MINISTERIO DE PRESIDENCIA Y PARA LAS AATT
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN

REF: 2016-47-INF-2126 v1

Target: Público

Date: 20.10.2017

Created by: CERT11

Revised by: CALIDAD

Approved by: TECNICO

CERTIFICATION REPORT

File: 2016-47 Huawei WLAN AP Series Product V200R007C10SPC200

Applicant: 440301192W HUAWEI Technologies Co., Ltd.

References:

[EXT-3182] Certification request of Huawei WLAN AP Series Product V200R007C10SPC200

[EXT-3625] Evaluation Technical Report of Huawei WLAN AP Series Product V200R007C10SPC200.

The product documentation referenced in the above documents.

Certification report of the product Huawei WLAN AP Series Product V200R007C10SPC200, as requested in [EXT-3182] dated 07/11/2017, and evaluated by the laboratory Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-3625] received on 29/09/2017.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product “Huawei WLAN AP Series Product, version V200R007C10SPC200”.

The TOE, Huawei WLAN AP Series Product version V200R007C10SPC200, is a WLAN Access Point (AP for networking functionality) software that provides 802.11-compliant wireless access for STAs to connect wired networks to wireless networks.

The evaluation has been performed on the following platforms:

Series	Model
WLAN AP Series	AP2030DN
	AP4030DN
	AP4130DN
	AP5030DN
	AP5130DN
	AP6050DN
	AP6150DN
	AP7050DE
	AP8130DN
	AD9430DN-12
	AD9430DN-24

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 R4 EAL2.

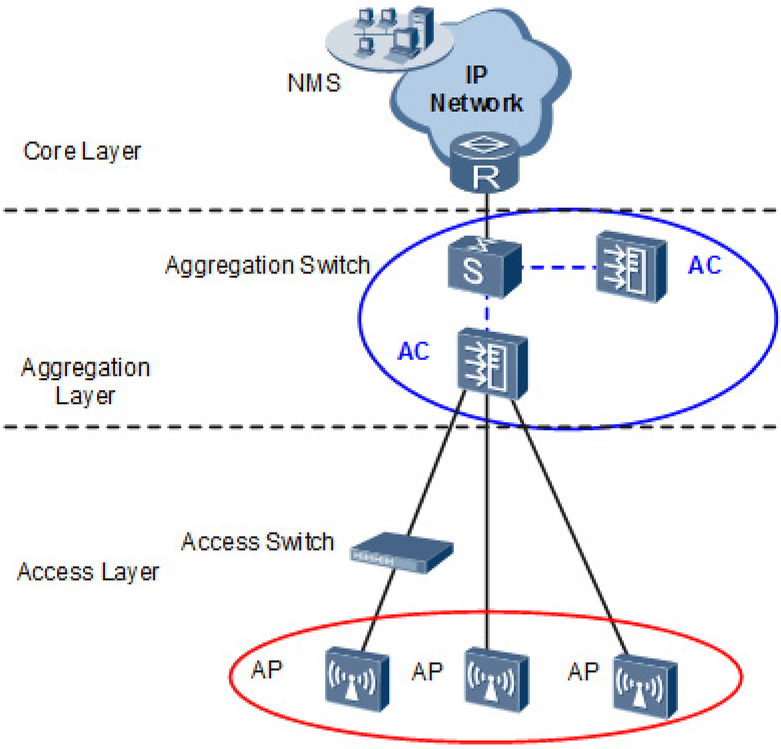
Evaluation end date: 25/09/2017.

All the assurance components required by the evaluation level of the [CC_P3] 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 EAL2 assurance level packages, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4. Considering the obtained evidences during the instruction of the certification request of the product “Huawei WLAN AP Series Product, version V200R007C10SPC200”, a positive resolution is proposed.

TOE summary

The TOE is a WLAN Access Point (AP for networking functionality) software that provides 802.11-compliant wireless access for STAs to connect wired networks to wireless networks.

The AP resides at the Access layer as depicted in the following figure of the overall network solution.



