SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

SERTIT-108 CR Certification Report

Issue 1.0 21 February 2018

Huawei iTrustee v2.0

CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009 VERSION 2.1 11.11.2011

SERTIT, Postboks 814, 1306 Sandvika, NORWAY

Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Sec urity, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognized under the terms of the CCRA July 2nd 2014.

The recognition under CCRA is limited to cPP related assurance packages or EAL2 and ALC_FLR CC part 3 components

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Agreement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Agreement and is the Party's claim that the certificate has been issued in accordance with the terms of this Agreement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Mutual recognition under SOGIS MRA applies to components up to EAL 4.

Contents

1 Certification Statement

Huawei iTrustee v2.0 is a simplified Real-time Operating System (OS) aiming to provide the Trusted Execution Environment (TEE) on Android Platforms running alongside a standard OS or Rich Execution Environment (REE).

Huawei iTrustee version 2.0 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL 2+ for the specified Common Criteria Part 2 (ISO/IEC 15408) extended by AVA_TEE.2.

Author	Kvassnes, Kjartan Jæger Certifier
Quality Assurance	Arne Høye Rage Quality Assurance Arne H. Rage
Approved	Jørn Arnesen Head of SERTIT
Date approved	21 February 2018

2 Abbreviations

CA	Client Application
CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
CM	Configuration Management
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
IPC	Inter-Process Communication
POC	Point of Contact
QP	Qualified Participant
OS	Operating System
RAM	Random Access Memory
SERTIT	Norwegian Certification Authority for IT Security
SPM	Security Policy Model
ST	Security Target
TEE	Trusted Execution Environment
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TUI	Trusted User Interface

3 References

[1] CC Huawei iTrustee Software Security Target,Version 2.1, 2018-01-25.

[2] CC Huawei iTrustee Software ADV_ARC Version 1.2, 2017-11-30

[3] Huawei iTrustee Software V2.0 Functional Specification, Version 1.4, 2017-12-22

[4] CC Huawei iTrustee Software V2. TOE Design, Version 1.2, 2017-12-19

[5] CC Huawei iTrustee Software V2.0 Operational User Guidance, Version 1.4, 2018-01-16

[6] CC Huawei iTrustee Software V2.0 Preparative Procedures for User, Version 1.5, 2017-12-25

[7] TrustedCore Developer Guide TrustedCore Developer Guide, Version 01, 2015-12-03

[8] GlobalPlatform Device Technology TEE Client API Specification, Version 1.0, Public Release July 2010

[9] GlobalPlatform Device Technology TEE Internal API Specification, Version 1.0, Public Release December 2011

[10] Huawei iTrustee Software V2.0 ALC_CMC.2, Version 1.0, 2017-12-23

[11] Huawei iTrustee Software V2.0 CM Scope, Version 1.7, 2018-01-25

[12] CC Huawei iTrustee Software V2.0 Delivery, Version 1.2, 2017-12-25

[13] CC Huawei iTrustee V2.0 Functional Tests & Coverage, Version 1.3, 2018-01-25

[14] Test Guide, Version 1.0

[15] Common Criteria Part 1, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[16] Common Criteria Part 2, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[17] Common Criteria Part 3, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[18] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.

[19] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[20] Evaluation Technical Report 18-RPT-033 ETR SERTIT-108 Huawei TEE iTrustee v2.0.

[21] GlobalPlatform Device Committee TEE Protection Profile Version 1.2.1

[22] GlobalPlatform Technology Application of Attack Potential to Trusted Execution Environment – Confidential version Version 1.5.0 Draft 02

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Huawei iTrustee version 2.0 to the Sponsor, Huawei Technologies Co., Ltd., and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The version of the product evaluated was Huawei iTrustee and version 2.0.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Huawei Technologies Co., Ltd..

Huawei iTrustee v2.0 is a simplified Real-time Operating System (OS) aiming to provide the Trusted Execution Environment (TEE) on Android Platforms running alongside a standard OS or Rich Execution Environment (REE).

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

An overview of the TOE's security architecture can be found in Annex B.

4.3 TOE scope

The scope of the Huawei iTrustee v2.0 is limited to only the Secure Operating System of a TEE and its guidance for the secure usage of the TOE after delivery to the end-user referred by [5] and [6].

The Huawei iTrustee v2.0 does not comprise:

- Hardware and firmware used to provide the TEE security functionality.
  - Bootloader
  - Bl31 monitor
- The Trusted Applications
- The Rich Execution Environment
  - EMUI, Huawei customized Android OS
  - SDK for Android app to communicate with iTrustee
- The Client Applications
  - Device driver for iTrustee in Android

4.4 Protection Profile Conformance

The Security Target [1] claims no conformance to any Protection Profile (PP).

