Certification Report

Kinibi-510a-V007

Sponsor and developer:	***Trustonic*** **Les Aqueducs Bâtiment 2** **535 route des Lucioles** **Sophia Antipolis** **06560 Valbonne** **France**
Evaluation facility:	***Riscure B.V.*** **Delftechpark 49** **2628 XJ Delft** **The Netherlands**
Report number:	**NSCIB-CC-0291872-CR**
Report version:	**1**
Project number:	**0291872**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**04 April 2022**
Number of pages:	**11**
Number of appendices:	**0**

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.

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 Kinibi-510a-V007. The developer of the Kinibi-510a-V007 is Trustonic located in Valbonne, 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 implements the core functionalities defined in GlobalPlatform TEE Internal API Specification and Trustonic's proprietary APIs. The TOE is a TEE operating system running on a hardware/firmware. The hardware and firmware are not part of the TOE and are considered to be part of the TOE environment.

The TOE has been evaluated by Riscure B.V. located in Delft, The Netherlands. The evaluation was completed on 16 March 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 Kinibi-510a-V007, 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 Kinibi-510a-V007 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 EAL5 augmented (EAL5+) 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).

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 Kinibi-510a-V007 from Trustonic located in Valbonne, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	Kinibi-Src-Exynos64-510a-V007-r0- 20211117.125042-1-2021 1117_124837_19.zip	V007

The TOE is required to run on specific hardware as specified in chapter 4.4 of the *[ST]*.

To ensure secure usage a set of guidance documents is provided, together with the Kinibi-510a-V007. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE provides all the following main security features:

- Components authenticity and rollback protection
- Memory Management and Isolation mechanism
- User and device identification
- Inter-TA communication
- Secure storage of Keys and Data
- RNG, Key Management and Cryptographic operations
- Secure time

The Security Target covers two possible configurations for the TOE:

- Normal mode: This mode is in line with the GP TEE base PP. Kinibi Secure Storage is not rollback protected and Trusted Application are not downgrade protected.
- Time&RollbackProtection (T&R) mode: Secure Storage Rollback Protection and Trusted Application downgrade protection are enforced with the RPMB support provided by the underlying hardware. In this configuration, the TOE enforces GP TEE Time & Rollback PP modules security objectives.

2.3 Assumptions and Clarification of Scope

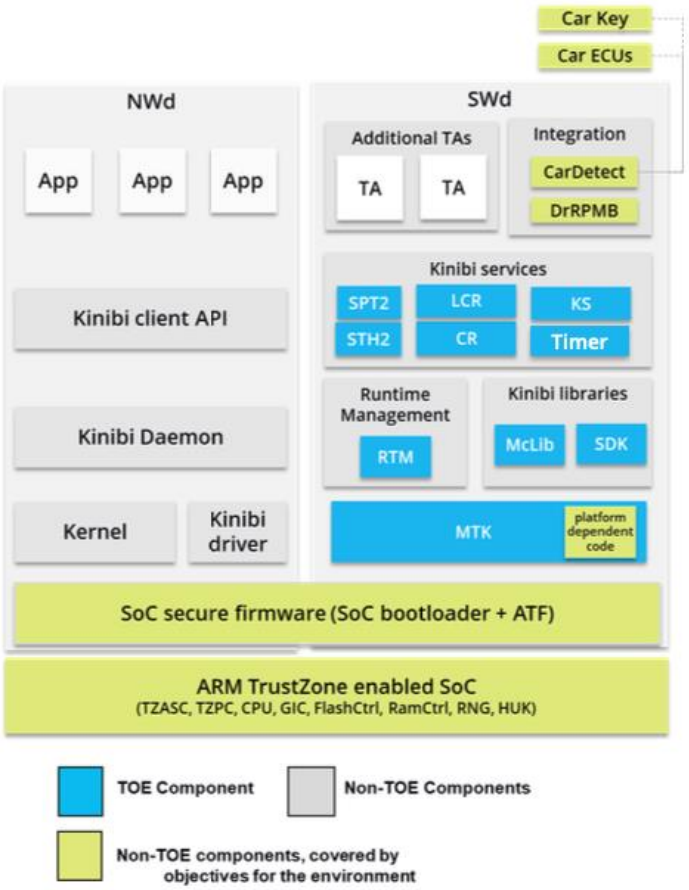
2.3.1 Assumptions

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 6.2 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 overview shows the technical implementation in a traditional layered representation. Isolation between the normal world and the secure world is shown with the use of the vertical grey boxes. The figure shows the software components which are part of the TOE in blue. These components implement amongst others the communication with the normal world, the management of Trusted Applications as well as their secure loading and the micro kernel which provides low level functionalities to the Kinibi Operating System.

The Green boxes show the hardware dependent functionalities which are covered by objectives for the environment and must be taken into account during the integration process.

2.5 Documentation

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

Identifier	Version
Kinibi Integration Guide	510A - 10 November 2020
Kinibi Driver Developers Guide	2.9
Kinibi Driver API Documentation	2.14
Kinibi Developers Guide	5.5
Kinibi API Documentation	API Level 12
[AGD_PRE] Kinibi v510A Preparative Procedures Guidance	1.13

[AGS_OPE] Kinibi v510A Operational User Guidance	1.9

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, subsystem and SFR-enforcing module level.

All parameter choices have been addressed at least once. All boundary cases identified have been tested explicitly, and additionally the near-boundary conditions have been covered probabilistically. 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 test results of the underlying base TOE are extendable to composite evaluations, as the base TOE is used according to its guidance and the composite evaluation requirements are met.

Amount of developer testing performed:

- The tests are performed on security mechanisms and on subsystem and module level with a total amount of several thousand test scenarios.
- As demonstrated by ATE_COV.2 the developer has tested all security mechanisms and TSFIs.
- As demonstrated by ATE_DPT.3 the developer has tested all the TSF subsystems and modules against the TOE design and against the security architecture description.

2.6.2 Independent penetration testing

For the testing performed by the evaluators, the developer has provided samples and a test environment. The evaluators have verified the execution of a selection of the developer tests, and conducted a number of test cases designed by the evaluator.

The total test effort expended by the evaluators was 10 days. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The TOE configuration used for testing was the Trustonic Kinibi-510a-V007 which 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.

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 Kinibi-510a-V007. The TOE is software only, and the validity of its source package can be verified by computing the SHA-256 of the delivered

package (as per section 2.3.1 of [AGD_PRE] mentioned in chapter 2.5 "Documentation") and compare with the expected value from section 2.2.2 of the *[ST]*.

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 Kinibi-510a-V007, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with ALC_FLR.1**. This implies that the product satisfies the security requirements specified in the 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 Trustonic Kinibi 510A Security Target, TT_510A_CC_ST , Version 1.2, 28 February 2022 *[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:

API	Application Programming Interface
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
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]	Evaluation Technical Report for Kinibi-510a-V007, 20190580-D2, Version 1.1, 3 March 2022
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	Trustonic Kinibi 510A Security Target, TT_510A_CC_ST , Version 1.2, 28 February 2022

(This is the end of this report.)