Certification Report

Kernel layer of the Shuniu 4.0-Lite Microkernel 2.0.12

Sponsor and developer: ***Beijing SmartChip Microelectronics Technology Company Limited***
Building 11, No. 79, Shuangying West Road, Nanshao Town
Changping District, Beijing
P.R.C.

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

Report number:	**NSCIB-CC-2300075-01-CR**
Report version:	**1**
Project number:	NSCIB-**2300075-01**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**10 December 2024**
Number of pages:	**11**
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 Kernel layer of the Shuniu 4.0-Lite Microkernel 2.0.12. The developer of the Kernel layer of the Shuniu 4.0-Lite Microkernel 2.0.12 is Beijing SmartChip Microelectronics Technology Company Limited located in Beijing,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 is the kernel layer of a microkernel which is an embedded operating system designed to run on M4 Cortex processors with MPU support.

The TOE performs the kernel functionalities of the OS including address space management, thread management and scheduling, exception and interrupt handling, inter-thread communication, access control, and other basic microkernel services.

The TOE has been evaluated by Keysight Technologies Netherlands Riscure B.V located in Delft, The Netherlands. The evaluation was completed on 10 December 2024 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 Kernel layer of the Shuniu 4.0-Lite Microkernel 2.0.12, 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 Kernel layer of the Shuniu 4.0-Lite Microkernel 2.0.12 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).

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 Kernel layer of the Shuniu 4.0-Lite Microkernel 2.0.12 from Beijing SmartChip Microelectronics Technology Company Limited located in Beijing,China.

The TOE is comprised of the following main components:

Delivery item type	Kernel layer of the Shuniu 4.0-Lite Microkernel	Version
Software	Kernel layer of the Shuniu 4.0-Lite Microkernel Hash Value: 3eee585c67118ccad8df9b8931fda2852e866b93269c7d423b07f91bcdb389e3	2.0.12

The TOE is running on the SCMB90051A_V2.0 board which contains Cortex M4 processors with MPU support.

To ensure secure usage a set of guidance documents is provided, together with the Kernel layer of the Shuniu 4.0-Lite Microkernel 2.0.12. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE has the following security features:

- System Invoking / System call
- Access Control
- Inter-thread communication
- Interrupt Management
- Thread management and scheduling
- Hardware abstraction layer (HAL)
- Space Isolation and Address Space
- System initialization

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

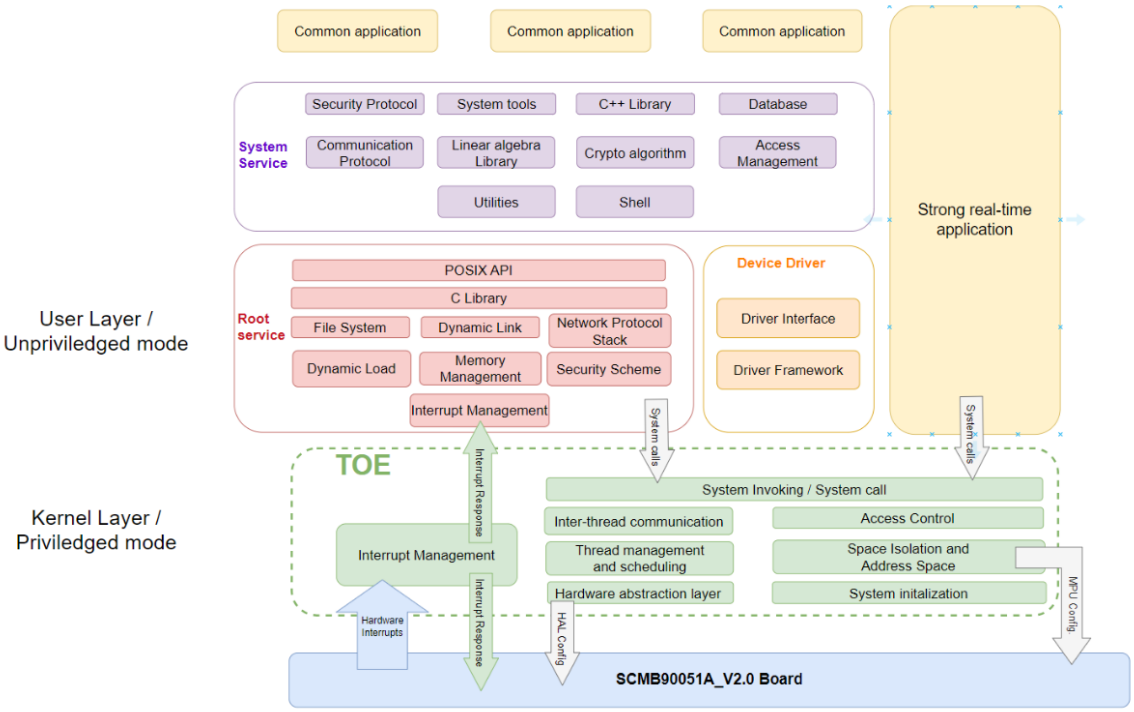
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

