TÜV Rheinland Nederland B.V.

Certification Report

Unisoc TEE OS version 2.1.2

Sponsor and developer:	***Spreadtrum Communications(Shanghai)Co., Ltd*** **Building 1, Spreadtrum Center, Lane 2288, Zuchongzhi Road** **Shanghai** **P.R. China**
Evaluation facility:	***Riscure B.V.*** **Delftechpark 49** **2628 XJ Delft** **The Netherlands**
Report number:	**NSCIB-CC-0492117-CR**
Report version:	**1**
Project number:	**0492117**
Author(s):	**Jordi Mujal**
Date:	**12 December 2023**
Number of pages:	**11**
Number of appendices:	**0**

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

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

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

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

Recognition of the Certificate

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

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

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

European recognition

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

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

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Unisoc TEE OS version 2.1.2. The developer of the Unisoc TEE OS version 2.1.2 is Spreadtrum Communications(Shanghai)Co., Ltd located in Shanghai, China 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 type is a Trusted Operation System (TOS), which is only the software part of the Trusted Execution Environment (TEE). The TOE hosts a set of Trusted Applications (TA) and provides them with a set of security services including integrity of execution, secure communication with the Client Applications (CA) running in the REE, trusted storage and cryptographic algorithms.

The TOE has been evaluated by Riscure B.V. located in Delft, The Netherlands. The evaluation was completed on 12 December 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 Unisoc TEE OS version 2.1.2, 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 Unisoc TEE OS version 2.1.2 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 EAL2 augmented (EAL2+) assurance requirements for the evaluated security functionality. This assurance level is augmented with AVA_VAN_AP.3 (TEE Vulnerability Analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 *Identification of Target of Evaluation*

The Target of Evaluation (TOE) for this evaluation is the Unisoc TEE OS version 2.1.2 from Spreadtrum Communications(Shanghai)Co., Ltd located in Shanghai, China.

The TOE is comprised of the following main components:

Delivery item type	**Identifier**	**Version**
Software	Unisoc TEE OS	2.1.2

To ensure secure usage a set of guidance documents is provided, together with the Unisoc TEE OS version 2.1.2. For details, see section 2.5 “Documentation” of this report.

2.2 *Security Policy*

The TOE has the following security features:

- Trusted Storage
- User Identification and Authentication
- Protection of Trusted Applications (TA)
- Communication Data Protection between Client Applications (CA) and Trusted Applications (TA)
- Cryptographic operations support:
  - Symmetric AES and DES/TDES
  - Asymmetric RSA and ECC

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-Lite]*.

