is part of the Ministry of Economic Affairs.

TrustCB B.V. has been licensed by the RDI as a Certification Body (CB) for the task of ISO/IEC 17065 Certification Activities up to and including CSA assurance level high for ICT security products, as well as for protection profiles. Part of the procedure is the technical examination (evaluation) of the product, protection profile according to the NP002 EUCC processes published by the Dutch NCCA.

Evaluations of ICT products are performed by an IT Security Evaluation Facility (ITSEF) licensed by the Dutch NCCA as a CAB for ISO/IEC 17025 Evaluation Activities, with scope aligning to the requested Evaluation Assurance Level of the Object for the evaluation, referred to as the Target of Evaluation (TOE) in this report.

By awarding an EUCC certificate as a Common Criteria certificate, TrustCB B.V. asserts that the ICT product complies with the security requirements specified in the associated 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 security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the ICT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the ICT product satisfies the security requirements stated in the security target.

Reproduction of this report is authorised only if it is reproduced in its entirety.

International recognition of the certificate

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of published 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.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the TESS v6.1 Platform, version 1.0, identified in this document as either the ICT Product or as the Target of Evaluation (TOE).

The developer of the ICT Product is Thales DIS France SAS located in Meudon, France and they also act as the sponsor of the evaluation and certification.

This Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the ICT product for their particular requirements.

The TOE as an eSE product, it 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. TESS v6.1 is built upon an open platform implementing the Javacard and GlobalPlatform standards and compliant to *[PP]*.

The TOE claims conformance to the following Protection Profiles *[PP]*:

- GlobalPlatform Technology - Secure Element Protection Profile, GPC_SPE_174, Version 1.0, 17 February 2021, registered under the reference CCN-CC-PP-5/2021

A certification procedure was conducted on the TOE by TrustCB B.V., in accordance with the provisions of the EUCC as described in Commission implementing regulation (EU) 2024/482 of 31 January 2024, amended by (EU) 2024/3144 of 18 December 2024 and (EU) 2025/2462 of 8 December 2025.

The successful completion of the certification procedure resulted in TrustCB issuing an EUCC certificate, The certificate identifier is **EUCC-3110-2026-2500171-01**, dated 25 September 2026 and with a 5-year validity.

The evaluation of the TOE was performed by SGS Brightsight located in Delft, The Netherlands. The evaluation was completed on 23 September 2026 with the issuance of the evaluation technical report *[ETR]*. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CC:2022, R1 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 R1 *[CC]* (Parts 1, 2, 3, 4, 5).

The scope of the evaluation was defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the ICT Product, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements.

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) ALC_FLR.2 “Flaw Reporting Procedures” and AVA_VAN.5 (Advanced methodical vulnerability analysis). It also includes the assurance Composite product package as defined in *[CC]*(Part 5).

The AVA_VAN level applied during the evaluation was AVA_VAN.5. This assurance level is recognised by article 52 of [CSA] as ‘high’.

The evaluation included a patch management procedure aligning to *[EU-EUCC]* Section IV.4 of Annex IV.

Consumers of this ICT Product 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.

TrustCB B.V., as Certification Assessment Body licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC high certification activities, declares that the product will be listed on the ENISA EU Cybersecurity Certificates list and that the evaluation meets all the conditions for international recognition of Common Criteria Certificates.

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 ICT Product details

2.1 Identification of the ICT Product

The Target of Evaluation (TOE) for this evaluation is ICT product TESS v6.1 Platform, version 1.0 from Thales DIS France SAS located in Meudon, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	ST54L	IC Maskset name: K450, IC version: C, Master identification number: 0x0276
	Firmware	3.2.2
Software	TESS v6.1 OS	PDM counter: D0026A1628 OS release: 0102 OS update version: 00020000

Additional requirements for the operational environment of the certified ICT product are described in section 3.3.1 of the *[ST]*.

To ensure secure usage a set of guidance documents is provided with the TOE. For details, see section 2.6 of this report, “Supplementary Cybersecurity Information.