4.5 Assurance Level

The Security Target[1] specified the assurance requirements for the evaluation. The assurance incorporated predefined evaluation assurance level EAL 2, augmented by AVA_TEE.2. Common Criteria Part 3 [17] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [15].

4.6 Security Policy

The TOE security policies are detailed in ST[1], section 2.4.

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats and OSP's which these objectives counter or meet and security functional requirements and security functions to elaborate the objectives. Most of the SFR's are taken from CC Part 2[16]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered

All threats that are countered are described in the Security Target [1], section 3.3.1 and 3.3.2

4.9 Threats Countered by the TOE's environment

Threats that are covered by the TOE's environment are identified in the Security Target [1], section 3.3.1 and 3.3.2

4.10 Threats and Attacks not Countered

No threats or attacks are described that are not countered.

4.11 Environmental Assumptions and Dependencies

The assumptions that apply to this TOE are described in the Security Target [1], section 2.5.

4.12 IT Security Objectives

The security objectives for the TOE that apply to this TOE are described in the Security Target [1], section 3.1.

4.13 Non-IT Security Objectives

The security objectives for the environment that apply to this TOE are described in the Security Target [1], section 3.2.

4.14 Security Functional Requirements

The security functional requirements that apply to this TOE are described in the Security Target [1], section 5.2.

Security Functional Requirements	
FAU_ARP.1	Security alarms
FAU_SAR.1	Audit review
FAU_STG.1	Audit event storage
FCS_COP.1	Cryptographic operation
FIA_ATD.1	User attribute definition
FIA_UID.2	User identification before any action
FIA_USB.1	User-subject binding
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.2	Complete information flow control
FDP_IFF.1	Simple security attributes
FDP_RIP.1	Subset residual information protection
FDP_ROL.1	Basic rollback
FDP_SDI.2	Stored data integrity monitoring and action
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_SMR.1	Security roles
FMT_SMF.1	Management functions
FPT_FLS.1	Failure with preservation of secure state
FPT_TEE.1	Testing of external entities
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction

4.15 Security Function Policy

This ST defines the following access control and information flow security functional policies (SFP):

Runtime Data Information Flow Control SFP:

- Purpose: To control the flow of runtime data from and to executable entities and memory. This policy contributes to ensure the integrity and confidentiality of runtime data

TA Keys Access Control SFP:

- Purpose: To control the access to TA keys, which is granted to the TA that owns the key only. This policy contributes to the confidentiality of TA keys.

Trusted Storage Access Control SFP:

- Purpose: To control the access to TA storage where persistent TA data and keys are stored, which is granted on behalf of the owner TA only. This policy also enforces the binding of TA trusted storage to the TEE storage root of trust OB.SRT

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001[18]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[17] and the Common Evaluation Methodology (CEM)[19].

SERTIT monitored the evaluation which was carried out by the Name of EVIT Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR) [20] to SERTIT on 22 February 2018. SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC part 3 [4]. These classes comprise the EAL2 assurance package augmented with AVA_TEE.2.

Assurance class	Assurance Components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Use of CM System
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Evidence of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.2	Vulnerability analysis
	AVA_TEE.2	Vulnerability analysis of the TEE

All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[20] under the CC Part 3[17] headings.

The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

The ST[1] defines the life cycle and delivery phase of the toe in section 1.5.3

On receipt of the TOE, the consumer is recommended to check that the evaluated versions of its constituent components have been supplied, and to check that the security of the TOE has not been compromised in delivery.

The delivery procedure is described in the supporting document[12]

5.3 Installation and Guidance Documentation

Preparation and Operative procedures are described in supporting document[5]and[6]

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. The Huawei iTrustee v2.0 shall be used in combination with the guidance documentation [5]and[6] for the TOE in order to ensure that the TOE is operated in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

A Basic vulnerability analysis extended with the requirements extended by AVA_TEE.2 was done, consisting of the following steps:

- A design review session with the developer was performed focusing in understanding the technology and internals of the Secure Operating System which allows better compression of the key functionalities covered by SFRs claimed in ST and Security Mechanisms claimed in ARC.
- The review of the evaluation evidences (ST, the functional specification, the TOE design, the security architecture description and the guidance documentation) resulting in list of potential vulnerabilities. These potential vulnerabilities concluded in a penetration test plan after validate their applicability based on the assessment of multiple sources of information publicly available and the TOE environment.
- The penetration tests were performed according to the penetration test plan.

- Upon finalizing the initial penetration tests, the vulnerability analysis was revisited and some test were re-done. To solve the exploitations, the developer decided to remove some features from the TOE scope and extend the rules of the offline TA verification procedure.

