TÜV Rheinland Nederland B.V.

Certification Report

HongMeng v1.2

Sponsor and developer:	***Huawei Technologies, Co., Ltd*** **Headquarters of Huawei Technologies Co., Ltd. Bantian,** **Longgang District, Shenzhen, 518129** **P.R.C.**
Evaluation facility:	***Brightsight*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-217235-CR**
Report version:	**1**
Project number:	**217235**
Author(s):	**Wouter Slegers**
Date:	**5 September 2019**
Number of pages:	**12**
Number of appendices:	0

Reproduction of this report is authorized provided the report is reproduced in its entirety.

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

Version 2019-1

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Certificate

Standard
Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)

Certificate number **CC-19-217235**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer

Huawei Technologies Co., Ltd.

Headquarters of Huawei Technologies Co., Ltd. Bantian, Longgang District, Shenzhen, 518129, P.R.C.

Product and assurance level

HongMeng v1.2

Assurance Package:

- EAL5 augmented with ALC_FLR.1

Project number **217235**

Evaluation facility **Brightsight BV located in Delft, the Netherlands**

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL4

Validity
Date of 1st issue : **06-09-2019**
Certificate expiry : **06-09-2024**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

C.G.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

CONTENTS:

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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.eIDAS-Regulation

TÜV Rheinland Nederland BV, operating the Netherlands Scheme for Certification in the Area of IT Security (NSCIB), has been notified as a Designated Certification Body from The Netherlands under Article 30(2) and 39(2) of Regulation 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the HongMeng v1.2. The developer of the HongMeng v1.2 is Huawei Technologies, Co., Ltd located in Shenzhen, P.R.C. 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 (HongMeng) is a micro-kernel that provides fine-grained resource management for applications running on top of it.

By providing confidentiality and availability, HongMeng enforces secure access control and isolation for system resources. Thus it is a desired micro kernel for security scenarios.

HongMeng is supposed to run on a real mobile device (e.g., mobile phone) with hardware support for ARM TrustZone. Since TEE is not the only zone on mobile devices, it is common to see multiple unconstrained applications running on the non-TEE side. However even in that case, those unconstrained applications cannot interfere with TOE, neither the applications running on top of TOE.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 4 September 2019 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 HongMeng v1.2, 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 HongMeng v1.2 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 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_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]*.

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.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the HongMeng v1.2 from Huawei Technologies, Co., Ltd located in Shenzhen, P.R.C..

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	Internal Product Name: OS Kernel TD External Product Name: HongMeng Format: hm release.tar.gz Info: User can login the Version Management Platform (VMP) to download the software binary archive in accordance to the version of the TOE. User can verify the software by digital signature. The digital signature is also published on the VMP website.	Internal Version Number: V100R001C00SPC900B006 External Version Number: v1.2

To ensure secure usage a set of guidance documents is provided together with the HongMeng v1.2. Details can be found in section ”Documentation” of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 1.4.5.

2.2 Security Policy

The TOE has the following features:

- **Identification and Authentication:** The TOE does not identify physical users, only processes are identified by the TOE. Processes can be viewed as the users and subjects at the same time.
- **Capability-based Access Control:** The TOE enforces capability-based access control as the Discretionary Access Control (DAC) mechanism to protect the confidentiality of the kernel objects. The owner and the supervised visitor of a kernel objects manages the security attributes. When a kernel object is created, the owner and the supervised visitor specifies the initial rights to access it. The initial rights cannot be modified afterwards, and the rights granted to other processes must be less than the initial rights.
- **Information Flow Control and Residual Information Removal:** The TOE implements IPC Information Control Policy to control information flows associated with inter process communications, namely EBBCall and Async IPC. The other kernel objects do not have a dedicated memory region. In such cases, the object data is initialized with the corresponding default values, thus the kernel objects do not contain any trace of residual information.
- **Memory Management:** TOE uses kernel objects to record physical memory regions and virtual memory spaces. Access and privileges to this kernel objects are managed using capability-based access control system.
- **Thread Management:** A priority-based FIFO scheduling, ready threads with the same priority are linked in a queue which is sorted by the enqueue order. The scheduler is constructed with multiple queues where each queue stands for a given priority. Upon scheduling, the scheduler finds a non-empty queue with the highest priority, then chooses the thread in the head of the queue to run. Each thread has a timeslice to keep track of the current remaining time on the CPU, which will be decreased by 1 upon each timer tick.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

- **Platform attestation:** The TOE stores unique platform attestation data to be used in its operational state. Specifically, platform identification and allowed configuration values are stored in the kernel object.

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 4.2 of the *[ST]*.