2.2 Contact information related to the evaluation of the ICT Product

Holder of the EUCC Certificate

Organisation name:	Thales DIS France SAS
Address:	6 rue de la Verrerie, 92197 Meudon, FRANCE
Certified product contact details	michael.bruyere@thalesgroup.com

Developer of the certified ICT Product

ICT product developer	Thales DIS France SAS

Identification of CAB

The Certification Assessment Body for this ICT Product is TrustCB B.V located in Hoofddorp, The Netherlands.

Identification of ITSEF

Evaluation and testing for this ICT Product was performed by following ITSEF:

SGS Brightsight B.V. in Delft, the Netherlands.

Responsible national cybersecurity certification authority

Dutch Authority for Digital Infrastructure (RDI)

2.3 Security services and policies

2.3.1 Security services

As per the [ST], the platform implements (at least) the following services:

- Management and control of the communication between the eSE 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). The TESS v6.1 platform also provides the following Java Card System augmentation packages: Sensitive Result, Sensitive Array, Monotonic Counter, Cryptographic Certificate Management, Key Derivation Function and System Time.
- Proprietary Thales API: Secure API which provides security services to applications
- Initialization of the Issuer Security Domain (ISD) and management of the eSE life cycle
- Creation and management of Supplementary Security Domains (SSD)
- SCP02, SCP03, SCP11, SCP80 and SCP81 support
- RSA, ECC support
- Secure loading, installation and deletion of applications within each SD
- Secure loading of software patches (GemActivate)

2.3.2 Vulnerability management

The following vulnerability policy has been identified as applicable to the TESS v6.1 Platform, version 1.0

Document reference: ALC_FLR: Systematic Flaw Remediation, D1518483, version 1.5.

2.3.3 Assurance Continuity policies

This is a new product certification. An assurance continuity policy was not provided.

2.3.4 Lifecycle management processes and production facilities

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

2.3.5 Patch management process

A Patch Management process has been assessed as required by the EUCC Annex IV.4::

Patch Management Process	**Version**
Patch Loading Management for Certified Secure Elements	A05

The outcome of the assessment was the ITSEF verified that the patch management procedure and the patch mechanism fulfil the 3 points required to be verified by the ITSEF in section IV.4 of Annex IV, points 5.b.1, 5.b.2 and 5.b.3. The correctness of these points was confirmed in the *[ETR]*.

2.4 Assumptions and Clarification of Scope

2.4.1 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]*.

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE and its configuration in the environment to fulfil all Assumptions described in the [ST].

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.

2.4.2 Clarification of scope

Considering all Assumptions above, the evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product. It is important to remark that the *[PP]* implies some threats which are covered by the environment: T.EXE-CODE.1, T.EXE-CODE.2 and T.NATIVE. For details on the mappings, see section 7.3 in the *[ST]*.

Threats addressed by the TOE and the IT environment are presented in Section 6.3 of *[ST]* and include the threats as required in the *[PP]* according to the selected PP packages (DAP, MDAP, DM, CLFDB, GS, CVM) and PP modules (ELFU, CCCM, CTL, OS Update).