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:



The TOE is distributed as part of a full Operating System, known as the Shuniu 4.0-Lite Microkernel. There are components of the microkernel which reside in the user layer, not the kernel layer which is the TOE itself. All components within the user layer are therefore not part of the TOE, though it should be noted that these components do function together with the kernel in the overall operational environment.

Additionally, this includes the management of the communication interfaces (non-TOE hardware) as well, as this is also provided by the user layer.

2.5 Documentation

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

Identifier	Version
SmartChip Shuniu OS Kernel - Operational Guidance. Hash Value: 0eefd13b39872e5190debff0cf89fd9b46f848b17ebf4cce86f2911be7d41a5e	1.9
SmartChip Shuniu OS Kernel - Preparative Guidance. Hash Value: 003dd761a6e9f6a93c1575f60e40ca8f0526ceae63f7c2293158b70795d6e89c	1.10

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 analysis is performed considering (software) fault injection, (software) side-channel analysis, (software) exploitation of test features and Software attacks. The following is considered for each attack method:

- The design and implementation of the features relevant for the attack method
- Specific attack techniques from the evaluator's attack repository
- Implemented countermeasures
- User guidance

Based on these items, the lab determined whether an attack method is applicable to the TOE and should be tested during the penetration testing phase. Some attack categories are not applicable due to the pure software nature of the TOE and no claims on RNG or cryptographic requirements.

Additionally, a public domain vulnerability search was conducted by the evaluator to identify an TOE specific or related known vulnerabilities. This included checking Microkernel architectural issues, design practices for microkernels, debugging features as well as any specific information available on the TOE. The evaluator did not identify any vulnerabilities applicable to the TOE.

The total test effort expended by the evaluators was 15 days. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The TOE was tested in the following configuration:

- Kernel layer of the Shuniu 4.0-Lite Microkernel, version 2.0.12

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 Kernel layer of the Shuniu 4.0-Lite Microkernel 2.0.12.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and Site Technical Audit Report(s) for the site(s) *[STAR]* [2].

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

Based on the above evaluation results the evaluation lab concluded the Kernel layer of the Shuniu 4.0-Lite Microkernel 2.0.12, 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 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.

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

3 Security Target

The SmartChip Shuniu OS Kernel Security Target, Version 1.9, Dated 22 November 2024 *[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:

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 Kernel layer of the Shuniu 4.0-Lite Microkernel 2.0.12, Document ID 20220226-D1, Version 1.3, Dated 06 December 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
[ST]	SmartChip Shuniu OS Kernel Security Target, Version 1.9, Dated 22 November 2024
[ST-lite]	SmartChip Shuniu OS Kernel - Security Target Lite, Version 1.0, Dated 25 November 2024
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006
[STAR]	Site Technical Audit Report for Beijing SmartChip, project ID 20220226, Version 1.2, Dated 6 December 2024

(This is the end of this report.)