5.6 Developer's Tests

The developer tests consist of different parts, focused on the different core components as described in Annex B.

Testing is performed using development images, images implementing a debug version and the finalized design.

Test consists on executing the following proprietary test suites in a test device.

- Client API
- TA management
- Memory management
- Cryptographic service
- Trusted storage service
- Secure time
- Property
- Other API syscall

5.7 Evaluators' Tests

The evaluator's responsibility for performing independent testing is required by the ATE_IND.2 class.

The evaluator used different TOE test configurations using engineering samples, samples implementing a debug version and the finalized design.

The evaluator performed the testing only in Huawei Kirin 960 as the TEE OS is a software component that it is executed on either of the hardware platforms. As shown in the above-mentioned table, there are no security-relevant differences between the hardware platforms. The design of the SoC isolates the hardware via hardware abstraction layer which hides the minor differences between the hardware platforms without any relevant differences at security level

	Huawei Kirin 970		Huawei Kirin 960	
CPU architecture	64-bits BIG.LITTLE		64-bits BIG.LITTLE	
Core configuration	4x Cortex A73 @ 2.4GHz 4x Cortex A53 @ 1.8GHz		4x Cortex A73 @ 2.36GHz 4x Cortex A53 @ 1.84GHz	
Trustzone	Cortex A73	Cryptocells 300 (aes cryptographic	Cortex A53	Cryptocells 300 (aes cryptographic

		engine)		engine)
		Virtualization support		Virtualization support
		NX-bit		NX-bit
		SIMP		SIMP
GPU	Mali-G72 MP12		Mali-G71 MP8	
Manufacturing	TSMC 10nm		FinFET 16nm	
RAM	4X LPDDR4		2X LPDDR4	
LTE Modem	LTE cat 18		LTE cat 12	
Flash interface	UFS 1.2		UFS 1.2	
Media Processing	2160p60 HEVC & H.264 Decode 2160p30 Encode HR10		2160p30 HEVC & H.264 Encode & Decode 2160p60 HEVC decode	
Neural Processing Unit	Yes		No	

Note that all the testing approach is focused on the software features as no hardware dependency has been relevant in the whole test plan. The testing assurance on both devices could be considered commensurate and the results obtained on the Huawei Kirin 960 could be extended to the Huawei Kirin 970.

Tests:

- Chain of trust
- TA whitelist test
- Corrupted TA test
- Forbidden communication

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR [20], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Huawei iTrustee version 2.0 meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 2+ augmented with AVA_TEE.2 as claimed in the Security target [1].

6.2 Recommendations

Prospective consumers of Huawei iTrustee version 2.0 should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

These guidance documents include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

Component	Version	Package
TrustedCore Release RPRPion iTrustee_2.0	2.0	Binary Image
Huawei iTrustee Preparative Procedure for User	1.5	Document
Huawei iTrustee Operational User Guidance	1.4	Document

TOE Documentation

The supporting guidance documents evaluated were:

[a] Huawei iTrustee Preparative Procedure for User, version 1.5

[b] Huawei iTrustee Operational User Guidance, version 1.4

[Further discussion of the supporting guidance material is given in Section 5.3 "Installation and Guidance Documentation".]

TOE Configuration

The following configuration was used for testing:

The several TOE Software configurations has been used for testing.

IMAGE	*DESCRIPTION*	*IDENTIFIER (hash sha256sum)*
IMG_1	*Debug image without TEE OS verification*	*48c60024ec36c1b0816a559611e9a1636148186643fc1760f963f7d6edec415c*
IMG_2	*Debug image with TEE OS verification*	*ce16c89e1823bd45c1759e811dca4c6d8b66bfc500a085465a664e296353d78a*
IMG_3	*Debug image without TUI support*	*dacb504be1718c99d3cbdb306662bdf67915afafc2600daf441f9216c7532be5*
IMG_4	*Final Debug image*	*63b3570a1de1a19d9de99251f64af7bbbd3db2d5c1a18b31e211441ed182006b*
IMG_5	*Release Debug image*	*2ca9ece1224aebe53e74549cab3f3e66c78b14ad28e3b8f3ebc830874fcc5fea*

Environmental Configuration

The following environment configuration was used for testing:

- Hardware
  - Huawei Kirin series SOC, such as Kirin 960 or Kirin 970
- Firmware used to provide the TEE security functionality
  - Bootloader (fastboot v1.0)
  - Bl31 monitor (ARM Trusted Firmware v1.3)
- The Trusted Applications(1)
- The Rich Execution Environment
  - EMUI, Huawei customized Android OS
  - SDK for Android app to communicate with iTrustee
- The Client Applications.
  - Device driver for iTrustee in Android

[1] The TOE image (Huawei iTrustee v2.0) embeds some built-in TA/s which provides off-the-shelf features (such as: rpmb, ssa or antirooting among others) but these built-in TA/s are out of the scope.

