Reference: 2019-50-INF-3506- v1
Target: Público
Date: 17.05.2021

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

CERTIFICATION REPORT

Dossier #	**2019-50**
TOE	**Huawei ECC800 software management component version V100R021C00SPC100**
Applicant	**440301192203821 - Huawei Technologies Co., Ltd.**
References	

[EXT-5508] Certification request

[EXT-6723] Evaluation Technical Report

Certification report of the product Huawei ECC800 software management component version V100R021C00SPC100, as requested in [EXT-5508] dated 10/10/2019, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-5508] received on 23/03/2021.

CONTENTS

EXECUTIVE SUMMARY 3
TOE SUMMARY 3
SECURITY ASSURANCE REQUIREMENTS 4
SECURITY FUNCTIONAL REQUIREMENTS 5
IDENTIFICATION 5
SECURITY POLICIES 6
ASSUMPTIONS AND OPERATIONAL ENVIRONMENT 6
CLARIFICATIONS ON NON-COVERED THREATS 6
OPERATIONAL ENVIRONMENT FUNCTIONALITY 6
ARCHITECTURE 7
LOGICAL ARCHITECTURE 7
PHYSICAL ARCHITECTURE 8
DOCUMENTS 9
PRODUCT TESTING 9
EVALUATED CONFIGURATION 9
EVALUATION RESULTS 10
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM 10
CERTIFIER RECOMMENDATIONS 10
GLOSSARY 10
BIBLIOGRAPHY 11
SECURITY TARGET 11
RECOGNITION AGREEMENTS 12
European Recognition of ITSEC/CC – Certificates (SOGIS-MRA) 12
International Recognition of CC – Certificates (CCRA) 12

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei ECC800 software management component version V100R021C00SPC100.

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 - EAL3 + ALC_FLR.2.

Evaluation end date: 15/04/2021.

Expiration Date[1]: 18/05/2026.

All the assurance components required by the evaluation level EAL3 (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 EAL3 + 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 ECC800 software management component version V100R021C00SPC100, a positive resolution is proposed.

TOE SUMMARY

The ECC800 software is a software product running on the Linux operating system based on the ARM chip of the Cortex-A7 architecture. In the northbound direction, the ECC800 software provides web-based login for connecting to manage the TOE. In the southbound direction, the ECC800 controller collects and configures signals, and manages alarms for southbound components.

The TOE is a software to manage and monitor devices inside the smart module data center. It provides a web interface that allow users to operate with the TOE in order to change values and parameters

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.

- Authentication and Authorization: Only authenticated users are allowed to log in to the TOE, query TOE data, and set TOE parameters. Only authorized users are able to execute the previous actions based on their privileges. If a user fails to be authenticated for multiple consecutive times, the user is locked to prevent unauthorized access.
- Auditing: An operation log records the operation that a local administrator has performed on the system and the result of the operation and is used for tracing and auditing. Only authorized local administrators can review and query the records.
- Management: The TOE provides two different user roles (administrator and operator). Also, the TOE provides the functionality to manage: time settings, user configuration, updates and logs export.
- TOE Access: The TOE is able to manage the concurrent multiple sessions by limiting the number of active sessions per user. The TOE is also able to terminate an interactive session after an inactivity period of time.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL3 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.3
	ADV_TDS.2
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.3
	ALC_CMS.3
	ALC_DEL.1
	ALC_FLR.2
	ALC_DVS.1
	ALC_LCD.1
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.2
	ATE_FUN.1

	ATE_DPT.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_EXT.3
FAU_GEN.2
FAU_SAR.1
FAU_SAR.2
FAU_STG.1
FAU_STG.3
FDP_ACC.1
FDP_ACF.1
FDP_AFL.1
FDP_ATD.1
FIA_UAU.2
FIA_UAU.6
FIA_UID.2
FMT_MOF.1
FMT_MSA.1
FMT_MSA.3
FMT_SMF.1
FMT_SMR.1
FMT_MCS.1
FPT_STM.1
FTA_SSL.3
FTA_SSL.4
FTA_TSE.1
FTA_TAB.1

IDENTIFICATION

Product: Huawei ECC800 software management component version V100R021C00SPC100

Security Target: CC Huawei ECC800 V100R021C00SPC100 Security target, v1.3, March 4, 2021.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 - EAL3 + ALC_FLR.2.

SECURITY POLICIES

The use of the product Huawei ECC800 software management component version V100R021C00SPC100 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 3.3 (Organizational Security Policies).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions detailed in [ST], chapter 3.4 (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 ECC800 software management component V100R021C00SPC100, although the agents implementing attacks have the attack potential according to the High of EAL3 + ALC_FLR.2 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 (Security Objectives for the Operational Environment).

