Certification Report

Huawei iTrustee v5.0

Sponsor and developer:	***Huawei Technologies Co., Ltd.*** **D4 D Area Administration Building, No.6 City Avenue** **Songshan Lake Sci. &** **Tech. Industry Park, Dongguan 523808** **P.R.China**
Evaluation facility:	***Brightsight*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0016828-CR**
Report version:	**1**
Project number:	**0016828**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**11 December 2019**
Number of pages:	**12**
Number of appendices:	**0**

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.

Certificate

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

Certificate number
CC-19-0016828

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer

Huawei Technologies Co., Ltd.

D4 D Area Administration Building, No.6 City Avenue
Songshan Lake Sci. &
Tech. Industry Park, Dongguan 523808
P.R.China

Product and assurance level

Huawei iTrustee v5.0

Assurance Package:

- EAL2 augmented with AVA_TEE.2

Project number
0016828

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

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

SOGIS Mutual Recognition Agreement for components up to EAL 7

Validity
Date of 1st issue : **19-12-2019**
Certificate expiry : **19-12-2024**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

R. de Jonge, Managing Director
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

® 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 Huawei iTrustee v5.0. The developer of the Huawei iTrustee v5.0 is Huawei Technologies Co., Ltd. located in Dongguan, 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 type is the Trusted OS, which is only the software part of the Trusted Execution Environment (TEE). It is for embedded devices implementing GlobalPlatform TEE specifications [SA], TEE Internal API [IAPI] and TEE Client API [CAPI]).

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 24 November 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 Huawei iTrustee v5.0, 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 Huawei iTrustee v5.0 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]1for this product provides sufficient evidence that the TOE meets the EAL2 augmented (EAL2(+)) assurance requirements for the evaluated security functionality. This assurance level is augmented with AVA_TEE.2 (TEE 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.

® 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 Huawei iTrustee v5.0 from Huawei Technologies Co., Ltd. located in Dongguan, China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software (binary image)	Sec_trustedcore.img	6.1.0

To ensure secure usage a set of guidance documents is provided together with the Huawei iTrustee v5.0. 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 1.5.4.

2.2 Security Policy

The TOE is a Trusted OS, which is only the software part of the Trusted Execution Environment (TEE) defined by [TEE PP]. It is for embedded devices implementing GlobalPlatform TEE specifications [SA], TEE Internal API [IAPI] and TEE Client API [CAPI]). However, this TOE does not claim full functional compliance with GlobalPlatform TEE APIs specifications.

The TOE is an execution environment isolated from any other execution environment, including the usual Rich Execution Environment (REE), and their applications. The TOE hosts a set of Trusted Applications (TA) and provides them with a comprehensive set of security services including: integrity of execution, secure communication with the Client Applications (CA) running in the REE, trusted storage, key management and cryptographic algorithms, time management and arithmetical API.

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 3.2 of the *[ST]*.