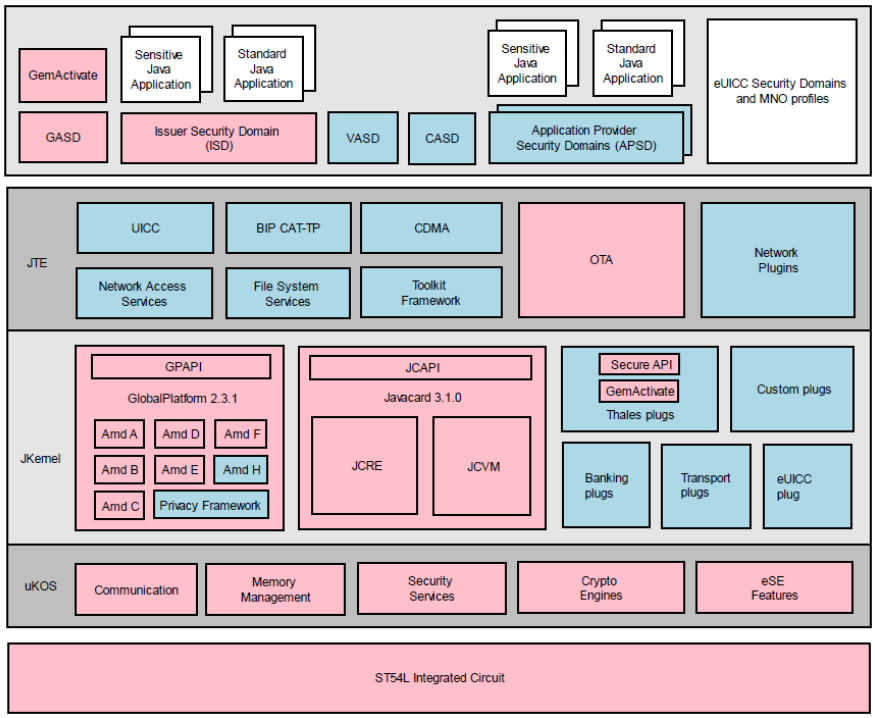
The Organizational Security Polices (OSPs) are the same as in *[PP]*. No OSPs have been added, removed or modified.

The TOE can be configured in without the support of GP Amendment H. Therefore, the assets, threats and OSPs related to the ELFU PP-module are only applicable to the platform configurations (i.e., customer profiles) in which GP Amendment H is supported.

Note that the product also contains eUICC and CSP supported functionalities. However, the related API and services are out of the scope of the present evaluation as no related security claims are present.

2.5 Architectural Information

As presented in [ST] see below the TOE architecture:



2.6 Supplementary Cybersecurity Information

The following website link was provided for the TESS v6.1 Platform, version 1.0 for the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881:

https://www.thalesgroup.com/en/search/enterprise/mobile-communications/thales-eucc-certification-mobile-communications-solutions

This link provides further details and links on:

- Guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the TESS v6.1 Platform, version 1.0.
- The period during which the TESS v6.1 Platform, version 1.0 security support will be offered to end users, in particular as regards the availability of cybersecurity related updates, is stated as 5 years aligned with the validity of the issued EUCC certificate.
- Contact information and accepted method for receiving vulnerability information from end users and security researchers for the TESS v6.1 Platform, version 1.0.
- the online repository listing publicly disclosed vulnerabilities related to the TESS v6.1 Platform, version 1.0 and to any relevant cybersecurity advisories .

Note: The following documentation, guidance and recommendations, is provided with the product by the developer to the customer to assist end users with the secure configuration, installation, deployment, operation and maintenance of the TESS v6.1 Platform, version 1.0:

Name	Version	Date
D1642736, Operational guidance on CC platforms – TESS v6.1	1.2	May 2026
D1642737, Operational guidance on CC platforms for Verification Authority – TESS v6.1	1.0	June 2025
D1642735, Preparative guidance On CC platforms – TESS v6.1	1.0	June 2025
D1578508, Guidance for profile set up vs. JavaCard System Protection Profile	1.6	July 2024
GlobalPlatform Card, Composition Model Security Guidelines for Basic Applications	2.0	November 2014
D1516176, Guidance for Secure application development on Thales Embedded Secure Solutions	4.2	April 2026
D1344508, Patch Loading Management for Certified Secure Elements	A05	August 2026
D1653452A, TESS v6.1 Applet Development Guide	November 20th, 2025	November 20th, 2025
D1641329, Guidance for Secure applet development with Secure API On TESS v6.1 platform	1.0	June 2025
D1641328, TESSv6.1 - APDU Guide	June 10th 2025	June 10th 2025
D1641327, TESSv6.1 - User Guide	May 9th 2025	May 9th 2025
D1258682, Application Verification for Certified Secure Elements	C03b	October 2023

3 Evaluation summary

3.1 Identification of used assurance components

The assurance components used in the product testing were:

- **EAL 4 augmented with ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5**
- **Composition evaluation package (COMP)**,

as defined by, and detailed in, *[CC]* and *[CEM]*.

3.2 EUCC State of the Art documents and Protection Profiles

EUCC state-of-the-art documents *[SotA Documents]* were applied as referenced in the Bibliography.

