Reference: 2020-16-INF-3880-v1
Target: Pública
Date: 23.08.2022

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

CERTIFICATION REPORT

Dossier #	**2020-16**
TOE	**Huawei Cyber Security Compliance Testing Center**
Applicant	**440301192203821 - Huawei Technologies Co., Ltd.**
References	

[EXT-5823] Certification Request

[EXT-7737] Evaluation Technical Report

Certification report of the site Huawei Cyber Security Compliance Testing Center, as requested in [EXT-5823] dated 03/03/2020, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-7737] received on 29/04/2022.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the site Huawei Cyber Security Compliance Testing Center.

Developer/manufacturer: Huawei Technologies Co., Ltd.

Sponsor: Huawei Technologies Co., Ltd.

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Applus Laboratories

Protection Profile: No.

Evaluation Level: Common Criteria v3.1 R5

To re-use ALC certified security assurance components in evaluations up to EAL4 + AVA_VAN.5

Security Assurance Components: ALC_CMC.4, ALC_CMS.4, ALC_DVS.1, ALC_LCD.1, AST_INT.1, AST_CCL.1, AST_SPD.1, AST_OBJ.1, AST_ECD.1, AST_REQ.1 and AST_SSS.1

Resistance to Attack Potential: High.

Evaluation end date: 29/06/2022.

Re-use expiration date: 27/07/2022[1].

All the assurance components required by the evaluation have been assigned a “PASS” verdict are resistant to attackers with an High attack potential. Consequently, the laboratory Applus Laboratories assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied, as defined by the Common Criteria v3.1 R5, the supporting document guidance CCDB-2007-11-001 Site Certification [SCER] and the JIWG supporting document Minimum site security requirements [MSSR].

The assurance components are chosen in order to re-use ALC certified security assurance components in evaluations up to EAL4 + AVA_VAN.5. It has been assumed that the security measures are resistant to attacks performed by attackers with an *High* attack potential.

Considering the obtained evidences during the instruction of the certification request of the site Huawei Cyber Security Compliance Testing Center, a positive resolution is proposed.

[1] This audit was performed as a virtual site audit according to [IT-013] and [JIL-COVID] policies, and therefore the re-use of evaluation activities is limited at most to 18 months since the site audit date (27/01/2021) as this site has been previously certified by means of a virtual site audit only.

SITE SUMMARY

The Huawei Cyber Security Compliance Testing Center is located at

2F D4 D Area Administration Building,

Southern Factory of Huawei Technologies Co., Ltd.,

No. 6 Xincheng Avenue, Songshan Lake Technology Industrial Park,

Dongguan City, 523808, P.R. of China

SITE DESCRIPTION

HCSCTC is a secure testing center that provides testing design and compliance testing for information and communication technology (ICT) products and solutions, such as taxonomy Data encryption storage devices / tools, Firewall, Network Access Control Devices. Wireless Network Devices, Mobile devices, Routers, Network management tools, other devices – Virtualization software, Operating systems, Switches, Smart Cards and similar devices and Data exchange gateways. The client will provide ICT products and solutions to HCSCTC. After analysis, the testing center will perform a test design. This testing design will be related with security standards, such as the class ATE in common criteria (CEMv3.1R5). The HCSCTC will test if the product behaves as described in the ST and as specified in the evidence provided by the client, which is considered as the compliance testing.

The following zones have been taking into account in this security target and therefore they are the scope of the site certification regarding the physical measures implemented in their local perimeter.

- O1, O2: office room
- T1-T4: testing room
- S1: seminar room

TYPICAL LIFE CYCLE OF SUPPORTED TOEs

It is assumed that product certifications which refer to this certificate are related ATE activities of CC. It is expected that ITSEF reusing activities should evaluate the specific product life-cycle to verify that it is conformant to defined life-cycle defined ALC_LCD.1 evidences for this site. This site is not specific for the SmartCards and Similar devices technical domain and therefore it is not compliant to any defined life-cycle in [PP84]

SECURITY ASSURANCE REQUIREMENTS

The site was evaluated with all the evidence required to fulfil the evaluation activities resistant to attackers with a **High** attack potential, according to Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5.

The assurance components are chosen in order to re-use ALC certified security assurance components in evaluations up to EAL4 + AVA_VAN.5. Therefore, it has been assumed that the security measures are resistant to attacks performed by attackers with a High attack potential.

