

Certification Report

VOS AutoSAR OS V3.0.0

Sponsor and developer: ***Huawei Technologies Co., Ltd.***
**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
China**

Evaluation facility: ***SGS Brightsight B.V.***
**Brassersplein 2
2612 CT Delft
The Netherlands**

Report number: **NSCIB-CC-2300032-01-CR**

Report version: **1**

Project number: **NSCIB-2300032-01**

Author(s): **Jordi Mujal**

Date: **30 June 2023**

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	3
Recognition of the Certificate	4
International recognition	4
European recognition	4
1 Executive Summary	5
2 Certification Results	6
2.1 Identification of Target of Evaluation	6
2.2 Security Policy	6
2.3 Assumptions and Clarification of Scope	6
2.3.1 Assumptions	6
2.3.2 Clarification of scope	6
2.4 Architectural Information	6
2.5 Documentation	7
2.6 IT Product Testing	7
2.6.1 Testing approach and depth	7
2.6.2 Independent penetration testing	8
2.6.3 Test configuration	8
2.6.4 Test results	8
2.7 Reused Evaluation Results	8
2.8 Evaluated Configuration	8
2.9 Evaluation Results	8
2.10 Comments/Recommendations	9
3 Security Target	10
4 Definitions	10
5 Bibliography	11

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 VOS AutoSAR OS V3.0.0. The developer of the VOS AutoSAR OS V3.0.0 is Huawei Technologies Co., Ltd. located in Dongguan, China 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 the kernel of the Huawei intelligent vehicle control operating system. As the operating system kernel software for vehicle control, the TOE can be used in various Electronic Control Unit (ECU) products of a vehicle. The TOE provides a software platform for application developers to develop applications that control the ECU.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 30 June 2023 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 VOS AutoSAR OS V3.0.0, 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 VOS AutoSAR OS V3.0.0 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.1 (Basic Flaw Remediation) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

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 VOS AutoSAR OS V3.0.0 from Huawei Technologies Co., Ltd. located in Dongguan, China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	VOS AutoSAR-OS	V3.0.0
	VOS AutoSAR-OS (signature file)	V3.0.0

To ensure secure usage a set of guidance documents is provided, together with the VOS AutoSAR OS V3.0.0. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The following security mechanisms are supported and included within the TSF:

- Permission based access control to OS objects
- Memory access control for OS applications isolation.
- Stack monitoring.
- Error and exception handling to secure state

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].

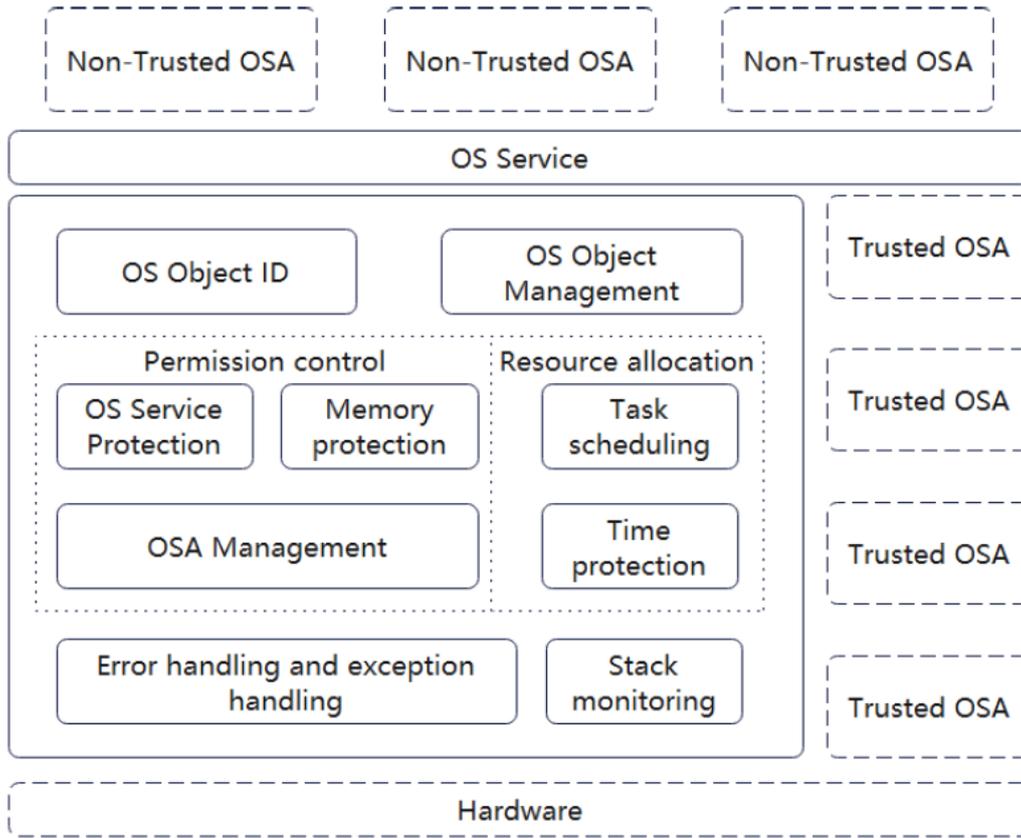
2.3.2 Clarification of scope

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

Note that the [ST] has the OE.PLATFORM which claims the environment for the TOE protects against physical invasive attacks, environmental stress malfunction attacks and side channel analysis attacks. Therefore, these types of threats are not considered in the scope of the TOE evaluation and need to be considered for developing a product solution that integrates the TOE into a larger system including a hardware platform.

2.4 Architectural Information

The TOE architecture and part of its environment (Hardware and OS applications), as it is represented in the [ST] can be depicted as follows:



2.5 Documentation

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

Identifier	Version	Date
HUAWEI VOS 3.0.0 Os 参考手册	Rev. 01	2023-04-15
VOS AutoSAR-OS V3.0.0 Preparation Procedure	Rev.1.9	2023-04-17
VOS AutoSAR-OS 3.0.0 Operation User Guide	Rev.1.4	2023-03-04

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.

The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

The independent vulnerability analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considered whether potential vulnerabilities could already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review was performed on the TOE. During this attack-oriented analysis the protection of the TOE was analysed using the knowledge gained from all evaluation classes. This resulted in the identification of (additional) potential vulnerabilities.
- All potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities were addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The total test effort expended by the evaluators was 2 weeks. During that test campaign, 100% of the total time was spent on logical tests. No attacks including exploitation of test features, physical invasive attacks, side channel analysis or fault injection were defined as the TOE is not claimed to be resistant against these types of attacks.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the [ST].

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.

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 2 site certificates and 3 Site Technical Audit Reports.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number VOS AutoSAR OS V3.0.0.

2.9 Evaluation Results

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

The verdict of each claimed assurance requirement is "Pass".

Based on the above evaluation results the evaluation lab concluded the VOS AutoSAR OS V3.0.0, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_FLR.1 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target [ST].

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.

2.10 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.

3 Security Target

The VOS AutoSAR-OS V3.0.0 Security Target, version 1.5, 30 June 2023. [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:

ECU	Electronic Control Unit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
OS	Operating System
OSA	Operating System Application
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 VOS AutoSAR - OS V3.0.0 – EAL4+, 23-RPT-068, version 7.0, 30 June 2023 |
| [NSCIB] | Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022 |
| [ST] | VOS AutoSAR-OS V3.0.0 Security Target, version 1.5, 30 June 2023. |
| [STAR] | Site Technical Audit Report - Huawei Shanghai Jingci 4-1-58R Development Site, 22-RPT-1176, version 3.0, 12 June 2023 |

(This is the end of this report.)