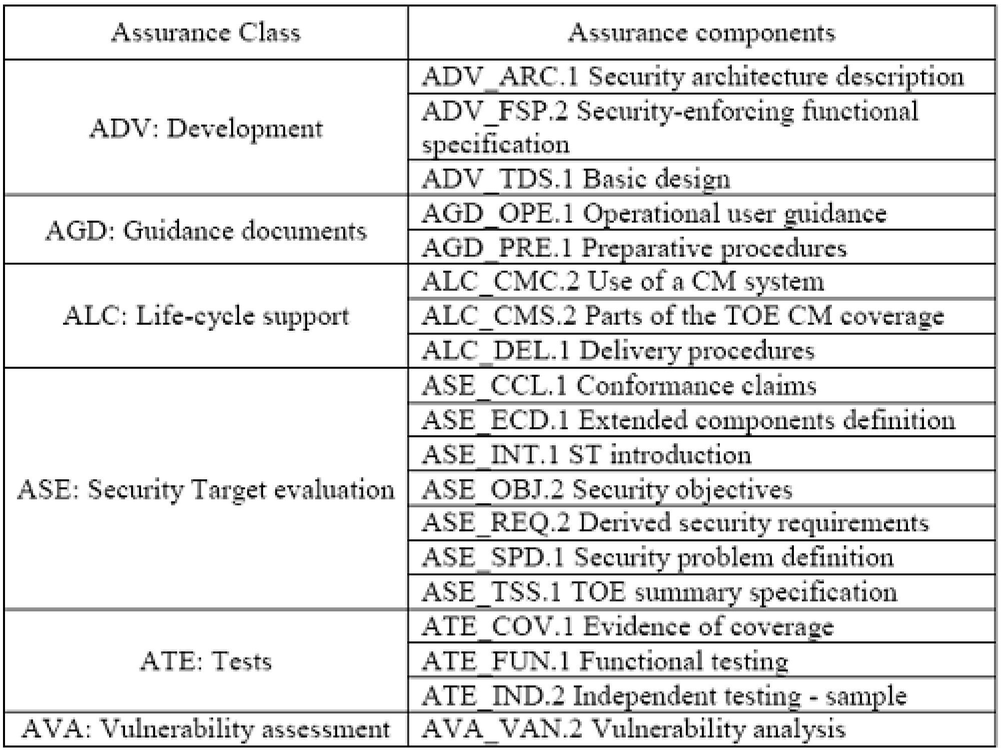
TOE major security features

The major security features implemented by the TOE and subject to evaluation can be summarised as follows:

- Authentication: Authenticate administrative users by user name and password and AC devices using a pre-shared key.
- Communication Security: Establishing a trusted path between itself and RMT and ACs is one of its features.
- ACL: Access Control Lists (ACLs) to filter traffic destined to the TOE.
- Security Management: Offers management functionality for its security functions.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidences required to fulfil the assurance packages of EAL2, according to Common Criteria v3.1 R4.



Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R4:

Class	Comp.
User Data Protection (FDP)	Subset information flow control (FDP_IFC.1)
	Simple security attributes (FDP_IFF.1)
Identification & Authentication (FIA)	Authorization Failure Handling (FIA_AFL.1)
	User attribute definition (FIA_ATD.1)
	User authentication before any action (FIA_UAU.2)
	User identification before any action (FIA_UID.2)
Security Management (FMT)	Management of security attributes (FMT_MSA.1)
	Static attribute initialisation (FMT_MSA.3)
	Specification of Management Functions (FMT_SMF.1)
	Security roles (FMT_SMR.1)
TOE Access (FTA)	TSF-initiated termination (FTA_SSL.3)

	TOE session establishment (FTA_TSE.1)
Trusted Path/Channels (FTP)	Trusted Path (FTP_TRP.1)

IDENTIFICATION

Product:: Huawei WLAN AP Series Product, version V200R007C10SPC200

Security Target: CC Huawei WLAN AP Series Product V200R007C10SPC200 Security Target, version 0.8, September 2017

Protection Profile: None

Evaluation Level: Common Criteria v3.1 R4: assurance packages EAL2

SECURITY POLICIES

There are no Organizational Security Policies defined for this evaluation.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions included in the [ST], are constraints to the conditions used to assure the security properties and functionalities compiled by the security target [ST]. 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.

