Reference: 2018-58-INF-3355-v1
Target: Público
Date: 08.02.2021

Created by: CERT11
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2018-58**
TOE	**Huawei FusionSphere 6.5.RC1.T7**
Applicant	**440301192203821 - Huawei Technologies Co., Ltd.**
References	

[EXT-4414] Certification Request

[EXT-6275] Evaluation Technical Report

Certification report of the product Huawei FusionSphere 6.5.RC1.T7, as requested in [EXT-4414] dated 09/11/2018, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-6275] received on 19/10/2020.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei FusionSphere 6.5.RC1.T7.

The Target of Evaluation (TOE) is a cloud operating system (OS) solution. The TOE consists of the cloud resource management layer and virtualization layer of the solution, that is, FusionSphere OpenStack and UVP.

Developer/manufacturer: Huawei Technologies Co., Ltd.

Sponsor: Huawei Technologies Co., Ltd..

Certification Body: Centro Criptológico Nacional (CCN).

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

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 - EAL2 + ALC_FLR.2.

Evaluation end date: 10/11/2020.

Expiration Date[1]: 03/02/2026.

All the assurance components required by the evaluation level EAL2 (augmented with ALC_FLR.2) 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 EAL2 + ALC_FLR.2, 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 FusionSphere 6.5.RC1.T7, a positive resolution is proposed.

TOE SUMMARY

The Target of Evaluation (TOE) consists of FusionSphere OpenStack and the Unified Virtualization Platform (UVP).

The TOE provides the following key security features:

[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.

- VM Network Separation: The TOE supports virtual switches and virtual networks. VMs can be separated by creating different networks. Administrators can configure network isolation policies.
- VM isolation: The hypervisor isolates VMs running on the same physical server to prevent data theft and malicious attacks. VM users can only access resources (hardware and software resources and data) that belong to their own VMs.
- User and Privilege Management: The TOE supports role-based access control, used for the system maintenance personnel to access the virtualization platform and VMs. The table below shows list of roles defined in the TOE and the description of each role.
- TOE Access: The TOE offers functionality for terminating active sessions automatically after an inactivity period of time.
- Communications security: The TOE can be remotely accessed using a SSH connection, creating a trusted path between the TOE and the authorized users.
- Security audit: Operation logs record the security-relevant events performed by users on the system and the result of the operation and is used for tracing and auditing.
- Access control: Huawei FusionSphere software implements role-based access control, limiting access to different management functions to different roles as defined in administrator-defined access control associations.
- Authentication: Operators who access the TOE locally or remotely in order to execute device management functions are identified by individual user names and authenticated by passwords.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2 + and the evidences required by the additional component ALC_FLR.2, according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ADV	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.2
	ALC_CMS.2

	ALC_DEL.1
	ALC_FLR.2
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
ATE	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

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

SECURITY FUNCTIONAL REQUIREMENTS
FAU_GEN.1
FAU_GEN.2
FAU_SAR.1
FAU_SAR.2
FAU_STG.1
FAU_STG.3
FDP_ACC.1
FDP_ACF.1
FDP_IFC.1/VM Data
FDP_IFF.1/VM Data
FDP_IFC.1/VM Network
FDP_IFF.1/VM Network
FDP_RIP.1
FIA_AFL.1
FIA_UID.2
FIA_UAU.2
FIA_SOS.1
FIA_ATD.1
FMT_MSA.1
FMT_MSA.3
FMT_SMR.1
FMT_SMF.1

FMT_MOF.1
FTA_SSL.3
FTP_TRP.1

IDENTIFICATION

Product: Huawei FusionSphere 6.5.RC1.T7

Security Target: Huawei FusionSphere 6.5.RC1.T7 Security Target, version 1.0. 2020-10-06.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 - EAL2 + ALC_FLR.2.

SECURITY POLICIES

The use of the product Huawei FusionSphere 6.5.RC1.T7 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in [ST], chapter 3.4 (Organizational Security Policies).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions detailed in [ST], chapter 3.3 (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.

CLARIFICATIONS ON NON-COVERED THREATS

The threats detailed in [ST], chapter 3.2 (Threats) not suppose a risk for the product Huawei FusionSphere 6.5.RC1.T7, although the agents implementing attacks have the attack potential Basic of EAL2 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

