Certification Report

HongMeng Kernel V100R006C00SPC020B030

Sponsor and developer: ***Huawei Technologies, Co., Ltd***
Huawei Industrial Base, Bantian,
Longgang, Shenzhen 518129,
People's Republic of China

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-0618835-CR**
Report version:	**1**
Project number:	**0618835**
Author(s):	**Wim Ton**
Date:	**23 July 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 HongMeng Kernel V100R006C00SPC020B030. The developer of the HongMeng Kernel V100R006C00SPC020B030 is Huawei Technologies, Co., Ltd located in Shenzhen, P.R. 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 a micro-kernel that provides fine-grained resource management for applications running on top of it. The TOE provides:

- Confidentiality: the resources of a subject (code, data, registers, interrupts, devices) cannot be observed by other subjects without an explicit authorization.
- Availability: the system resources (code, data, registers, interrupts, devices) can be used by a subject (i.e. process) if and only if the subject is allowed by the TOE based on a priority-based queue.

The TOE has been evaluated by SGS Brightsight B.V located in Delft, The Netherlands. The evaluation was completed on 2023/07/23 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 Kernel V100R006C00SPC020B030, 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 Kernel V100R006C00SPC020B030 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 EAL6 augmented (EAL6+) 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 HongMeng Kernel V100R006C00SPC020B030 from Huawei Technologies, Co., Ltd located in Shenzhen, P.R. China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	HongMeng Kernel	V100R006C00SPC020B030

To ensure secure usage a set of guidance documents is provided, together with the HongMeng Kernel V100R006C00SPC020B030. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.4.5.

2.2 Security Policy

The TOE provides following the security services:

2.2.1 User identification and TSF protection

All processes must be identified before performing any TSF-mediated activity. The TOE preserves a secure state when a TOE panic occurs.

2.2.2 Capability-based access control

In the TOE, each kernel object is associated with a capability. To access a kernel object, a process must show the capability associated with the specific rights of the kernel object explicitly.

2.2.3 Information flow control and residual information removal

Only authorized processes can exchange information via IPC. In addition, any residual information in message related structures will be filled with zeros before use.

2.2.4 Memory management

The TOE uses memory management to achieve fine-grained access control for physical memory and virtual memory.

2.2.5 Thread management

By means of kernel scheduling and Futex functionalities, that ensure that only processes with a higher priority are allowed to use the resources.

2.2.6 Safe and secure state preservation

The TSF supports reaching and keeping a safe and secure state of the TOE. After the TOE has been successfully initialized, the global configuration is correct and matches the hardware conditions.
The TSF ensures also that the TOE is not compromised in the event of a failure during operation by means of logical checks on key paths of the code.

2.2.7 Platform attestation

The TOE provides the means to uniquely identify the underlying platforms.