Annex B: TOE's security architecture

The TEE is embedded in the device and runs alongside a standard OS or Rich Execution Environment. Figure 1 provides a high level view of the software components of a TEE-enabled device, independently of any hardware architecture.

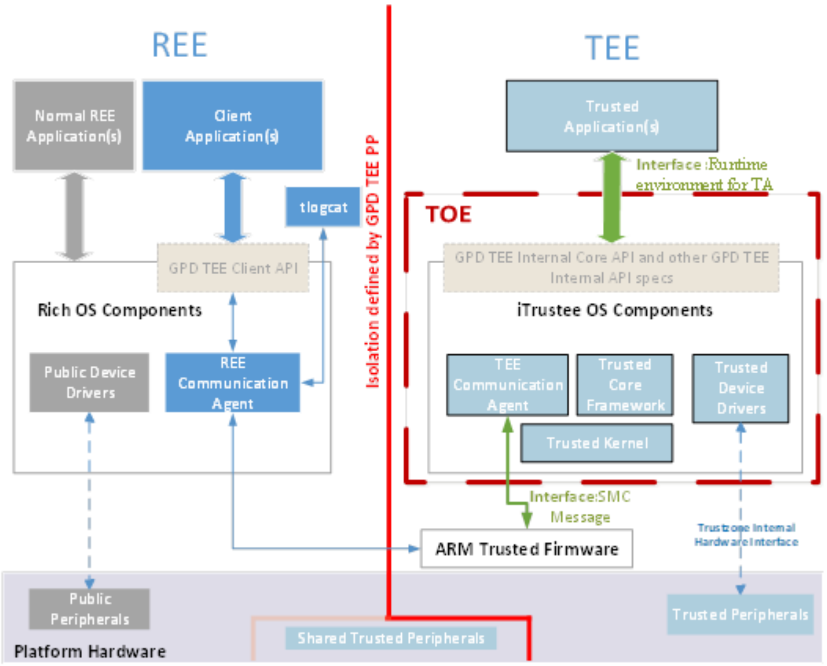

Figure 1 The architecture of a TOE-enabled device

The TEE software architecture identifies two distinct classes of components:

- The Trusted Applications that run on the TEE and use the TEE Internal API
- The Trusted OS Components whose role 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

The REE software architecture identifies also two distinct classes of components:

- The Client Applications which make use of the TEE Client API to access the secure services offered by TAs running on the TEE
- The Rich OS, which provides the TEE Client API and sends requests to the TEE

The TEE software external interface comprises the TEE Internal API (used by the Trusted Applications) and the TEE Communication Agent protocol (used by the REE).

The communication protocol between the REE and the TEE, used below the TEE Client API level, is implementation-dependent, and therefore this ST does not mandate any particular protocol. The security targets conformant to this ST shall describe all software interfaces used for communication with the TEE from the REE.

The trusted peripherals including timer modules which are provided by the SoC. The TOE acquires reliable time and RNG from trusted peripherals via the Trustzone internal Hardware interface.

The IT product identified in this certificate has been evaluated at the Norwegian evaluation facility described on this certificate using Common Methodology for IT Security Evaluation, according to the version number described on this certificate, for conformance to the Common Criteria for IT Security Evaluation according to the version number described on this certificate. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunctionwith the complete Certification report. The evaluation has been conducted in accordance with the provisions of The Norwegian Certification Authority for IT Security (SERTIT) and the conclusions of the evaluation technical report are consistent with the evidence adduced. Certification does not guarantee that the IT product is free from security vulnerabilities. This certificate only reflects the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown of this certificate. This certificate is not an endorsement of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.

Certificate

Product Manufacturer: Huawei Technologies Co., Ltd

Product Name: Huawei iTrustee

Type of Product: IC

Version and Release Numbers: V2.0

Assurance Package: EAL 2 augmented with augmented by AVA_TEE.2

Evaluation Criteria: Common Criteria v. 3.1 R4

Name of IT Security Evaluation Facility: Brightsight B.V.

Name of Certification Body: SERTIT

Certification Report Identifier: SERTIT-108 CR Issue 1.0, 22 February 2018

Certificate Identifier: SERTIT-108 C

Date Issued: 22 February 2018

Kjartan Jæger Kvassnes
Certifier

Arne H. Rage
Arne Høye Rage
Quality Assurance

Jørn Arnesen
Head of SERTIT

SERTIT
Norwegian Certification Authority for IT Security

CCRA recognition for components up to EAL 2 and ALC_FLR only.

SOGIS
SOGIS MRA recognition for components up to EAL 4.