TrustCB B.V.

Certification Report

Samsung ExynosTEE, version 2.0

Sponsor and developer: ***Samsung Electronics Co., Ltd.***
1-1,Samsungjeonja-ro, Hwaseong-si
Gyeonggi-do 18448
Korea

Evaluation facility: ***Keysight Technologies Netherlands Riscure B.V.***
Delftechpark 49
2628 XJ Delft
The Netherlands

Report number:	**NSCIB-CC-2400088-01-CR**
Report version:	**1**
Project number:	NSCIB-**2400088-01**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**10 February 2025**
Number of pages:	**11**
Number of appendices:	**0**

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

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.

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

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 Samsung ExynosTEE, version 2.0. The developer of the Samsung ExynosTEE, version 2.0 is Samsung Electronics Co., Ltd. located in Hwaseong-si, Korea and they also act as the sponsor of the evaluation and. 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 is a Trusted OS as part of a Trusted Execution Environment (TEE) for embedded devices implementing GlobalPlatform TEE specifications (TEE System Architecture, TEE Internal Core API [IAPI] and TEE Client API [CAPI])

The TOE has been evaluated by Keysight Technologies Netherlands Riscure B.V. located in Delft | Amsterdam | Leiden | Essen, The Netherlands. The evaluation was completed on 10 February 2026 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 Samsung ExynosTEE, version 2.0, 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 Samsung ExynosTEE, version 2.0 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 EAL3 augmented (EAL3+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.1 (Basic flaw remediation).

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 Samsung ExynosTEE, version 2.0 from Samsung Electronics Co., Ltd. located in Hwaseong-si, Korea.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	ExynosTEE	2.0

To ensure secure usage a set of guidance documents is provided, together with the Samsung ExynosTEE, version 2.0. For details, see section 2.5 “Documentation” of this report.

2.2 *Security Policy*

The TOE provides the following security functionality:

- Isolation of the TEE services, the TEE resources involved and all the Trusted Applications from the REE
- Isolation between Trusted Applications and isolation of the TEE from Trusted Applications
- Trusted storage of TA and TEE data and keys, ensuring consistency, confidentiality, atomicity and binding to the TEE
- Cryptographic API including:
    - Generation of cryptographic keys
    - Support for cryptographic algorithms as described in Table 2 of the *[ST]*. The table includes a reference to the SOG-IS document *Crypto Evaluation Scheme, Agreed Cryptographic Mechanisms v1.3 (Feb. 2023)* in respect of recommended and legacy mechanisms. Mechanisms not mentioned in Table 2 of the *[ST]* are not in the scope of the evaluation.
- TA instantiation that ensures the authenticity and contributes to the integrity of the TA code
- Correct execution of TA services.

2.3 *Assumptions and Clarification of Scope*

2.3.1 Assumptions

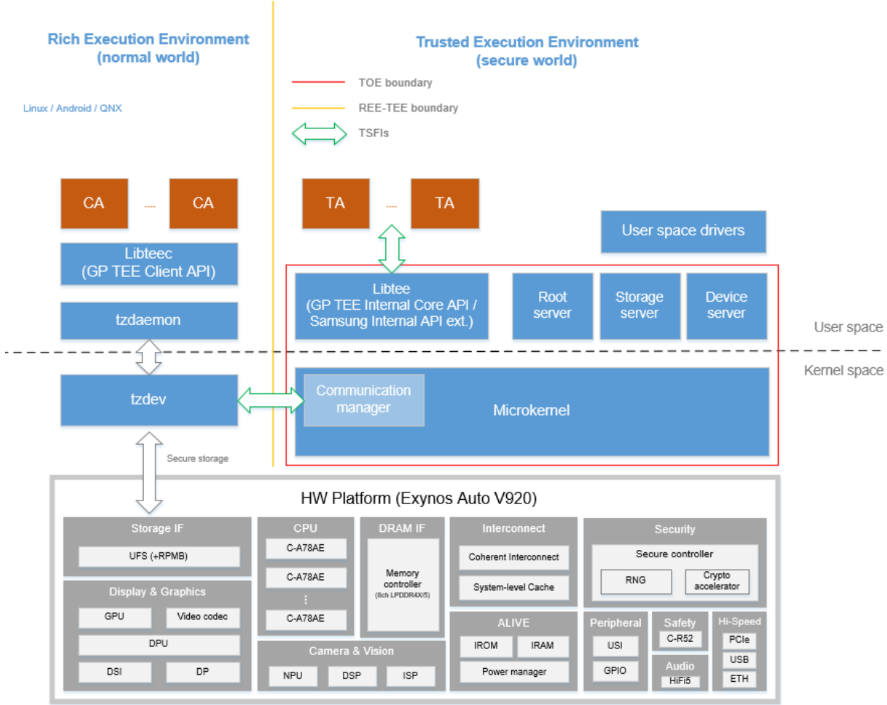
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

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.

2.4 *Architectural Information*

The TOE architecture can be depicted as follows:



2.5 *Documentation*

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

Identifier	**Version**
ExynosTEE 2.0 Preparative Guidance, dated December 2025	V1.0
ExynosTEE 2.0 Operational Guidance, dated December 2025	V1.0
GlobalPlatform TEE Internal Core API Specification, dated May 2019	v1.2.1
ExynosTEE 2.0 Samsung Internal Core API Extensions, dated January 2024	v0.2
ExynosTEE 2.0 Secure Monitor Calls, dated August 2024	v0.2

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 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.

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 total penetration testing effort expended by the evaluators was 16 work-days. During the test campaign out of the total effort spent on penetration testing; 0% was on physical attacks, 0% was on overcoming sensors and filters, 0% was on perturbation attacks, 0% was on retrieving keys with FA, 0% was on side-channel attacks, 0% was on exploitation of test features, 0% was on attacks on RNG, 0% was on ill-formed Java Card applications, 100% was on software attacks, and 0% was on application isolation penetration tests.

2.6.3 Test configuration

The TOE is only available in one security configuration; Samsung ExynosTEE, version 2.0.

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.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Samsung ExynosTEE, version 2.0.

2.9 Evaluation Results

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

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

Based on the above evaluation results the evaluation lab concluded the Samsung ExynosTEE, version 2.0, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 3 augmented with ALC_FLR.1**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

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 Samsung ExynosTEE Security Target, Revision 1.1, Dated December 5, 2025 *[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
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TEE	Trusted Execution Environment
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
[ETR]	Samsung ExynosTEE 2.0 Evaluation Technical Report, Version 1.3, Dated 11 December 2025
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	Samsung ExynosTEE Security Target, Revision 1.1, Dated December 5, 2025

(This is the end of this report.)