Assurance Class	Assurance Components
AST: Site Security Target Evaluation	AST_INT.1 SST introduction
	AST_CCL.1 Conformance claims
	AST_SPD.1 Security problem definition
	AST_OBJ.1 Security objectives
	AST_ECD.1 Extended components definition
	AST_REQ.1 Security assurance requirements
	AST_SSS.1 Site summary specification
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model

Please note that ALC_TAT is omitted, because the development tools and its versions are TOE specific and therefore it is more efficient to cover the whole ALC_TAT together with the product evaluation process

Please note that ALC_DEL.1 has been excluded from the SST since this site does not perform external deliveries and ALC_DEL.1 is therefore not applicable.

IDENTIFICATION

Site Name	Huawei Cyber Security Compliance Testing Center

Site Location	2F D4 D Area Administration Building, Southern Factory of Huawei Technologies Co., Ltd., No. 6 Xincheng Avenue, Songshan Lake Technology Industrial Park, Dongguan City, 523808, P.R. of China
Areas in the scope of the certificate as declared in the SST	See section 2.2 of [SST]
Activities in the product development	Life cycle phases: • No PP-0084 life-cycle phases covered. • Only ATE related activities expected in the scope.
Site Security Target	Site Security Target Huawei Cyber Security Compliance Testing Center, version 0.21. 28/02/2022.
Evaluation Level	Common Criteria v3.1 R5 To re-use ALC certified security assurance components in evaluations up to EAL4 + AVA_VAN.5.
Security Assurance Components	ALC_CMC.4, ALC_CMS.4, ALC_DVS.1, ALC_LCD.1, AST_INT.1, AST_CCL.1, AST_SPD.1, AST_OBJ.1, AST_ECD.1, AST_REQ.1 and AST_SSS.1.
Attack Potential	High

SECURITY POLICIES

Huawei Cyber Security Compliance Testing Center 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 Site Security Target [SST], section 4.3 Organisational Security Policies.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

Each site operating in a production flow must rely on preconditions provided by the previous site. Each site has to rely on the information received by the previous site/client. This is reflected by the assumptions that must be defined for the interface.

The detail of the assumptions considered to be applicable is documented in the Site Security Target [SST], section 4.4 Assumptions.

CLARIFICATIONS ON NON-COVERED THREATS

The threats documented in the Site Security Target [SST], section 4.2 Threats do not suppose a risk for the site Huawei Cyber Security Compliance Testing Center, although the agents implementing attacks have a High attack potential for the Security Assurance Requirements ALC_CMC.4, ALC_CMS.4, ALC_DVS.1, ALC_LCD.1, AST_INT.1, AST_CCL.1, AST_SPD.1, AST_OBJ.1, AST_ECD.1, AST_REQ.1 and AST_SSS.1, and always fulfilling the assumptions and the proper security policies satisfaction.

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

DOCUMENTS

The site evaluation has been based on the evidences listed in the chapter 5 (Evaluation evidence) of the Evaluation Technical Report of Huawei Cyber Security Compliance Testing Center [EXT-7737].

These evidences describe the global procedures and security measures in the site. For each specific TOE, some accessory documents including specific characteristics of the TOE should be provided in addition to the above evidences.

The above evidences should be made available to ITSEFs in order to re-use the results of this certificate.

EVALUATION RESULTS

The site Huawei Cyber Security Compliance Testing Center has been evaluated against the Security Target [SST].

All the assurance components required by the evaluation have been assigned a “PASS” verdict are resistant to attackers with a High attack potential. Consequently, the laboratory Applus Laboratories assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied, as defined by the Common Criteria v3.1 R5, the supporting document guidance CCDB-2007-11-001 Site Certification [SCER] and the JIWG supporting document Minimum site security requirements [MSSR].

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

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

- There are not recommendations by the evaluation team.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the site Huawei Cyber Security Compliance Testing Center, a positive resolution is proposed.

This Certification Report only applies to the site and its evaluated scope as indicated. The confirmed assurance components is only valid on the condition that all assumptions and preconditions required by the site, as given in this report and in the Site Security Target, are observed.

