TÜVRheinland®
Precisely Right.

Certification Report

MSP V1.0

Sponsor and developer: ***HiSilicon***
Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Evaluation facility: ***Brightsight***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-0138342-CR**
Report version:	**1**
Project number:	**0138342**
Author(s):	**Wouter Slegers**
Date:	**20 August 2020**
Number of pages:	**12**
Number of appendices:	**0**

Headoffice:
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 Dutch Chamber of Commerce 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 license 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, in order 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 and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the MSP V1.0. The developer of the MSP V1.0 is HiSilicon located in Shenzen, 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 an independent subsystem that is integrated in a system-on-chip (SoC) running closed security software. The TOE enables system services in mobile phones that require security protection services such as secure storage for TAs, an anti-rollback counter storage function, a root of trust function, with key management and cryptographic services, weaver authentication mechanism for mobile user authentication, storing files encrypted under different class keys, supporting functionality for biometric authentication (does not include the biometric authentication itself), and functions for PSA services.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 20 August 2020 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 MSP V1.0, 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 MSP V1.0 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 provides sufficient evidence that the TOE meets the EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical 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]*.

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. It should be noted that the certification results only apply 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 releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the MSP V1.0 from HiSilicon located in Shenzen, China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	MSP_HW	V100
Firmware	Bootrom	V100
	UpdateOS	V100
Test-software	TestOS	V100
Software	SEE	V100R001
	Secure Storage SA	V100R001
	Anti-rollback SA	V100R001
	Root of Trust SA	V100R001
	Weaver authentication SA	V100R001
	File encryption SA	V100R001

To ensure secure usage a set of guidance documents is provided together with the MSP V1.0. Details can be found in section 2.5 of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 1.4.3.

2.2 Security Policy

The TOE enables system services in mobile phones that require security protection services such as:

- Secure Storage SA Service: secure storage for TAs.
- Anti-Rollback SA Service: anti-rollback counter storage function.
- Root of Trust SA Service: root of trust function, with key management and cryptographic services.
- Weaver Authentication SA Service: weaver authentication mechanism for mobile user authentication.
- File Encryption SA Service: storing files encrypted under different class keys.
- Biometric Authentication Supporting service for TSA: supporting functionality for biometric authentication (does not include the biometric authentication itself).
- Security functions for PSA 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. Detailed information on these

security objectives that must be fulfilled by the TOE environment can be found in section 4.1 of the *[ST]*.

2.3.2 Clarification of scope

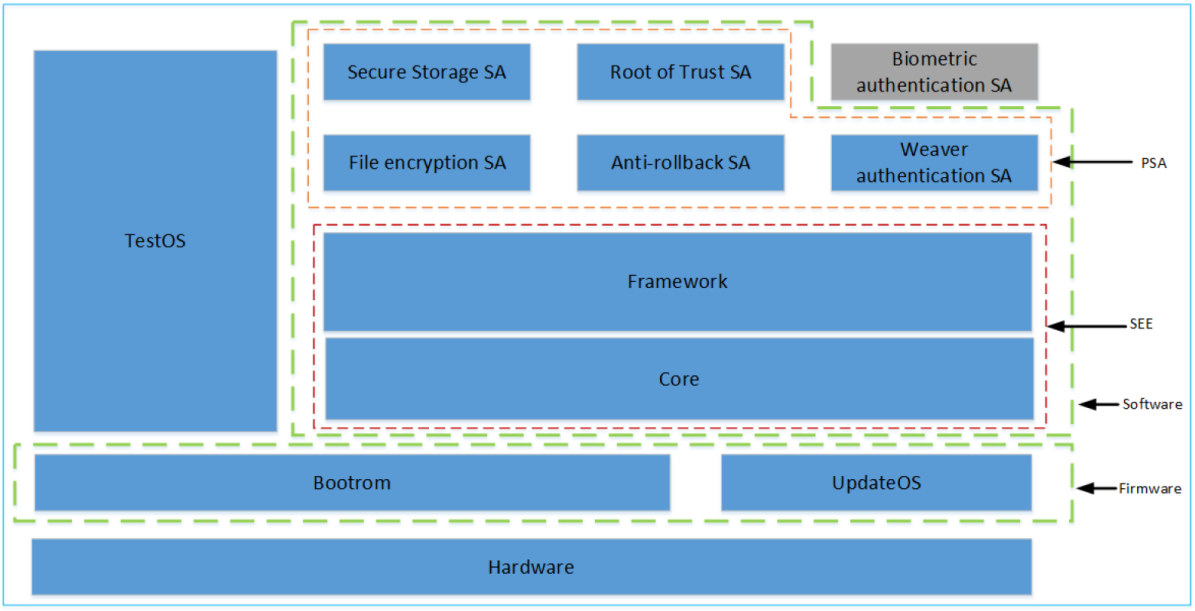
The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

Note that the *[ST]* clearly states that the biometric authentication supporting function is not an implementation of the biometric authentication, and that the TOE must be used with a secure flash component in accordance to OE.Secure-Component.

