

Certification Report

Huawei BaseBIOS 2.0

Sponsor and developer: **Huawei Technologies Co.,Ltd.**
No. 6 Xincheng Avenue, Songshan Lake Technology
Industrial Park
Dongguan City, 523808
P.R.C.

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

Report number: **NSCIB-CC-0570590-CR**
Report version: **1**
Project number: **0570590**
Author(s): **Kjartan Jæger Kvassnes**
Date: **24 January 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	7
2.5 Documentation	7
2.6 IT Product Testing	7
2.6.1 Testing approach and depth	7
2.6.2 Independent penetration testing	7
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	8
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, TÜV Rheinland Nederland 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 TÜV Rheinland Nederland 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 TÜV Rheinland Nederland 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, TÜV Rheinland Nederland 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

The 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 BaseBIOS 2.0. The developer of the Huawei BaseBIOS 2.0 is Huawei Technologies Co.,Ltd. located in Dongguan City, 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 BaseBIOS which is a secure bootloader, it is the second piece of software codes that is used in the start-up process of a secure embedded hardware product, such as an integrated secure element or SoC, to ensure the product securely initializes into a secure state. The TOE is critically dependent on the environment providing security protections, as detailed in section 2.3.1 “Assumptions”.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 18 January 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 Huawei BaseBIOS 2.0, 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 Huawei BaseBIOS 2.0 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 EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) 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).

TÜV Rheinland Nederland 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 BaseBIOS 2.0 from Huawei Technologies Co.,Ltd. located in Dongguan City, P.R.C..

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	Huawei BaseBIOS 2.0	B006

To ensure secure usage a set of guidance documents is provided, together with the Huawei BaseBIOS 2.0. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE provides the following security features:

Software image signature decoding

- Automated recovery attempt
- Boot failure handling
- Sensitive data handling
- Anti-rollback version checking
- Debug functionality (for software development)

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

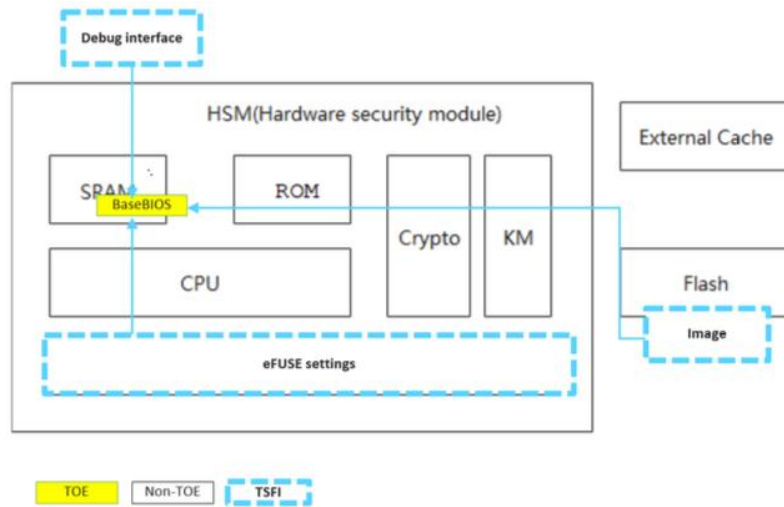
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the [ST].

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, originating from the [ST] can be depicted as follows:



The TOE is located in HSM, which is based on the resource of HSM, and ensure the higher layers of software are securely loaded. The TOE is only a piece of secure bootloader code and stored in SRAM of HSM.

2.5 Documentation

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

Identifier	Version
Huawei BaseBIOS 2.0 Guidance Document, dated 09 August 2022	V1.4

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.

The evaluator witnessed on-premise a repetition of a selection of the developer tests, additionally a small number of test cases designed by the evaluator was performed.

2.6.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can 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 is performed on the TOE. During this attack oriented analysis, the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this analysis will be performed according to the attack methods in [JIL-AM].

- All potential vulnerabilities are 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 are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

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

2.6.3 Test configuration

The evaluator-defined tests were performed on the test chip. The test board environment consists of the test chip, flash, and power supply. The TOE runs on the test chip and the flash stores the AP Bios image as well as IMU Firmware images. There are two UARTs in this test board UART1 and UART2. (UART1 and UART2). The UART1 is used to load the eXtensibleBIOS image, and UART2 is used to load the IMU Firmware image.

All test cases were performed on the TOE secure boot mode.

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 3 Site Technical Audit Reports.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Huawei BaseBIOS 2.0.

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.

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

Based on the above evaluation results the evaluation lab concluded the Huawei BaseBIOS 2.0, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target [ST].

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>, which are out of scope as there are no security claims relating to these.

Not all key sizes specified in the [ST] have sufficient cryptographic strength to satisfy the AVA_VAN.5 "high attack potential". To be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The Huawei BaseBIOS 2.0 Security Target, Version 1.5, 08 September 2022 [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:

HSM	Hardware Security Module
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
SRAM	Static Random Access Memory
TOE	Target of Evaluation
UART	Universal Asynchronous Receiver-Transmitter

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 BaseBIOS 2.0 – EAL5+, 22-RPT-955, Version 2.0, 11 January 2023.
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	Huawei BaseBIOS 2.0 Security Target, Version 1.5, 08 September 2022

(This is the end of this report.)