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

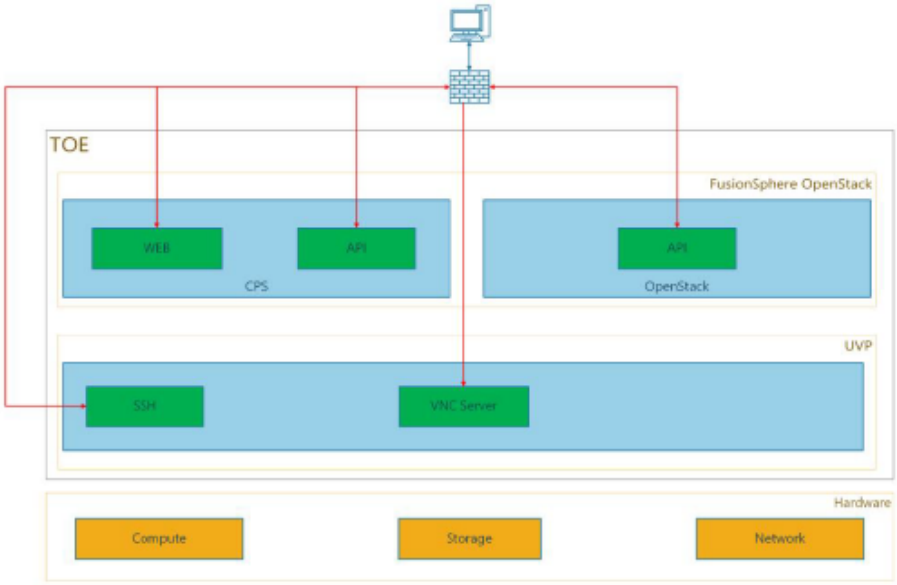
The security objectives declared for the TOE operational environment are detailed in [ST], chapter 4.2 (Objectives for the operational environment).

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ARCHITECTURE

LOGICAL ARCHITECTURE

Huawei FusionSphere is a cloud operating system (OS) solution. The TOE consists of the cloud resource management layer and virtualization layer of the solution, that is, FusionSphere OpenStack and UVP. The figure below illustrates the TOE architecture:



- FusionSphere OpenStack is the cloud resource management layer. Based on open-source OpenStack, FusionSphere OpenStack builds an open infrastructure platform and provides APIs for interoperability with community members. The southbound interfaces are based on the OpenStack ecosystem and ensure compatibility with heterogeneous compute, storage, and network devices from multiple vendors. AZ (Availability Zones) are created to isolate heterogeneous resources. Besides the open-source OpenStack, FusionSphere OpenStack

also includes a sub-system named CPS (Cloud Provision System), which implements the installation & deployment and configuration management of FusionSphere OpenStack.

- The UVP is the virtualization layer. Enhanced KVM (Kernel-based Virtual Machine) is used as the virtualization technology, with special focus on optimized performance and reliability. The UVP also provides the capability to generate and manage the audit logs and offers the support to secure communications for remote administration via SSH.

PHYSICAL ARCHITECTURE

FusionSphere software packages are binary compressed files. The following software packages are required and are part of the TOE:

- FusionSphere OpenStack 6.5.RC1.iso (Version 6.5.RC1).
- FusionSphere OpenStack Patch 6.5.T7.tar.gz (Version 6.5.T7).

DOCUMENTS

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

- Huawei FusionSphere 6.5.RC1.T7 Operational User Guidance, issue V0.6. 2020-10-05.
- Huawei FusionSphere 6.5.RC1.T7 Preparative Procedures, issue V0.6. 2020-10-05.
- Huawei FusionSphere 6.5.RC1.T7 Installing and Configuring single-Host, issue V0.3. 2019-06-24.
- Huawei FusionSphere 6.5.T7 Patch Guide, issue v0.1. 2019-06-19.
- Huawei FusionSphere 6.5.RC1.T7 API Reference, issue v0.4. 2019-06-24.

PRODUCT TESTING

The tests performed by both the evaluator and the developer are based on the TSFIs description included in the functional specification and the SFRs description included in the Security Target [ST].

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals. The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to the Security Target [ST].

The evaluator has repeated all the cases specified by the developer in the test documentation and has compared the obtained results with those obtained by the developer and documented in each associated report. The test repetition performed by the evaluator has demonstrated that the test

plan and report provided by the vendor contains information enough to make a reader able to repeat all tests included. Additionally, after the repetition, the evaluator has obtained the same results as the expected ones. The independent testing has covered 100% of SFRs of the [ST] and TSFIs defined in the functional specification for the TOE, sampling has not been performed. The test cases have taken into account critical parameters values, searching that the TOE behaves in a non-expected manner. There has not been any deviation from the expected results under the environment defined in the Security Target [ST].

EVALUATED CONFIGURATION

The TOE is defined by its commercial name and version number: Huawei FusionSphere 6.5.RC1.T7.

The acceptance procedure for the evaluated configuration of the TOE is described in section 2 (Secure Acceptance by User) of the preparative user guidance Huawei FusionSphere 6.5.RC1.T7 Preparative Procedures, issue V0.6. 2020-10-05.

To obtain the proper operation of the product according to the evaluated configuration the components indicated in section 1.3.3 (Non-TOE hardware and software) of the Security Target [ST] are required.

EVALUATION RESULTS

The product Huawei FusionSphere 6.5.RC1.T7 has been evaluated against the Security Target Huawei FusionSphere 6.5.RC1.T7 Security Target, version 1.0. 2020-10-06.

All the assurance components required by the evaluation level EAL2 + ALC_FLR.2have 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 EAL2 + ALC_FLR.2, 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.

- 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.
- The user guidance must be read and understood in order to operate the TOE in and adequate manner according to the security target.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product DEKRA Testing and Certification S.A.U., a positive resolution is proposed.

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 FusionSphere 6.5.RC1.T7 Security Target, version 1.0. 2020-10-06.

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is published. This document is identified as:

- Huawei FusionSphere 6.5.RC1.T7 Security Target, version 1.0. 2020-10-06.

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.org.

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.