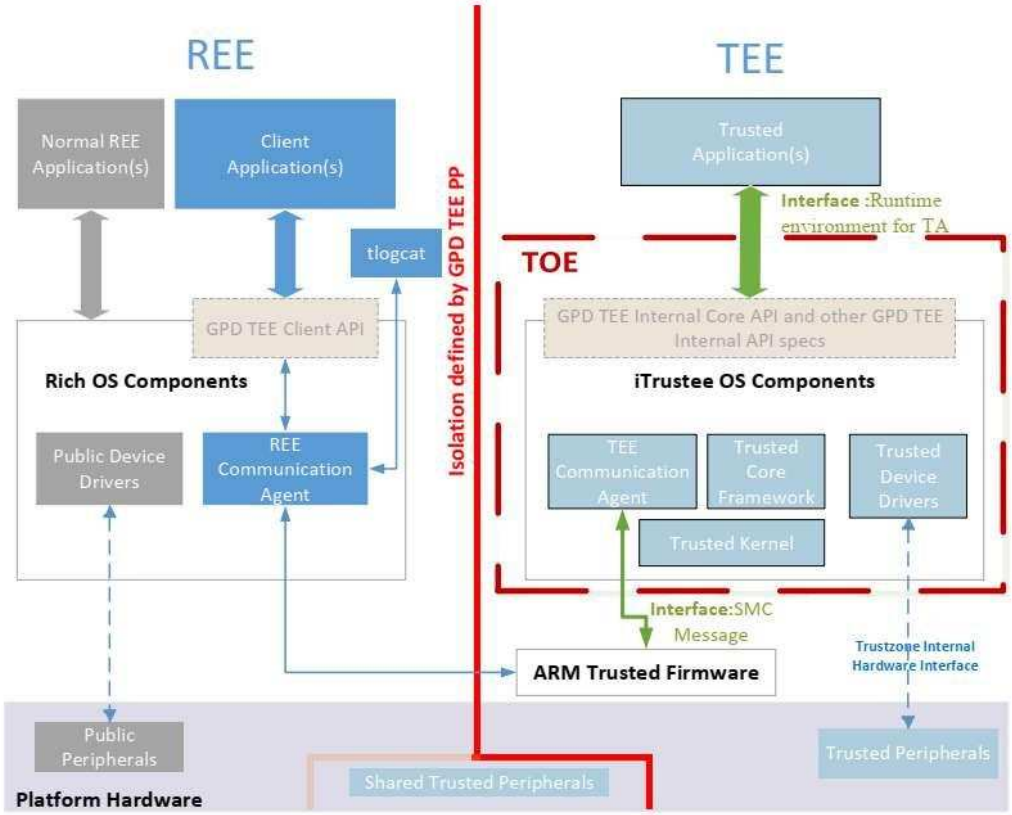
2.3.2 Clarification of scope

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 components of the TOE are identified in [ST] Section 1.5.1. The TEE is embedded in the device and runs alongside a standard OS or Rich Execution Environment. The role of the Trusted OS Components, of which the TOE is comprised, is to provide communication facilities with the REE software and the system level functionality required by the Trusted Applications, accessible from the TEE Internal API. This is depicted in the figure below:

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



The TOE is composed of the following four components:

iTrustee Component	Description
iTrustee Kernel	iTrustee Kernel provides task creation, memory management, IPC etc.
TEE Communication Agent	TEE communication Agent will send/receive SMC calls to/from REE, resolve SMC messages and forward messages to other components of the TOE.
Trusted Core Framework	Trusted Core Framework will manage the tasks already created.
Trusted Device Drivers	Trusted Device Drivers will talk to Trusted Peripherals, and provide trusted functions to the TOE.

2.5 Documentation

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

Identifier	Version
Huawei iTrustee Software V5.0 Preparative Procedures for User	1.1
Huawei iTrustee Software V5.0 Operational User Guidance	1.5
TrustedCore Developer Guide	2.3.2

2.6 IT Product Testing

Testing (coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

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

2.6.1 Testing approach and depth

The developer provided a working test environment for the evaluator, allowing the execution of any of the defined test cases, as well as allowing the creation of additional test cases.

Due to the availability of the test environment in the evaluation premises, and the short execution time of the developer's test cases defined in the test documentation, the evaluator decided to perform a full repetition of all the test cases performed by the developer instead of following a sampling strategy.

2.6.2 Independent Penetration Testing

To identify potential vulnerabilities, the evaluator performed the following activities:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considered whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
  During this attack oriented analysis, the protection of the TOE was analysed using the knowledge gained from all previous evaluation classes. This results in the identification of potential vulnerabilities.
- The evaluator performed a search in the public domain in order to identify potential vulnerability.
- A preliminary reverse engineering task was performed in order to identify additional potential vulnerabilities and to refine the definition of the prenetratio9n test cases.
- 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.

2.6.3 Test Configuration

The Huawei iTruste v5.0 was tested in the following configurations:

- Huawei iTruste v5.0 (sec_trustedcore.img version 6.1.0) in a kirin 980 SoC (Huawei Mate 20).

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 Re-used evaluation results

None.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Huawei iTrustee v5.0.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] and 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 Huawei iTrustee v5.0, to be **CC Part 2 extended, CC Part 3 extended**, and to meet the requirements of **EAL 2 augmented with**

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

AVA_TEE.2. 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.

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.

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

3 Security Target

The CC Huawei iTrustee Software Security Target version 6.0 *[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 Applications
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
REE	Rich Execution Environment
TA	Trusted Applications
TEE	Trusted Execution Environment
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:

[CAPI] TEE Client API Specification, GlobalPlatform, version 1.0, July 2010, GPD_SPE_007

[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 iTrustee v5.0, 19-RPT-680 Evaluation Technical Report iTrustee v5 – EAL2+, Version 3.0, 07 November 2019.

[IAPI] TEE Internal API Specification, GlobalPlatform, version 1.0, December 2011, GPD_SPE_010

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

[SA] TEE System Architecture, GlobalPlatform, version 1.2, November 2018, GPD_SPE_009

[ST] CC Huawei iTrustee Software Security Target version 6.0.

[TEE_PP] GlobalPlatform Device Committee - TEE Protection Profile Version 1.2.1, Public Release November 2016, Document Reference: GPD_SPE_021

(This is the end of this report).

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