The following Protection Profiles were applied:

GlobalPlatform Technology - Secure Element Protection Profile, GPC_SPE_174, Version 1.0, 17 February 2021, registered under the reference CCN-CC-PP-5/2021

3.3 ICT 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.

3.3.1 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 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.

3.3.2 Independent penetration testing

3.3.3 Test configuration

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

PDM counter: D0026A1628

OS release: 0102

OS update version: 00020000

Independent evaluator testing and penetration testing was also performed on an earlier revision of the TOE:

PDM counter: D0026A1628

OS release: 0100

OS update version: 000000001

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.

3.3.4 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.

3.4 ICT Product evaluation

The evaluation was performed referencing ISO/IEC 18045, Common Evaluation Methodology, and the EUCC State of the Art documents listed in section 6 of this report as *SotA* Documents

3.4.1 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 multiple site certificates and Site Technical Audit Reports.

No sites have been visited as part of this evaluation.

3.4.2 Evaluated configuration

The TOE is defined uniquely by its name and version number TESS v6.1 Platform, version 1.0.

3.4.3 Assessment against each assurance requirement

As it is described in the [ETR]:

ASE

ASE	
ST introduction	ASE_INT.1
Conformance claims	ASE_CCL.1
Security problem definition	ASE_SPD.1
Security objectives	ASE_OBJ.2
Extended components definition	ASE_ECD.1
Security requirements	ASE.REQ.2
TOE summary specification	ASE.TSS.1
Consistency of Composite product ST	ASE.COMP.1

The TOE introduction, conformance claim, security problems, security objectives, extended components, security requirements and TOE summary specification are appropriately addressed, and the TOE description is accurate and adequate for the evaluation level. Consequently, the ASE activities fulfil the assurance requirements EAL4 package-augmented ALC_FLR.2, ALC_DVS.2 and AVA_VAN.5, with no issues or deviations identified.

ADV

ADV	
Security architecture	ADV_ARC.1
Functional specification	ADV_FSP.4
Implementation representation	ADV_IMP.1
TOE design	ADV_TDS.3
Composite design compliance	ADV_COMP.1

The evaluation has demonstrated that the developer's evidence meets ADV specified requirements. The TOE model is complete, clearly showing all interfaces (TSFI/non-TSFI), user roles, and relations, with explanations on completeness and tracing requirements met. The subsystem/module level model is sensible, useful, and shows TSFIs and subsystem/module decomposition. The security architecture is thoroughly explained, design compliance rationale is complete and coherent. Consequently, the ADV activities fulfil the assurance requirements EAL4 package-augmented ALC_FLR.2, ALC_DVS.2 and AVA_VAN.5, with no issues or deviations identified.

AGD

AGD	
Operational user guidance	AGD_OPE.1
Preparative procedures	AGD_PRE.1

The evaluation has demonstrated that the guidance documentation is clear, complete, and sufficient to support the secure acceptance, installation, configuration, and operation of the TOE within its intended environment by its user roles. The guidance effectively helps prevent common misconfigurations and promotes correct usage. Consequently, the AGD activities fulfil the assurance requirements EAL4 package- augmented ALC_FLR.2, ALC_DVS.2 and AVA_VAN.5, with no issues or deviations identified.

ALC

ALC	
CM capabilities	ALC_CMC.4
CM Scope	ALC_CMS.4
Delivery	ALC_DEL.1
Development security	ALC_DVS.2
Life cycle definition	ALC_LCD.1
Flaw remediation	ALC_FLR.2
Tools and techniques	ALC_TAT.1
Integration of composition parts and consistency check of delivery procedures	ALC_COMP.1

The evaluation has demonstrated that the developer's evidence meets ALC specified requirements. The CI-list was comprehensive and uniquely identified all configuration items, with clear identification of the developer. The CM documentation effectively described unique identification methods, a CM plan for development, procedures for accepting modified or new CIs, and the CM system was operated in accordance with the CM plan to maintain all configuration items by automated means. Delivery procedures were well-documented, ensuring security during TOE distribution. Security measures for protecting the confidentiality and integrity of the TOE in physical, procedural, personnel, logical and other areas were justified as sufficient. Flaw remediation procedures were comprehensive, including methods for receiving reports, tracking flaws, providing corrective actions, and updating users. The development life-cycle model provided necessary control; tools were well-defined with clear documentation and implementation standards have been applied by the developer. Consequently, the ALC activities fulfil the

assurance requirements EAL4 package- augmented ALC_FLR.2, ALC_DVS.2 and AVA_VAN.5, with no issues or deviations identified.