Assumption Name	Assumption Definition
A.PhysicalProtection	It is assumed that the TOE (including any console attached, including any USB storage device attached) is protected against unauthorized physical access. The TOE is assumed not to contain any residual information that could be used for an attack when it is removed from the physically protected environment (e.g. for repair by a third party or at the end of life when the device is disposed).
A.NetworkElements	The environment is supposed to provide securely and correctly working network devices as resources that the TOE needs to cooperate with. Behaviors of such network devices provided by operational environment shall be also secure and correct. These devices are: • Peer device(s) for the exchange of dynamic routing information; • Remote entities (PCs) used for administration of the TOE; • WLAN ACs intended to manage the TOE.

A.NoEvil	The authorized administrators are not careless, willfully negligent or hostile. They will follow and abide the instructions provided by the TOE documentation

THREATS

The threats to the IT assets against which protection is required by the TOE or by the security environment included in the [ST] are listed below.

Threat Name	Threat Definition
T.UnauthenticatedAccess	A subject that is not an authenticated user of the TOE gains access to the TOE and modifies TOE configuration data without permission.
T.UnwantedNetworkTraffic	Any network user that sends unwanted/unexpected L3 network traffic to/through the TOE will reach resources on the network that it is not allowed to reach.
T. Eavesdroppping	An eavesdropper (remote attacker) in the management network served by the TOE is able to intercept, and potentially modify or re-use information assets which are not protected against modification and disclosure that are exchanged between TOE and RMT and ACs.

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 in the [ST] are categorized below.

Object Name	Object Definition
OE.NetworkElements	The operational environment shall provide securely and correctly working network devices as resources that the TOE needs to cooperate with. Behaviors of such network devices provided by operational environment shall be also secure and correct. The operational environment shall provide network devices that the TOE needs to cooperate with: • Peer device(s) for the exchange of dynamic routing information;

	• AC for the management of AP devices; • Remote entities (PCs) used for administration of the TOE.
OE.Physical	The TOE (i.e., the complete system including attached peripherals, such as a console and USB mass storage devices) shall be protected against unauthorized physical access. Whenever the TOE is removed from the physically protected environment, it shall not contain any residual information that could be used for an attack.
OE.Person	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE. This includes instruction to follow and abide the instructions provided by the TOE documentation.

ARCHITECTURE

LOGICAL ARCHITECTURE

Logical boundaries

Conceptually the TOE can be thought of as a collection of the following security services which the security target describes with increasing detail:

Authentication

User authentication is always enforced for virtual terminal sessions via SSH, and SFTP (Secured FTP) sessions. The use of SSH connection is always required for accessing the TOE via RMT. Also, it authenticates AC devices in the network using pre-shared keys.

Communication Security

The TOE enforces communication security by implementing the SSH2 (SSH2.0) protocol for RMT. The trusted path provides data encryption, data integrity and authentication of both sides to protect the TOE from eavesdropping and to ensure data transmission security and confidentiality. Beside SSH (which is sometimes also referred to as ‘Secure Telnet’ or ‘STelnet’) SFTP is provided implementing secure FTP based on SSH as communication protocol. Also, DTLS v1.0 encryption provides a secure communication between the WLAN ACs deployed in the network and the TOE.

ACL

TOE internetworking devices are deployed at the edges of untrusted networks (such as the Internet), in order to provide controlled communications between two networks that are physically separated. When a packet flow reaches the TOE, the TOE applies an information flow security policy in the form of access control lists to the traffic before forwarding it into the remote network. Packet flows on Layer 3 arriving at a network interface of the TOE are checked to ensure that they conform the configured packet filter policy. For this, the TOE offers a feature Access Control List (ACL) for filtering incoming and outgoing information flow to and from interfaces.
Users with sufficient access rights can create, delete, and modify rules for ACL configuration to filter, prioritize, rate-limit the information flow destined to TOE or other network devices through interfaces by matching information contained in the headers of connection-oriented or connectionless packets against ACL rules specified. Ethernet protocol type, Source IP address, destination IP address, IP protocol number, source port number if TCP/UDP protocol, destination port number if TCP/UDP protocol, TCP flag if TCP protocol, etc., can be used for ACL rule configuration. Packet flows matching a deny rule in the ACL are dropped. If no rule is specified for an incoming packet, it is forwarded by default.

Security functionality management

According to security functionality management, customized security is provided. The TSF shall be capable of performing the following management functions:

1. Authentication, encryption policy
2. ACL policy.

PHYSICAL ARCHITECTURE

Physical boundaries

The TOE does not include any hardware or network infrastructure components between the computers that comprise the distributed TOE.

