Reference: 2019-30-INF-4106- v1
Target: Pública
Date: 07.07.2023

Created by: CERT10
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2019-30**
TOE	**Huawei DOPRA SSP V300R005C00SPC123B200**
Applicant	**440301192W - HUAWEI Technologies Co., Ltd.**
References	
	[EXT-5169] Solicitud certificación DOPRA

Certification report of the product Huawei DOPRA SSP V300R005C00SPC123B200, as requested in [EXT-5169] dated 12/07/2019, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-8470] received on 31/03/2023.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei DOPRA SSP V300R005C00SPC123B200.

The TOE is a software library widely used in Huawei products. It can be dynamically linked with a designated APP.

Developer/manufacturer: HUAWEI Technologies Co., Ltd.

Sponsor: HUAWEI Technologies Co., Ltd..

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: DEKRA Testing and Certification S.A.U.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL4+ (ALC_FLR.1).

Evaluation end date: 01/06/2023

Expiration Date[1]: 05/07/2028

All the assurance components required by the evaluation level EAL4 (augmented with ALC_FLR.1) have been assigned a “PASS” verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product Huawei DOPRA SSP V300R005C00SPC123B200, a positive resolution is proposed.

TOE SUMMARY

The TOE is a software library widely used in Huawei products. It can be dynamically linked with a designated APP and implements these major security feature:

- Auditing

  The TOE records audit logs for detected security events.

- Message Protection

  The TOE monitors and verifies the incoming and outgoing messages. Generates a security log with an associated alarm severity level and sends an alarm to the user.

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

- Memory monitoring

  The TOE monitors the memory. Generates a security log with an associated alarm severity level and sends an alarm to the user.

- Black Box Protection

  The black box monitors the internal memory and the file system of the TOE, transfers logs from memory to files (dumping mechanism).

- Resource utilization

  The TOE detects system resources (memory) overload and message flow control mechanism. Allocates resources for each APP process.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4 and the evidences required by the additional component ALC_FLR.1, according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE.TSS.1
ADV	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1
	ADV_TDS.3
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.1
	ALC_LCD.1
	ALC_TAT.1
	ALC_FLR.1
ATE	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.3

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5:

	Functional Requirements
FAU_GEN.1	Audit data generation
FAU_SAA.1	Potential violation analysis
FAU_ARP.1	Security alarms
FAU_STG.4	Prevention of audit data loss
FRU_PRS.1	Limited priority of service
FRU_RSA.2	Minimum and maximum quotas
FDP_SDI.2	Prevent data user modification and action
FDP_UIT.1	Data exchange integrity
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes

IDENTIFICATION

Product: Huawei DOPRA SSP V300R005C00SPC123B200

Security Target: Huawei DOPRA SSP V300R005C00SPC123B200 Security Target (version 1.3, 29/03/2023).

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL4+ (ALC_FLR.1).

SECURITY POLICIES

The use of the product Huawei DOPRA SSP V300R005C00SPC123B200 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target, section 3.2 (“Organizational Security Policies (OSP)”).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The detail of these assumptions is documented in the Security Target, section 3.3 (“Assumptions”).

CLARIFICATIONS ON THREATS

Generally speaking, the threats, when listed in the security target, do not suppose a risk for the TOE although the agents implementing attacks have the attack potential according to the *Enhanced Basic* attack potential of EAL4 (when fulfilling the usage assumptions and the proper security policies satisfaction). For any other threat not included in the security target, the evaluation results of the product security properties and the associated certificate do not guarantee any resistance.

Nevertheless, in this case, all the security objectives of the security target are derived from assumptions and Organizational Security Policies (OSPs) only. Therefore, there is no any threat identified for this TOE.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 4.2 (“Security Objectives for the operational Environment”).

ARCHITECTURE

LOGICAL ARCHITECTURE

From a logical perspective, the security features of the TOE are:

1. Auditing
    - Records log in the TOE internal memory, when a security event is detected by the TOE.
    - Associates timestamp with each security events detected by the TOE.
2. Message Protection:
    - Monitoring and Alarm
        - When message is damaged, the TOE sends alarm to the APP, and generates an event log.
    - Message transmission verification

- Inserts CRC (for more details about CRC, please refers to Appendix C) in each outgoing message.
- Check the CRC for each incoming message. If the verification fails, the message is discarded, the TOE generates an event log.

3. Memory monitoring
   - Monitoring and Alarm
     - When memory is damaged, the TOE sends alarm to the APP, and generates an event log.
4. Black Box Protection
   - Supports log dumping[2], when the memory black box area is full.
5. Resource Utilization
   - Resource specification restriction and partition
     - Creates different message/memory partitions and message token buckets for each module with their own minimum and maximum size setting.
     - Message priority management to ensure that high-priority messages obtain resources first in each module.
     - When each message/memory partition usage is exceeding the threshold, the TOE sends alarm to APP, and generates an event log.
     - Each APP process[3] partitions (message and memory) are independent, even if one partition is damaged or insufficient, partitions from another APP process will be not affected.
   - Running Overload Protection
     - The message scheduling supports message priority scheduling control. In addition, supports the message token bucket mechanism to implement message flow control.

PHYSICAL ARCHITECTURE

From a physical point of view, the TOE is comprised of a software package and guidance documents.

[2] Dumping: Action to write the content of the memory black box area into a file in the black box file system.