2.3.2 Clarification of scope

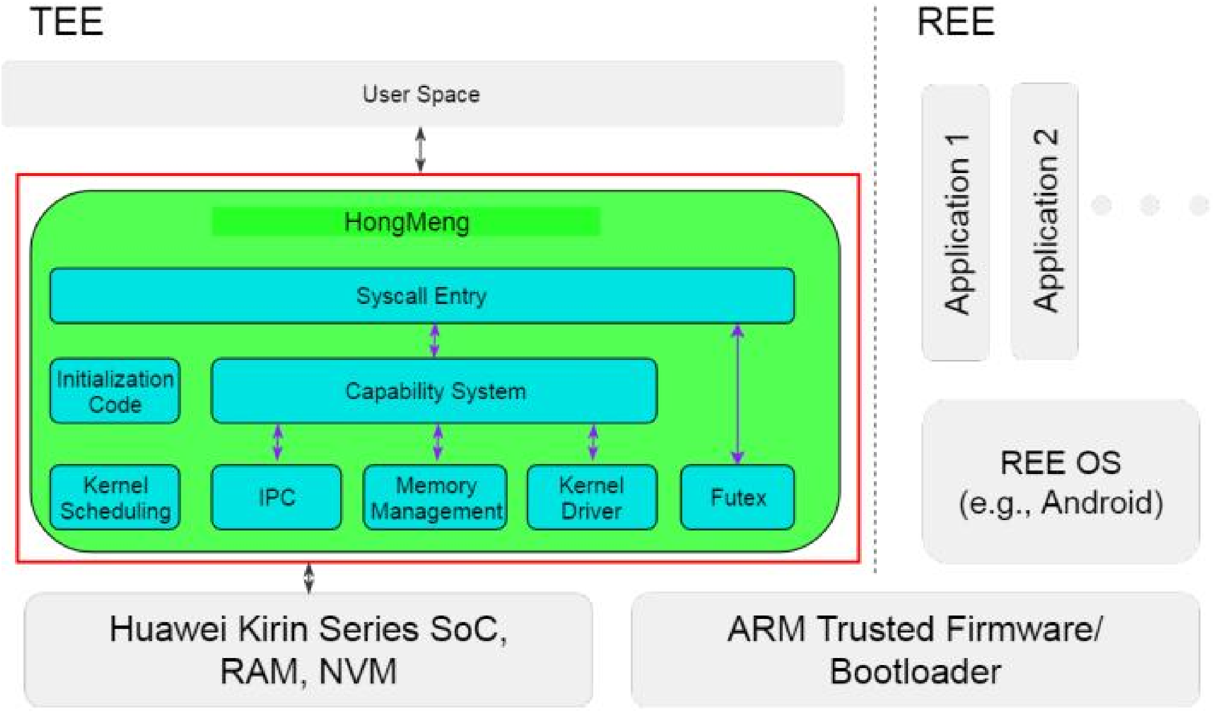
The TOE is a software microkernel that relies on the underlying hardware to fulfil the objective OE.ENVIRONMENT as described to *[ST]* section 4.2:

The environment ensures the following properties:

- The bootloader initializes the hardware so the TOE starts in a safe and secure state.
- The memory managed by the TOE, and the Kirin 970/980 SoC required by the TOE are protected in confidentiality and integrity from the outside of the TOE.
- The bootloader and ARM Trusted Firmware are protected in integrity from the outside of the TOE.

2.4 Architectural Information

The logical architecture, originating from the Security Target *[ST]* of the TOE can be depicted as follows:



2.5 Documentation

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

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Identifier	Version
Huawei HongMeng Common Criteria Evaluation AGD OPE: Operational User Guidance [OPE] Format: HongMeng AGD OPE-v2.0.pdf Info: The document is delivered on VMP website in accordance to the version of the TOE.	2.0
Huawei HongMeng Common Criteria Evaluation AGD PRE: Preparative Procedures [PRE] Format: HongMeng AGD PRE-v1.4.pdf Info: The document is delivered on VMP website in accordance to the version of the TOE.	1.4

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 and proprietary test suites. Test scripts were extensively used to verify that the functions return the expected values.

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

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ADV potential vulnerabilities were identified from generating questions to the type of TOE and the specified behaviour. From the ASE and AGD classes, no potential vulnerabilities were identified.
- For ADV_IMP a thorough implementation representation review was performed on the TOE. During this attack oriented analysis, the protection against the attack scenarios was analysed using the knowledge gained from all previous evaluation classes. This resulted in the identification of additional potential vulnerabilities. This analysis was performed according to the public sources and software related attack list.
- All potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. For the potential vulnerabilities relevant for the TOE a penetration test was defined. Several potential vulnerabilities were found to be not exploitable due to an impractical attack path.

The penetration tests that were distributed as follows:

Penetration test category	% of total number of penetration tests
Public interfaces penetration tests	50%
Memory management	30%
TOE functional features	20%

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Total	100%

2.6.3 Test Configuration

The TOE (HongMeng version v1.2 (V100R001C00SPC900B006)) in release version and with debug enabled, was tested on the Huawei Kirin 970 SoC (Huawei MATE 10 smart phone) and Huawei Kirin 980 SoC (Huawei MATE 20 smart phone).

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.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number HongMeng v1.2, running on the Huawei Kirin 970 SoC or Huawei Kirin 980 SoC.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references a 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 HongMeng v1.2, 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]*.

2.9 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 access control, depend on accurate conformance to the user guidance 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, as there are no cryptographic algorithms and protocols implemented.

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

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

3 Security Target

The Huawei HongMeng Common Criteria Evaluation ST: Security Target for Specified Hardware, version 2.8 *[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:

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

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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 “Huawei Hongmeng” – EAL5+, document reference 19-RPT-602, version 3.0, dated 3 September 2019.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, April 12019.

[ST] Huawei HongMeng Common Criteria Evaluation ST: Security Target for Specified Hardware, version 2.8.

(This is the end of this report).

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.