ATE

ATE	
Coverage	ATE_COV.2
Depth	ATE_DPT.1
Functional tests	ATE_FUN.1
Independent testing	ATE_IND.2
Composite functional testing	ATE_COMP.1

The evaluation has demonstrated that the developer's evidence for ATE requirements meets all specified requirements. The testing approach used by the developer effectively covered the TSFIs and modules. The developer's rationale for testing all TSFIs and modules was presented and verified. The developer test results show that for all tests either the result was pass or a proper rationale was given why the test failed. For the evaluator's independent testing, the overall approach for test selection, goals for the witnessing session, and independent test plan were clearly outlined. The evaluator's testing results showed that all sampled tests were passed. Consequently, the ATE activities fulfil the assurance requirements EAL4 package-augmented ALC_FLR.2, ALC_DVS.2 and AVA_VAN.5, with no issues or deviations identified.

AVA

AVA	
Vulnerability analysis	AVA_VAN.5
Composite vulnerability assessment	AVA_COMP.1

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. This analysis was performed according to the attack methods and application of attack potential to smartcards and similar devices in *[SotA_AAPS]*. 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.

Consequently, the AVA activities fulfil the assurance requirements EAL4 package-augmented ALC_FLR.2, ALC_DVS.2 and AVA_VAN.5, providing a high level of confidence in the TOE's resistance to exploitation.

3.5 Results of the evaluation

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

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 evaluation results the evaluation lab concluded the TESS v6.1 Platform, version 1.0, to be **CC:2022 R1 Part 2 conformant, CC:2022 R1 Part 3 conformant**, at an assurance level recognised by article 52 of [CSA] as '**High**', with **AVA_VAN 5** and to meet the requirements of **EAL 4 augmented with ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

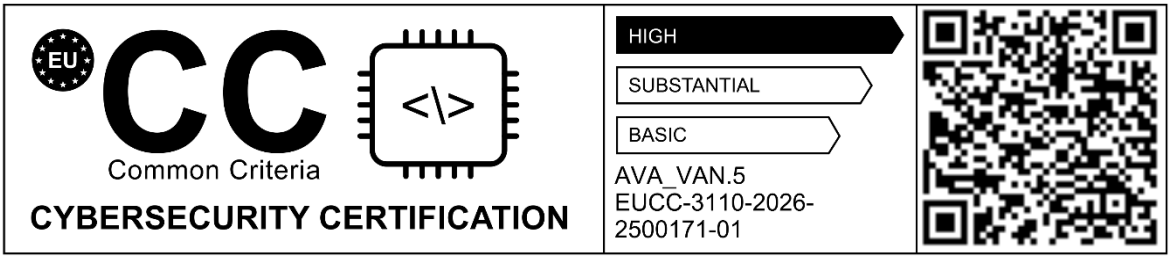
The Security Target claims 'demonstrable' conformance to the Protection Profile *[PP]*.

3.6 Certificate information and scheme label

A Certificate has been issued recognising this evaluation result as follows:

Unique identifier: EUCC-3110-2026-2500171-01

Date of issuance: 25-09-2026 and with a validity period of **5 years**.



3.7 Comments and Recommendations

The user guidance as outlined in section 2.6 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).

4 Security Target

The certification references the following security target:

TESS v6.1 Platform – Security Target, version 1.1, 18 August 2026 *[ST]*.