[3] APP Process: A consistent and closely related software organization, consisting of program (APP linked to the TOE) and data structures. One process runs multiple modules.

Software and Documents	Description	Remark
DOPRA SSP V300R005C00SPC123B200 SDK.rar March 2022, SHA256 checksum: 7fb343952f55614728a21ec217d32e106757a5e5930bd0e6adc396cd2ba5df3f	Middleware software package (In the form of binary compressed files). The suffix of the software package is '.rar'	The software package includes the TOE.
Huawei DOPRA SSP V300R005C00SPC123B200 AGD_OPE v0.73.pdf February 2023, SHA256 checksum: 758bb09cee309c4eaf86bfc1eec2f3debc226e394288b25c6114714d84012477	Security management guide.	The security management guide of DOPRA SSP Software.
Huawei DOPRA SSP V300R005C00SPC123B200 AGD_PRE v0.73.pdf March 2023, SHA256 checksum: 3406a247d916720f1394fc3f577f60bf75cb0eb59c6c9fb053fcfa5be032d34f	Installation Guide.	The installation guide of DOPRA SSP Software.
Huawei DOPRA SSP V300R005C00SPC123B200 API and Configuration Reference.chm V3.0 August 2022, SHA256 checksum: 9e70462503a99a3ed5cc34a72d4ad5ec0ed5e8c9f57c141d5c1d7bf1c6eea788	Interface guide	The interface guide of DOPRA SSP Software.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- **Huawei DOPRA SSP V300R005C00SPC123B200 AGD_OPE v0.73.pdf**
  - Description: Security management guide.
  - Date: February 2023.
  - SHA256 checksum: 758bb09cee309c4eaf86bfc1eec2f3debc226e394288b25c6114714d84012477
- **Huawei DOPRA SSP V300R005C00SPC123B200 AGD_PRE v0.73.pdf**
  - Description: Installation Guide.
  - Date: March 2023
  - SHA256 checksum: 3406a247d916720f1394fc3f577f60bf75cb0eb59c6c9fb053fcfa5be032d34f
- **Huawei DOPRA SSP V300R005C00SPC123B200 API and Configuration Reference.chm V3.0**

- Description: Interface guide.
- Date: August 2022
- SHA256 checksum: 9e70462503a99a3ed5cc34a72d4ad5ec0ed5e8c9f57c141d5c1d7bf1c6eea788

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests verifying that the obtained results are consistent with the results obtained by the developer.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product Huawei DOPRA SSP V300R005C00SPC123B200 it is necessary the disposition of the following software components:

Item	Item type	Comments
libdopra.so (TOE)	Software library	libdopra.so is the shared object resulting of compiling the DOPRASSP SDK
APP	Software	an application developed by the evaluator to test the functionality of the TOE. Each program developed for the testing that has dopra as dependency can be thought as an APP
Python version 3.10.0 with scapy 2.4.5	Software. Auxiliary testing component	
GCC version 7.3.0	Software. Auxiliary testing component	
VMWare Environment 16.2.3 build-19376536	Virtual Machine	Host of the SUSE Linux Enterprise Server 12 x64. All the testing of the TOE was executed within the SUSE operating system
SUSE Linux Enterprise Server 12 x64	Operating system	Guest OS of the virtual machine

EVALUATION RESULTS

The product Huawei DOPRA SSP V300R005C00SPC123B200 has been evaluated against the Security Target: Huawei DOPRA SSP V300R005C00SPC123B200 Security Target (version 1.3, 29/03/2023).

All the assurance components required by the evaluation level EAL4 have been assigned a "PASS" verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL4 + ALC_FLR.1, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

- It is mandatory to strictly follow the steps indicated in the installation documentation in order to download and install the correct version of the TOE and the cumulative update in a proper manner.
- The user guidance must be read and understood in order to operate the TOE in an adequate manner according to the security target.
- The fulfilment of the assumptions indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.

COMMENTS & RECOMMENDATIONS FROM THE CERTIFIER

Considering the obtained evidences during the instruction of the certification request of the product Huawei DOPRA SSP V300R005C00SPC123B200, a positive resolution is proposed.

- Since the assumption A.OS defined in the section 3.3 Assumptions within the [ST] states that the applications that can send data to the TOE are not attackers, these applications will not try to send malformed data that could cause buffer overflow, integer overflow, etc, leading into the execution of arbitrary code, denial of service, etc.
- Although the TOE has potential public vulnerabilities, according to the evaluator's vulnerability analysis, the restrictions described throughout the complete security problem remove the attack paths that could be used to successfully provoke the behaviour described in those public vulnerabilities. Moreover, according to the evaluator's analysis of the [ST], the TOE is protected against physical access, users and persons in charge of the installation procedures are trusted, data received from TOE environment should not be constructed in a form that induces errors in the system, etc. This is why all TOE security objectives are traced to organizational security policies OSPs.

GLOSSARY

CCN Centro Criptológico Nacional

CNI Centro Nacional de Inteligencia

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

OC Organismo de Certificación

TOE Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[ST] Huawei DOPRA SSP V300R005C00SPC123B200 Security Target (version 1.3, 29/03/2023).

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- Huawei DOPRA SSP V300R005C00SPC123B200 Security Target (version 1.3, 29/03/2023).

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-

2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.