Reference: 2017-60-INF-2765-v1
Target: Pœblico
Date: 10.05.2019

Created by: CERT9
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2017-60**
TOE	**Huawei OptiX PTN Series Products**
Applicant	**440301192203821 - Huawei Technologies Co., Ltd.**
References	

[EXT-3653] Solicitud Certificaci—n Huawei PTN

Certification report of the product Huawei OptiX PTN Series Products, as requested in [EXT-3653] dated 23/11/2017, and evaluated by Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-4913] received on 12/04/2019.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei OptiX PTN Series Products.

The TOE is a Network Element composed of a hardware platform and a software running within the platform as a whole system. The underlying operating system contained in the evaluated platforms (RTOS) is not part of the TOE.

Developer/manufacturer: Huawei Technologies Co., Ltd.

Sponsor: Huawei Technologies Co., Ltd..

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

ITSEF: Epoche & Espri S.L.U.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL3.

Evaluation end date: 12/04/2019.

All the assurance components required by the evaluation level EAL3 have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL3, 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 OptiX PTN Series Products, a positive resolution is proposed.

TOE SUMMARY

The TOE is a network element designed to be located in the core layer, aggregation layer and access layer of the metro transport network. It sets up the network of various types of services such as mobile communication and group customers. OptiX PTN series support mainly Layer 3 forwarding .

The major security features include: Authentication, Access Control, ACL, Auditing, Communication Security, Flow Control Policy, Security Management, Cryptographic functions.

The evaluated TOE includes several models including single-chassis systems and cluster systems. These models differ in their modularity and throughput by deploying different LPUs or different number of chassis, but they offer exchangeable forwarding unit modules, switch fabrics, and use the same version of software.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL3, according to Common Criteria v3.1 R5 .

Assurance class	Assurance components
ASE	ASE_INT.1 ASE_CCL.1 ASE_SPD.1 ASE_OBJ.2 ASE_REQ.2 ASE_TSS.1
ADV	ADV_ARC.1 ADV_FSP.3 ADV_TDS.2
AGD	AGD_OPE.1 AGD_PRE.1
ALC	ALC_CMC.3 ALC_CMS.3 ALC_DEL.1 ALC_DVS.1 ALC_LCD.1
ATE	ATE_COV.2 ATE_DPT.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_STG.1
FAU_STG.3
FCS_COP.1/AES Cryptographic operation
FCS_COP.1/ RSA Cryptographic operation

FCS_COP.1/ DSA Cryptographic operation
FCS_COP.1/SHA2
FCS_CKM.1/AES Cryptographic operation
FCS_CKM.1/ RSA Cryptographic operation
FCS_CKM.1/ DSA Cryptographic operation
FDP_ACC.1
FDP_ACF.1
FDP_IFC.1
FDP_IFF.1
FIA_AFL.1
FIA_ATD.1
FIA_SOS.1
FIA_UAU.1
FIA_UAU.5
FMT_MOF.1
FMT_MSA.1/VRP
FMT_MSA.1/ACLs
FMT_MSA.3/VRP
FMT_MSA.3/ACLs
FMT_SMF.1
FMT_SMR.1
FTA_SSL.3
FTA_TSE.1
FTP_TRP.1

IDENTIFICATION

Product: Huawei OptiX PTN Series Products

Security Target: CC Huawei OptiX PTN Series Products V100R009 Security Target, v0.5 (11 April 2019).

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL3.

SECURITY POLICIES

The Security Target [ST] does not define any Organizational Security Policy.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions detailed in [ST], chapter 3.2 (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 3.1 (Threats) do not suppose a risk for the product Huawei OptiX PTN Series Products, although the agents implementing attacks have the attack potential according to the Basic of EAL3 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

The TOE consists of three subsystems:

1. Management plane (MP).
    - Managing the external access, for example, access by means of SSH port.
    - Providing the authentication and authorization functions.
    - Providing the Command communication with user.

- Receiving the log information of CP and MP subsystems.
- Exporting logs in the specified format to logfile.
- Managing all log.

2. Control plane (CP).

- Managing and executing the configuration commands of all the subsystems.
- Parsing and executing command.
- Saving, restarting, and recovering configuration information.
- Sending log information to the MP subsystem

3. Forwarding plane (FP).

- Managing routing information (including the static routes configured through the CLI).
- Forwarding packets or sending packets receiving and formatting ACL rule data into formation required.
- Associating ACL number to a whitelist entry in policy.
- Sending log information to the MP subsystem.
- Filtering packets according to ACL.