The owner of the certificate is obliged:

1. when advertising the Site Certificate or the fact of the Site Certification, to refer to the Site Certification Report as well as to provide the Site Certification Report and the Site Security Target and documentation mentioned herein to any client for the application and proper usage of the certified site,
2. to inform this Certification Body immediately about vulnerabilities of the site that have been identified by the sponsor or applicant or any third party after issuance of the certificate,
3. to inform this Certification Body immediately about security relevant changes in the scope of the evaluated site, e.g. changes related to the logical and physical development and production environment, to processes, and to services of the site.

In case of changes to the certified site, the validity can be extended to the changed site, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified site, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

Additionally, this Certification Body wants to remark the following:

- The scope of the activities in this site are Common Criteria ATE related activities for general software based ICT products. No specific Smart Card and Similar Devices nor Hardware Devices with Security Boxes defined life-cycle activities have been audited in this site, and therefore re-use of ALC activities for these specific SOGIS technical domains is not expected.

RE-USE OF THE SITE CERTIFICATE

The re-use of this Site Certificate is limited to the extent defined in the Spanish Certification Body (CCN) Technical Interpretation “IT-003 Instrucción técnica: reutilización de resultados mediante la certificación de centros de desarrollo” [IT003], the Supporting Document Guidance Site Certification [SCER] and the SOG-IS Smartcard and similar devices supporting documents, such as the Minimum site security requirements [MSSR].

The results from a site certification can be re-used for product certifications. For each specific TOE, accessory documents including specific TOE characteristics should be evaluated in addition to the

above specified documents. These evidences shall rely and shall be consistent with the evidences used in the site certificate evaluation and in the Site Security Target.

Currently the Recognition Agreements in place do not cover the recognition of Site Certificates. However, the evaluation process performed was outlined according to the rules of the agreements and by using the agreed supporting document on Site Certification [SCER] and [MSSR]. Therefore, the results of this evaluation and certification procedure can be re-used by the issuing scheme in a subsequent product evaluation and certification procedure.

When re-using the results of the activities that uphold this site certificate in a product evaluation, the scheme responsible for certifying the product may decide to fully recognize the results or contact this scheme to query about specific assurance activities carried out in the scope of this site certification.

SITE CERTIFICATE VALIDITY REVIEW

In this case, and according to arrangements in SOG-IS, to re-use the evaluation activities that uphold this Site Certificate in a product specific evaluation, a reassessment of the assurance activities validity should be done at most 18 months after the site audit date as virtual site audit procedure of [IT-013] and [JIL-COVID] policies has been applied and this site has not been previously certified by means of an on-site audit by this Certification Body. Therefore, a reassessment of the assurance activities validity should be done before 27/07/2022.

According to [JIL-COVID], despite from the 18 months mentioned, a “virtual audit” should be replaced by a regular on-site audit as soon as the restrictions of the pandemic situation and scheduling of the parties involved allows for.

SHARED TECHNICAL AUDIT REPORT (STAR)

The evaluation activities carried out in this site certification dossier has not been summarized in a Shared Technical Audit Report (STAR).

SITE SECURITY TARGET

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

- Site Security Target Huawei Cyber Security Compliance Testing Center, version 0.21. 28/02/2022.

The public version of this document constitutes the SST Lite. The SST Lite has also been reviewed for the needs of publication according to sanitation [SANT], and it is published along with this certification report in the Certification Body. The SST Lite identifier is:

- Site Security Target Lite Huawei Cyber Security Compliance Testing Center, version 0.5. 28/02/2022.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ITSEF	Information Technology Security Evaluation Facility
JIWG	Joint Interpretation Working Group of SOG-IS
OC	Organismo de Certificación
SOG-IS	Senior Officials Group Information Systems Security
SST	Site Security Target
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.

[IT-003] Instrucción técnica: reutilización de resultados mediante la certificación de centros de desarrollo. Versión 3. Date 07-11-2019.

[MSSR] Joint Interpretation Library. Minimum site security requirements. Version 3.0 Date February 2020.

[PP84] EUROSMART's protection profile "Security IC Platform Protection Profile with Augmentation packages. Version 1.0, 2014"

[SANT] Common Criteria Recognition Arrangement. ST sanitising for publication. Document number CCDB-2006-04-004. Date April, 2006.

[SCER] Common Criteria. Supporting Document Guidance. Site Certification. Document number CCDB-2007-11-001. Version 1.0, Revision 1, Date October, 2007.

[SST] Site Security Target Huawei Cyber Security Compliance Testing Center, version 0.21. 28/02/2022.