TrustCB B.V.

Version 2023-06

Certification Report

Huawei Yunshan software V600R023C00 running on AirEngine 9700 Series Access Controllers

Sponsor and developer:	***Huawei Technologies, Co., Ltd.*** **Administration Building, Headquarters of Huawei Technologies Co., Ltd.** **Bantian, Longgang District, Shenzhen, 518129** **P.R.C**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2300064-01-CR**
Report version:	**1**
Project number:	**NSCIB-2300064-01**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**26 April 2024**
Number of pages:	**11**
Number of appendices:	**0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Huawei Yunshan software V600R023C00 running on AirEngine 9700 Series Access Controllers. The developer of the Huawei Yunshan software V600R023C00 running on AirEngine 9700 Series Access Controllers is Huawei Technologies, Co., Ltd. located in Shenzhen, P.R.C and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a new- generation wireless access controller (AC), Works with Huawei's wireless access points to build campus networks, enterprise office networks, wireless MAN networks, and hotspot coverage environments.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 26 April 2024 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Huawei Yunshan software V600R023C00 running on AirEngine 9700 Series Access Controllers, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Huawei Yunshan software V600R023C00 running on AirEngine 9700 Series Access Controllers are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Flaw reporting procedures).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Huawei Yunshan software V600R023C00 running on AirEngine 9700 Series Access Controllers from Huawei Technologies, Co., Ltd. located in Shenzhen, P.R.C.

The TOE is comprised of the following main components:

Delivery item type	**Identifier**	**Version**
Software	AirEngine9700-H_V600R023C00.cc	V600R023C00
	AirEngine9701-L-T_V600R023C00.cc	V600R023C00

As the TOE is software only, it must be run on a non-TOE hardware platform. The hardware corresponding to the Huawei Access controllers are:

- AirEngine 9700-H for AirEngine9700-H_V600R023C00.cc
- AirEngine 9701-L-T for AirEngine9701-L-T_V600R023C00.cc.

To ensure secure usage a set of guidance documents is provided, together with the Huawei Yunshan software V600R023C00 running on AirEngine 9700 Series Access Controllers. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

TOE provides the following functionality:

- The TOE supports username/password, or public-key authentication mode and only users that are authenticated can access the TOE and its command line interface.
- The TOE is accessed by CLI locally or a Network Management Server (NMS) remotely over SSH so that a secure channel is established to protect the data between TOE and NMS. This channel is used for TOE management by administrators.
- For secure transmission of audit information between the TOE and the Syslog server a secure TLS channel is used.
- The TOE supports digital signature verification for software. Each of the software package or patch package released by Huawei includes a unique digital signature. When an NMS distributes the package to TOE, the TOE will verify the online digital signature before updating. The verification of the digital signature demonstrates the integrity and authenticity of the package. The package is only processed further after successful verification of the digital signature, otherwise the package will be discarded without processing. Software integrity is verified for software update packages and for installed firmware upon every boot.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

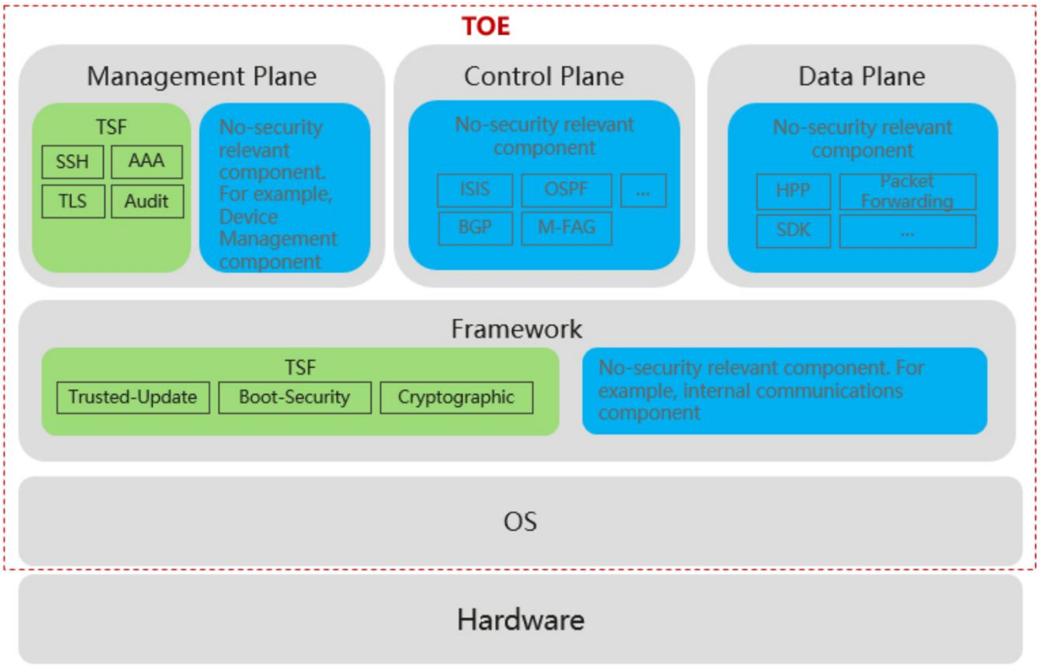
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The logical architecture of the TOE can be depicted as follows:


TOE
Management Plane
TSF
SSH
AAA
TLS
Audit
No-security relevant component. For example, Device Management component
Control Plane
No-security relevant component
ISIS
OSPF
...
BGP
M-FAG
Data Plane
No-security relevant component
HPP
Packet Forwarding
SDK
...
Framework
TSF
Trusted-Update
Boot-Security
Cryptographic
No-security relevant component. For example, internal communications component
OS
Hardware

The TOE is the software running on the AirEngine 9700 series access controllers as described in section 2.1. These access controllers consist of both hardware (non-TOE) and software (TOE). The software running on the access controllers is denominated Yunshan software developed by Huawei.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
AGD_PRE Huawei YunShan Software V600R023C00 running on AirEngine 9700 Series Access Controllers Preparative Procedures, dated 01 January 2024	v1.4
AGD_OPE Huawei YunShan Software V600R023C00 running on AirEngine 9700 Series Access Controllers Operational User Guidance, dated 27 January 2024	v1.4
WLAN V600R023C00 Product Documentation, dated 30 June 2023	01
WLAN V600R023C00 Upgrade Guide, dated 30 June 2023	01

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer’s testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer performed extensive testing on functional specification, subsystem and module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

The evaluator created additional test cases test to confirm verification of the version of the TOE / to supplement coverage of SFRs and/or TSFI / to further exercise the behaviour of critical functionality.

2.6.2 Independent penetration testing

To identify potential vulnerabilities the evaluator performed the following activities:

- SFR design analysis: Based on the information obtained in the evaluation evidence, the SFR implementation details were examined. The aspects described in CEM annex B were considered. During this examination several potential vulnerabilities were identified.
- Additional security analysis: When the implementation of the SFR was understood, a coverage check were performed on the relevant aspects of all SFRs. This expanded the list of potential vulnerabilities.
- Scanning the TOE using the applicable vulnerability scanning tools (e.g., NMAP, NESSUS) to collect information about the TOE and identify potential vulnerabilities.
- Public vulnerability search: The evaluator performed public domain vulnerability search based on the TOE name, TOE type, and identified 3rd party security relevant libraries and/or services. Several additional potential vulnerabilities were identified during a search in the public domain.
- The potential vulnerabilities identified were analyzed, and some of the potential vulnerabilities were concluded not exploitable within in the Enhanced-Basic attack potential, or covered by guidance. For remaining potential vulnerabilities, penetration tests were devised.

The total test effort expended by the evaluators was 6 weeks. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The following configurations was used for testing:

- Huawei AirEngine 9700 Series running the TOE with version V600R023C00 (hardware: AirEngine 9700-H)
- A special TOE build to enable direct access to the crypto library to test the FCS class tests

The developer provided an argument that the difference in the non-TOE hardware is not security relevant, and the code review performed by the evaluator showed that the security relevant code for different software packages are identical. The difference in the software packages are due to different drivers for the different hardware. Consequently, the evaluator concluded the difference in hardware and software does not impact the claimed security. To verify this conclusion, the evaluator decided to perform all the testing on AirEngine 9701-L-H onsite, with a sample of test cases to be perform on the AirEngine 9700-H remotely to ensure the difference indeed does not result in different security behaviour.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer’s tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 4 Site Audit reports. These were the Data Centres from NSCIB-CC-0629826, NSCIB-CC-0461863, NSCIB-CC-0611979 and NSCIB-SS-2300146.

Evaluated Configuration

The TOE is defined uniquely by its name and version number Huawei Yunshan software V600R023C00 running on AirEngine 9700 Series Access Controllers.

2.8 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and a Site Technical Audit Report for the site *[STAR]* [2].

The verdict of each claimed assurance requirement is “**Pass**”.

Based on the above evaluation results the evaluation lab concluded the Huawei Yunshan software V600R023C00 running on AirEngine 9700 Series Access Controllers, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_FLR.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.9 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” contains necessary information about the usage of the TOE. Certain aspects of the TOE’s security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: <none>

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

3 Security Target

The Huawei YunShan software V600R023C00 running on AirEngine 9700 Series Access Controllers Security Target, Version 1.8, Dated 27 January 2024 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
LAN	Local Area Network
NMS	Network Management Server
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[ETR]	Evaluation Technical Report “Huawei Yunshan software V600R023C00 running on AirEngine 9700 Series Access Controllers” – EAL4+, 23-RPT-1042, Version 5.0, Dated 19 April 2024
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	Huawei YunShan software V600R023C00 running on AirEngine 9700 Series Access Controllers Security Target, Version 1.8, Dated 27 January 2024
[STAR]	STAR Huawei Suzhou R&D Center A1 v1.0, 24-RPT-119, Version 1.0, Dated 12 February 2024

(This is the end of this report.)