The TOE is delivered as software binaries that are downloaded from Huawei website at http://e.huawei.com/uk/. The binaries are different depending on the evaluated platform where they are installed.

Name	FW and Version
AP4030DN	FitAP4X30XN_V200R007C10SPC200.bin
AP4130DN	FitAP4X30XN_V200R007C10SPC200.bin
AP2030DN	FitAP2X30XN_V200R007C10SPC200.bin
AD9430DN-12	FitAD9430DN-12_V200R007C10SPC200.bin
AD9430DN-24	FitAD9430DN-24_V200R007C10SPC200.bin

AP5030DN	FitAP5X30XN_V200R007C10SPC200.bin
AP5130DN	FitAP5X30XN_V200R007C10SPC200.bin
AP8130DN	FitAP8X30XN_V200R007C10SPC200.bin
AP6050DN	FitAP6050DN_V200R007C10SPC200.bin
AP6150DN	FitAP6150DN_V200R007C10SPC200.bin
AP7050DE	FitAP7050DE_V200R007C10SPC200.bin

DOCUMENTS

The product includes the following document that shall be distributed and made available together to the users of the evaluated version. These documents can be found in PDF format the CD provided in the product package upon delivery.

CC Huawei WLAN AP Series Product V200R007C10SPC200 Security Target	Version: 0.8
CC Huawei WLAN AP Series Product V200R007C10SPC200 Operational User Guidance	Version: 0.6
CC Huawei WLAN AP Series Product V200R007C10SPC200 Preparative Procedures for Production	Version: 0.5

Additional guides (Product Documentation and Command Reference) are downloaded from the website http://support.huawei.com/enterprise/en/newindex.html by clicking on WLAN in Enterprise Networking in CHM format.

AC6605&AC6005&ACU2 (AC&FITAP) V200R007C10 Product Documentation	Product version 0.6
Huawei Access Points (FIT AP) V200R007C10 Command Reference	Issue 05

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 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 security target [ST].

PENETRATION TESTING

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 does NOT present exploitable vulnerabilities under the environment defined in the security target [ST]. All identified vulnerabilities can be considered closed if the TOE is installed and operated according to the security target [ST] and related documentation. The overall test result is that no deviations were found between the expected and the actual test results taking into account that environment. No attack scenario with the attack potential “Basic” has been successful in the TOE’s operational environment as defined in the security target [ST] when all measures required by the developer are applied.

EVALUATED CONFIGURATION

The TOE under evaluation is “Huawei WLAN AP Series Product, version V200R007C10SPC200”.

The TOE has been tested on the following physical platforms:

Series	Model
WLAN AP Series	AP2030DN
	AP4030DN
	AP4130DN
	AP5030DN
	AP5130DN
	AP6050DN
	AP6150DN
	AP7050DE
	AP8130DN
	AD9430DN-12
	AD9430DN-24

EVALUATION RESULTS

The product “Huawei WLAN AP Series Product, version V200R007C10SPC200” has been evaluated against the “CC Huawei WLAN AP Series Product V200R007C10SPC200 Security Target, version 0.8, September 2017”.

All the assurance components required by the evaluation level EAL2 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 EAL2, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

The TOE usage is recommended given that there are not exploitable vulnerabilities in the operational environment. The following usage recommendation is given:

- 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.

CERTIFIER RECOMMENDATIONS

Considering the evidences obtained during the instruction of the certification request of the product “Huawei WLAN AP Series Product, version V200R007C10SPC200”, a positive resolution is proposed.

The certifier strongly recommends to the TOE consumer to strictly follow the security recommendations that can be found on guidance documents referenced in section DOCUMENTS of this certification report, as well as to observe the operational environment requirements and assumptions defined in the applicable security target.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación

SFR Security Functional Requirement

TOE Target Of Evaluation

TSF TOE Security Functionality

TSFI TSF Interface

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, R4 Final, Sept. 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, Sept. 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, Sept. 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, Sept. 2012.

[ST] CC Huawei WLAN AP Series Product V200R007C10SPC200 Security Target, version 0.8, September 2017

SECURITY TARGET

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

- CC Huawei WLAN AP Series Product V200R007C10SPC200 Security Target, version 0.8, September 2017