PHYSICAL ARCHITECTURE

The TOE provides several models including single-chassis systems and cluster systems. These models differ in their modularity and throughput by deploying different LPUs or different number of chassis, but they offer exchangeable forwarding unit modules and switch fabrics.

The details about the chassis and units included in each platform are described in [ST], chapter 1.4.1 (Physical scope).

DOCUMENTS

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

Document title	Version
CC OptiX PTN Series Product V100R009 Preparative Procedures for Production	0.4
CC OptiX PTN Series Product V100R009 Operational User Guide	0.4
OptiX PTN 905E V100R009C00 Command Reference 02.chm	0.2
OptiX PTN 910E-F V100R009C10 Command Reference 01.chm	0.1
OptiX PTN 990&970 V100R009C10 Command Reference 01.chm	0.1

OptiX PTN 7900 V100R009C10 Command Reference 01.chm	0.1
OptiX PTN 905E V100R009C00 Product Documentation 02.zip	0.2
OptiX PTN 910E-F V100R009C10 Product Documentation 03.zip	0.3
OptiX PTN 970 V100R009C10 Product Documentation 03.zip	0.3
OptiX PTN 990 V100R009C10 Product Documentation 03.zip	0.3
OptiX PTN 7900-12 V100R009C10 Product Documentation 03.zip	0.3
OptiX PTN 7900-24 V100R009C10 Product Documentation 03.zip	0.3
OptiX PTN 7900-32 V100R009C10 Product Documentation 03.zip	0.3

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.

In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

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

The TOE comprises seven platforms of the PTN Series products and two types of software (V100R009C10SPC100 & V100R009C00SPC200); the correspondence between the platform and the software version running on it is shown in the table below.

Evaluated platform identifier	Software version
Optix PTN 7900-32	V100R009C10SPC100
Optix PTN 7900-24	V100R009C10SPC100
Optix PTN 7900-12	V100R009C10SPC100
Optix PTN 905E	V100R009C00SPC200
Optix PTN 910E-F	V100R009C10SPC100
Optix PTN 970	V100R009C10SPC100
Optix PTN 990	V100R009C10SPC100

The software packages associated to each evaluated platform are shown in the table below.

Package name	Software	Platform ID	Software version
OptiX PTN 905E V100R009C00SPC200 .zip.asc	PTN90XV100R009C00SPC200.cc	905E	V100R009C00SPC200
OptiX PTN 910E-F V100R009C10SPC100 .zip.asc	PTN910E-FV100R009C10SPC100.cc	910F	V100R009C10SPC100
OptiX PTN 970 V100R009C10SPC100 .zip.asc	PTN970V100R009C10SPC100.cc	970	V100R009C10SPC100
OptiX PTN 990 V100R009C10SPC100 .zip.asc	PTN990V100R009C10SPC100.cc	990	V100R009C10SPC100
OptiX PTN 7900-12 V100R009C10SPC100 .zip.asc	PTN7900V100R009C10SPC100.cc	7900-12	V100R009C10SPC100
OptiX PTN 7900-24 V100R009C10SPC100 .zip.asc	PTN7900V100R009C10SPC100.cc	7900-24	V100R009C10SPC100
OptiX PTN 7900-32 V100R009C10SPC100 .zip.asc	PTN7900V100R009C10SPC100.cc	7900-32	V100R009C10SPC100

The product provides some additional functionalities which are not included in the evaluated configuration.

Excluded Functionality	Excluded Rationale
BGP, ISIS, OSPF	BGP ISIS, OSPF will be disabled in the evaluated configuration
RSVP	RSVP will be disabled in the evaluated configuration
SNMP	SNMP will be disabled in the evaluated configuration
TOE management through Netconf interface (port 830)	Netconf interface will be disabled in the evaluated configuration
TOE management through DCN interface (ports 1400 and 5432)	DCN interface will be disabled in the evaluated configuration.

EVALUATION RESULTS

The product Huawei OptiX PTN Series Products has been evaluated against the Security Target: CC Huawei OptiX PTN Series Products V100R009 Security Target, v0.5 (11 April 2019).

All the assurance components required by the evaluation level EAL3 have been assigned a "PASS" verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL3, 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 Epoche & Espri S.L.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] CC Huawei OptiX PTN Series Products V100R009 Security Target, v0.5 (11 April 2019).

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: CC Huawei OptiX PTN Series Products V100R009 Security Target, v0.5 (11 April 2019).

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 recognized 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.