2.3.2 Clarification of scope

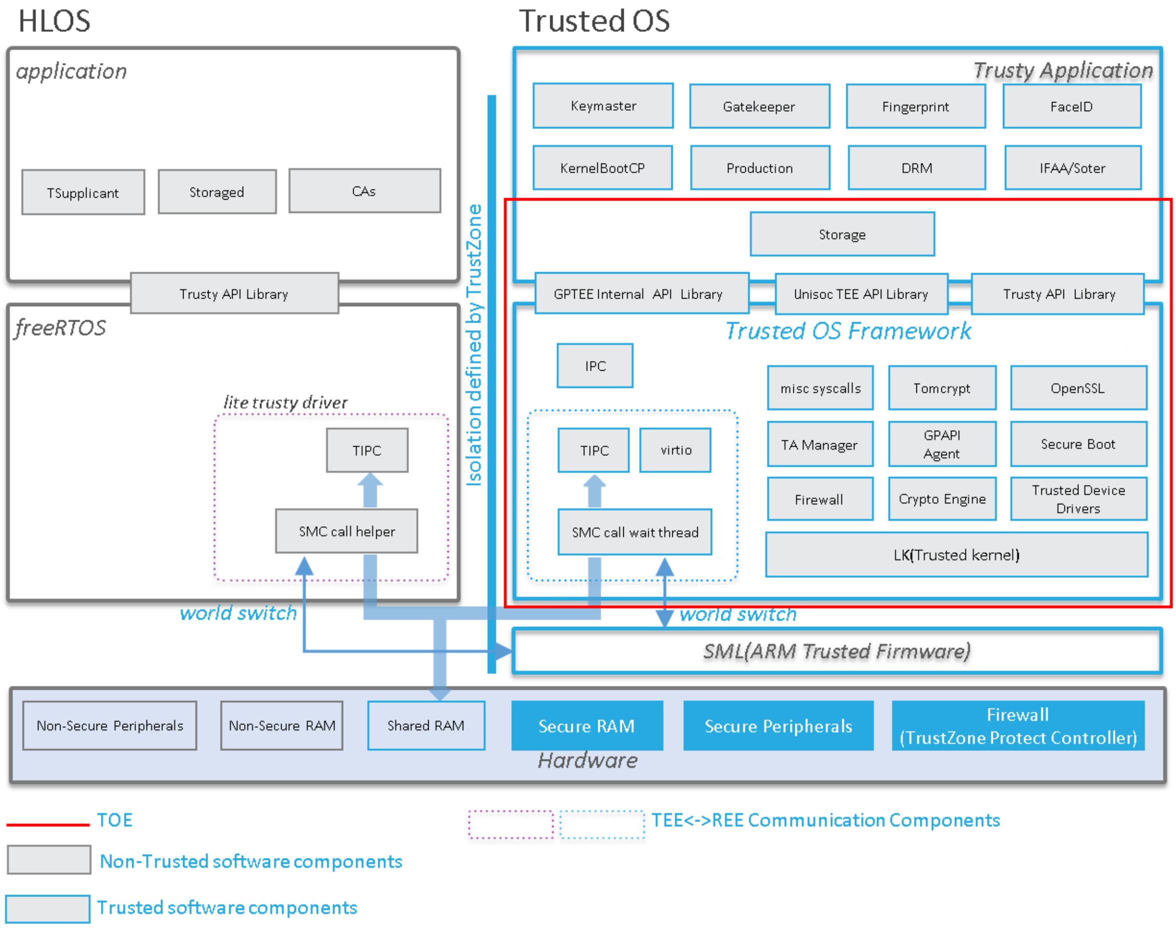
The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

Note that the *[ST]* has the A.SECURE_HARDWARE_PLATFORM assumption which requires the TOE environment to provide a secure HW which protects against physical invasive attacks, environmental stress malfunction attacks and side channel analysis attacks.

Therefore, these types of threats are not considered in the scope of the TOE evaluation and need to be considered for developing a product solution that integrates the TOE into a larger system including a hardware platform.

2.4 *Architectural Information*

The following figure depicts the TOE boundary and the main TOE architecture.



2.5 Documentation

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

Identifier	Version
Unisoc TEE OS - AGD_PRE Preparative Guidelines	0.14
Unisoc TEE OS – AGD_OPE Operational guidelines	0.11
Unisoc TEE OS - Functional Specification guidelines	0.15
Unisoc TEE SDK Guide	2.1
UNISOC Research Download User Guide V1.1 EN	1.1
TA Development Guide on Unisoc TEE	0.2
Driver Install and Uninstall Guide (EN)	1.1

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer’s testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer has performed extensive testing on functional specification and TSFIs. The testing was largely automated using industry standard and proprietary test suites. Test scripts were extensively used to verify that the functions return the expected values.

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

Considering the security assurance requirements for the AVA_VAN level, the following approach was considered by the Lab:

- Collect and review information available in the public domain.
- Collect and review information and prior work on the security evaluation evidences.
- Determine viable attack scenarios based on available information.
- Select attacks for the penetration testing phase.

The total test effort expended by the evaluators was 34 days. During that test campaign, 100% of the total time was spent on logical tests. No attacks including exploitation of test features, physical invasive attacks, side channel analysis or fault Injection were defined as the TOE is not claimed to be resistant against these types of attacks.

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]*.

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 Unisoc TEE OS version 2.1.2.

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 Unisoc TEE OS version 2.1.2, to be **CC Part 2 extended, CC Part 3 extended**, and to meet the requirements of **EAL 2 augmented with AVA_VAN_AP.3**. 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.

3 Security Target

The Unisoc TEE Security Target, version 0.30, 06 November 2023. *[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:

CA	Client Application
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
OS	Operating System
PP	Protection Profile
REE	Rich Execution Environment
TA	Trusted Application
TOE	Target of Evaluation
TOS	Trusted Operation System

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]	Evaluation Technical Report for Unisoc TEE OS v2.1.2, version 1.1, 11 December 2023
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	Unisoc TEE Security Target, version 0.30, 06 November 2023.
[ST-lite]	Unisoc TEE OS Security Target Lite, version 0.30 06 November 20
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)