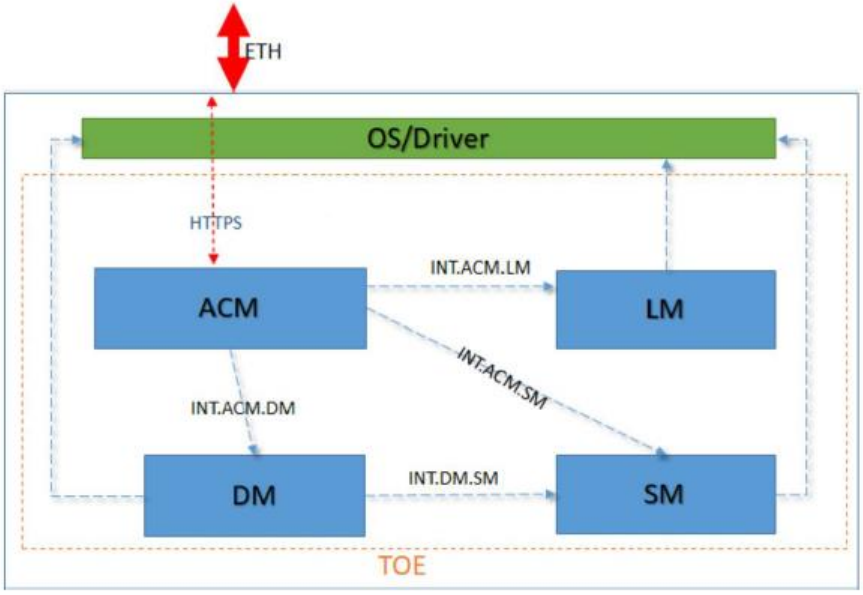
The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ARCHITECTURE

LOGICAL ARCHITECTURE

No	Subsystem	Description
1	ACM: Access and Control Management Subsystem	The ACM subsystem provides the following functions: - Remotely logs in to the TOE through web, and views the device running information and alarm status and modify configuration parameters.
2	LM: Log management Subsystem	The LM subsystem provides the following functions: - Records the details about device operations and control. - Records device run logs and security logs in real time.
3	SM: Security management Subsystem	The SM subsystem call for an external entity called KMC for the following functions: - Basic security algorithm functions. - Management security certificates.
4	DM: Data Storage	The DM subsystem provides the following functions: - Collects, processes, and locally stores device data. - Processes and reports device alarms.

Interaction Between TSF Subsystems:



The TOE provides the following key security features:

- Authentication and Authorization.
- Auditing.
- Management.
- TOE Access.

PHYSICAL ARCHITECTURE

The TOE is a 'software only', TOE consists of the application software, but not the underlying OS and hardware, which the application software is running on.

The software package (along with its signature file) and the guidance documentation are delivered in the support website. To TOE documentation is public and can be downloaded once a user has created a Huawei account in the webpage. The steps required to download the TOE software are described in the TOE documentation.

The components of the TOE are identified in the table below:

Type	Delivery Item	Version	Format	SHA256
Software	The package downloaded from the website is: ECC800V100R021C00SPC100.zip The TOE is a software included within the mentioned package and named as: ECC800V100R021C00SPC100.tar.gz	V100R021C00SPC100	Package: zip TOE: tar.gz	ECC800V100R021C00SPC100.zip: eaf076a0e9f8b9ae7bc39bdb3bfa5133beba062d3d4648b6d392d06966d7f41a ECC800V100R021C00SPC100.tar.gz: 12fa92e9cbeb1c1f2d13651b3d7070eb7b6a7032180a52591e8a8f420623bd50
Software Signature File	ECC800V100R021C00SPC100.zip.asc	-	.asc	-
Product Guidance	ECC800 Data Center Controller V100R021C00 User Manual (for ECC800-Pro).pdf	0.2	PDF	75b8ae894dab955d4e5a4da1652792f636b5cddd062f85ab80d8469438e1fae6
	CC Huawei ECC800 V100R021C00SPC100–AGD_OPE V1.8	1.8	PDF	06469a8bcf85f3c0b0328badfbfd4fe6fdf6a00a5cdd4285f1f908e1bbaed622
	CC Huawei ECC800 V100R021C00SPC100–AGD_PRE V1.7	1.7	PDF	2fc6d311b1e259eaba695e8364b011d0629b5d2011693af1d936baca16ddb19b

DOCUMENTS

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

- CC Huawei ECC800 V100R021C00SPC100 - AGD_PRE, 1.7, March 4 2021
- CC Huawei ECC800 V100R021C00SPC100 - AGD_OPE, 1.8, March 4 2021
- ECC800 Data Center Controller V100R021C00 - User Manual (for ECC800-Pro), version 0.2, September 7, 2020

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 ECC800 software management component version V100R021C00SPC100.

The acceptance and installation procedures are given in the preparative user guidance CC Huawei ECC800 V100R021C00SPC100 - AGD_PRE 1.7.

To obtain the proper operation of the product according to the evaluated configuration the components indicated in section 1.4.3 (Non-TOE hardware and Software) of the Security Target [ST] are required.

EVALUATION RESULTS

The product Huawei ECC800 software management component version V100R021C00SPC100 has been evaluated against the Security Target CC Huawei ECC800 V100R021C00SPC100 Security target, v1.3, March 4, 2021.

All the assurance components required by the evaluation level EAL3 + 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 evaluation level EAL3 + 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.

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

- CC Huawei ECC800 V100R021C00SPC100 Security target, v1.3, 2021-03-04.

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.