2.4 Architectural Information

The TOE is an independent subsystem that is integrated in a system-on-chip (SoC) running closed security software.

The logical architecture of the TOE is as follows (picture from the *[ST]*):



The TOE has the following features:

- Cryptographic support and random number generation
- Physical protection against non-invasive, semi-invasive, and invasive physical attacks
- Security update and boot
- Secure storage
- SA management
- Secure runtime
- Security services:
    - Secure storage SA
    - Anti-rollback SA
    - Root of Trust SA
    - Weaver Authentication SA
    - File Encryption SA
    - Biometric Authentication Supporting Service for TSA

2.5 Documentation

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

Identifier	Version
MSP V1.0 on Kirin 9000 Series Preparative Procedures for User	V10, dated 2020-07-30
MSP V1.0 on Kirin 9000 Series Preparative Procedures for Operational User Guidance	V10, dated 2020-07-29
MSP V1.0 IPC Command User Guidance	V01, dated 2020-07-22
Secure Flash User Guidance	V01, dated 2019-08-23
SA Development User Guidance	V02, dated 2020-05-20
Manufacture User Guidance	V01, dated 2020-07-29

2.6 IT Product Testing

2.6.1 Testing approach and depth

The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

For the hardware parts of the TOE, the developer performed three categories of testing: simulation, lab testing, and production testing. These test categories are combined to achieve a good coverage and depth of testing, both on the design of the hardware parts of the TOE and on each of the manufactured ICs.

For the software parts of the TOE, the developer performed four categories of testing: unit tests, system tests, SA-based system tests, and fuzzing tests. These categories were applied to (specific parts of) the TOE to achieve a good coverage and depth of testing, based on both the new functionality of the TOE as well as the experience and knowledge gained during previous projects incorporating existing functionality. The tests were executed using an automated framework.

For the testing performed by the evaluators, the developer has provided samples and a test environment on location. The evaluators have 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

Penetration testing was performed in accordance with the AVA_VAN level. The penetration test results confirm that the TOE, in its intended environment, is resistant to the attackers at AVA_VAN level.

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. For this analysis will be performed according to the attack methods in JIL document "Application of attack potential".
- 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.

The detailed testing effort is documented in the *[ETR]*. The total test effort was approximately 21 weeks for the penetration tests, which does not include the verification testing performed on the

software of approximately 8 weeks to assess whether the logical vulnerabilities were sufficiently addressed.

2.6.3 Test Configuration

The TOE was tested in its evaluated configuration and as open sample (with a test OS providing triggers and specific operations, and with additional hardware debug features enabled).

2.6.4 Testing 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.

The algorithmic security level exceeds 100 bits for all evaluated cryptographic functionality 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.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Re-used evaluation results

There is no re-use of evaluation results in this certification.

There has been re-use of the ALC aspects for the sites involved in the production of the TOE, by use of 5 site certificates.

Five sites have been visited as part of this evaluation and STARs have been generated. As part of this product evaluation, the STARs listed in the bibliography *([STAR-Xi'an], [STAR-WanGuo], [STAR-Shenzhen], [STAR-Shanghai],* and *[STAR-TSMC18]*) are issued.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]* and Site Technical Audit Reports[2] for the sites *([STAR-Xi'an], [STAR-WanGuo], [STAR-Shenzhen], [STAR-Shanghai],* and *[STAR-TSMC18]*) 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 MSP V1.0, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5** augmented with ALC_DVS.2 and AVA_VAN.5. 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 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against

[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.

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 with respect to 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 need to 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. In order for the evolution of attack methods and techniques to be covered, he 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 for satisfying the AVA_VAN.5 “high attack potential”. In order 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 *[ST]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

CA	Client Application
DDR	Double Data Rate
IPC	Inter-Process Communication
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MSP	Mobile Security Processor
NSCIB	Netherlands Scheme for Certification in the area of IT security
NVM	Non-Volatile Memory
OTP	One-Time Programmable
PP	Protection Profile
PSA	Platform security application
REE	Rich Execution Environment
SA	Security application
SEE	Secure Execution Environment
SoC	System on Chip
TA	Trusted Application
TEE	Trusted Execution Environment
TOE	Target of Evaluation
TSA	Third party security application

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 “MSP V1.0” – EAL5+ , 20-RPT-462, version 4.0, 13 August 2020.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[ST]	MSP V1.0 on Kirin 9000 Series Security Target, V12, 2020-08-10.
[STAR-Xi’an]	Site Technical Audit Report Huawei Xi'an Site v1.0, 20-RPT-699, v1.0
[STAR-WanGuo]	Site Technical Audit Report Huawei Shanghai DFWG Site v1.0, 20-RPT-697, v1.0
[STAR-Shenzhen]	Site Technical Audit Report Huawei Shenzhen Site v1.0, 20-RPT-696, v1.0
[STAR-Shanghai]	Site Technical Audit Report Huawei Shanghai Data Center v1.0, 20-RPT-698, v1.0
[STAR-TSMC18]	Site Technical Audit Report TSMC Fab18 Site v1.0, 20-RPT-700, v1.0

(This is the end of this report).