2.3 *Assumptions and Clarification of Scope*

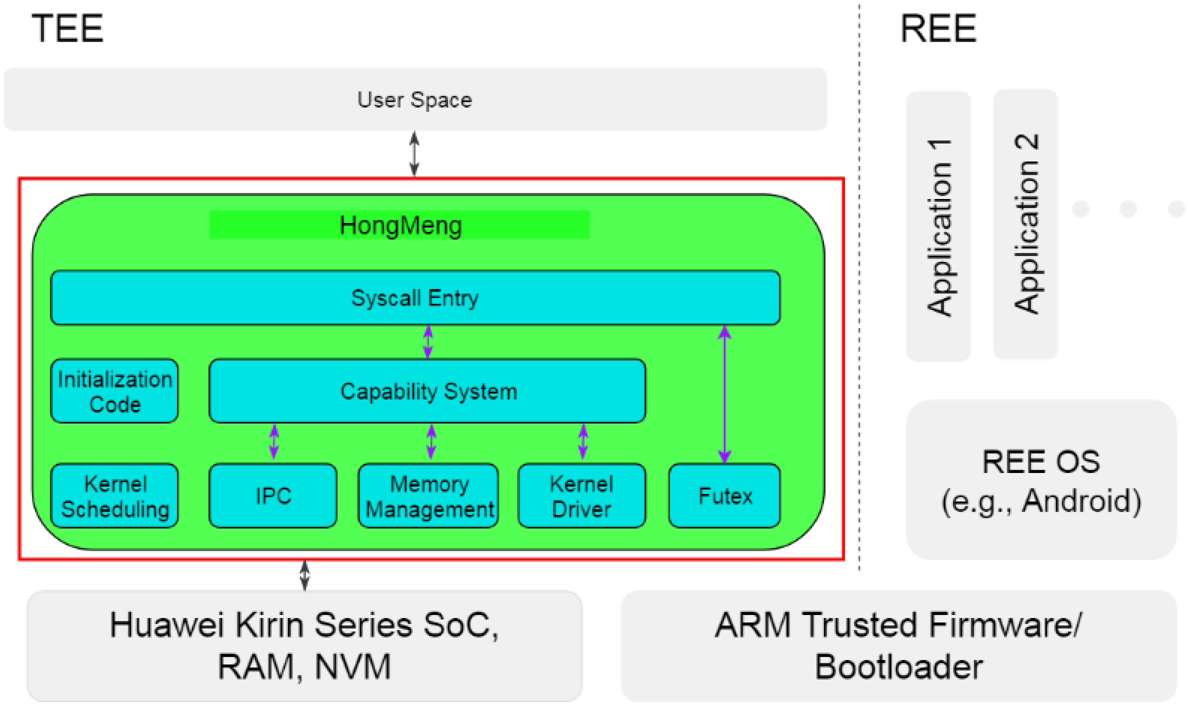
2.3.1 Assumptions

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 TOE is a software only TOE. The environment must provide a secure boot loader to ensure the TOE's integrity and ensure the correct initialization of the platform's hardware.

2.4 *Architectural Information*



The HongMeng Kernel employs a capability-based security model to control the usage of selected system resources and services (e.g., the memory, processor, communication channels, etc.).

A capability is a transferable, unforgeable token that represents authority. It refers to a value that uniquely references an object along with an associated set of access rights. By virtue of its possession by a process that uses the referenced object, the capability token grants that process the capability to interact with an object in certain ways.

The Fast Userspace muTEX (Futex), is a light-weight method for process synchronization in the HongMeng Kernel.

2.5 *Documentation*

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

Identifier	Version
Huawei HongMeng Kernel Common Criteria Evaluation AGD OPE: Operational User Guidance	2.0

Huawei HongMeng Kernel Common Criteria Evaluation AGD PRE: Preparative Procedures	2.0

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 evaluator repeated all developers tests on the intended configuration (the TOE installed on a Huawei Kirin 9000 SoC). The coverage of the developer test is 96.65% of the lines and 95.15% of the functions. A rationale was given for the missing coverage.

The evaluator created additional test cases test to: confirm verification of the version of the TOE, to supplement the test coverage of selected SFRs and TSFIs, and to further exercise the behaviour of the critical functionality.

2.6.2 Independent penetration testing

The total test effort expended by the evaluators was 10 weeks. During that test campaign, all the time was spent on logical tests. A fuzz test ran for 1200 hours.

2.6.3 Test configuration

The penetration tests were executed on specially instrumented versions of the TOE.

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 has been reuse of the ALC aspects for the sites involved in the development and production of the TOE, by reuse of the site certificate NSCIB-SS-0629826.

One site has been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number: HongMeng Kernel V100R006C00SPC020B030. Chapter 3.1 of the AGD_PRE describes how the user can verify the TOE version.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documentsThe verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the HongMeng Kernel V100R006C00SPC020B030, to be **CC Part 2 extended, CC Part 3 conformant**,and to meet the requirements of **EAL 6 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.

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 TOE does not contain cryptographic algorithms and protocols.

3 Security Target

The Huawei HongMeng Common Criteria Evaluation ST: Security Target for Specified Hardware, v2.0, 12 Jul 2023 *[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:

ARM	Advanced RISC Machines
ATF	ARM Trusted Framework
Futex	Fast Userspace muTEX
IPC	Inter Process Communication
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MMU	Memory Management Unit
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
REE	Rich Execution Environment
SoC	System on a Chip
SMC	Secure Monitor Call
SVC	Supervisor Call
TEE	Trusted Execution Environment
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[AIS34] Evaluation Methodology for CC Assurance Classes for EAL5+ and EAL6, version 3,

03.09.2009, Bundesamt für Sicherheit in der Informationstechnik

[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 HongMeng V100R006C00SPC020B030 – EAL6+, 23-RPT-281 v4.0 ETR Hongmeng.pdf, v 4.0, dated 19 July 2023

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019

[ST] Huawei HongMeng Common Criteria Evaluation ST: Security Target for Specified Hardware, v2.0, 12 Jul 2023

(This is the end of this report.)