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

5 Glossary

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
EUCC	European Cybersecurity Certification Scheme [EU-EUCC], created under the Cybersecurity Act [EU-CSA] and detailed in Commission Implementing Regulation (EU) 2024/482
IC	Integrated Circuit
IT	Information Technology
ISD	Issuer Security Domain
ITSEF	IT Security Evaluation Facility
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

6 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, CC:2022 Parts 1, 2, 3, 4 and 5, R1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 R1, November 2022
[CCMB-2024-002]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2
[CC2022_TP]	Transition Policy to CC:2022 and CEM:2022, CCMC-2023-04-001, 20 April 2023
[DEV_DOCS]	ST54L_v3.3.0_configuration_list, 12 December 2025
	Configuration Management Plan for TESS v6.1, MRDSECNOT250013, Rev: 1.1 09 December 2025
	TESS v6.1 Documentation configuration list for CC, D1651258, version 1.1
	TESSv6.1_ConfList, 04 May 2026
	D1654418 - ALR_TESSv6.1_v1.0_STM085, v1.0
	D1642736, Operational guidance on CC platforms – TESS v6.1, version 1.2, May 2026
	D1642737, Operational guidance on CC platforms for Verification Authority – TESS v6.1, version 1.0, June 2025
	D1642735, Preparative guidance On CC platforms – TESS v6.1, version 1.0, June 2025
	D1578508, Guidance for profile set up vs. JavaCard System Protection Profile, version 1.6, July 2024
	GlobalPlatform Card, Composition Model Security Guidelines for Basic Applications, version 2.0, November 2014
	D1516176, Guidance for Secure application development on Thales Embedded Secure Solutions, version 4.2, April 2026
	D1653452A, TESS v6.1 Applet Development Guide, 20 November 2025
	D1641329, Guidance for Secure applet development with Secure API On TESS v6.1 platform, version 1.0, June 2025
	D1641328, TESSv6.1 - APDU Guide, 10 June 2025
	D1641327, TESSv6.1 - User Guide, 9 May 2025
	D1258682, Application Verification for Certified Secure Elements, versionC03b, October 2023
[ETR]	Evaluation Technical Report “TESS v6.1 Platform revision 1.0” – EAL4+, 25-RPT-912, version 6.0, 23 September 2026
[ETRfC]	Evaluation Technical Report for Composition “TESS v6.1 Platform revision 1.0” –
	EAL4+, 25-RPT-913, version 4.0, 19 August 2026

[EU-CSA]	REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
[EU-EUCC]	COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)
[EU-EUCC-amdt.1]	Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation
[EU-EUCC-amdt.2]	Commission Implementing Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art documents
[HW-CERT]	NSCIB-CC-2300182-02.1
[HW-ETRfC]	Evaluation Technical report for Composition “ST54L and ST54LF B01” – EAL6+, 25-RPT-067, version 1.0, 31 March 2025
[HW-ST]	ST54L and ST54LF B01 Security Target for composition, Rev B01.1, February 2025
[PATCH MGMNT]	D1344508, Patch Loading Management for Certified Secure Elements, version A05, August 2026
[PP]	GlobalPlatform Technology - Secure Element Protection Profile, GPC_SPE_174, Version 1.0, 17 February 2021, registered under the reference CCN-CC-PP-5/2021
[SotA_AAPS]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Application of Attack Potential to Smartcards and Similar Devices, Version 2, February 2025
[SotA_COMP]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Composite product evaluation and certification for CC: 2022 Version 1, February 2025
[SotA_COSP]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT CERTIFICATION OF “OPEN” SMART CARD PRODUCTS VERSION 1.1, October 2023 .
[SotA_MSSR]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Minimum Site Security Requirements, Version 2, February 2025 .
[SotA_SARC]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Security Architecture requirements (ADV_ARC) for smart cards and similar devices extended to Secure Sub Systems in SoCs, version 1.1, October 2023 .
[SotA_STAR]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT, STAR methodology, version 1, February 2025 .
[ST]	TESS v6.1 Platform – Security Target, version 1.1, 18 August 2026
[ST-lite]	TESS v6.1 Platform – Security Target, version 1.1p, 18 August 2026
[ST-SAN]	Sanitization of a security target for publication, [EUCC] Annex V section V.2
	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)