Certification Report

Huawei BSBC 2.0

Sponsor and developer:	***Huawei Technologies Co., Ltd.*** **2F D4 D Area Administration Building, Southern Factory of HuaweiTechnologies Co., Ltd., No. 6 Xincheng Avenue Songshan Lake Technology Industrial Park, Dongguan City P.R.C.**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0448219-CR**
Report version:	**1**
Project number:	**0448219**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**25 February 2022**
Number of pages:	**11**
Number of appendices:	**0**

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

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

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, 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 BSBC 2.0 The developer of the Huawei BSBC 2.0 is Huawei Technologies Co., Ltd. located in Dongguan, 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 secure bootloader, it is the first piece of software code 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 12 February 2022 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 BSBC 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 BSBC 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 BSBC 2.0 from Huawei Technologies Co., Ltd. located in Dongguan, P.R.C..

The TOE is comprised of the following main components:

Delivery item type	**Identifier**	**Version**
Software	Huawei BSBC 2.0	B003

The TOE version Huawei BSBC 2.0 version B003 is the internal name corresponding to BSBC version 2.0 for external use, hence the certified TOE is same configuration as stated in the [ST].

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

2.2 Security Policy

The TOE is used by integrating it into a software stack running on a compatible hardware platform. As part of the initialization procedure of this hardware and software stack, the TOE will be used to ensure that the higher layers of software are securely loaded.

In order to support this, the TOE provides the following security features:

- Boot failure handling
- Sensitive data handling
- 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]*.

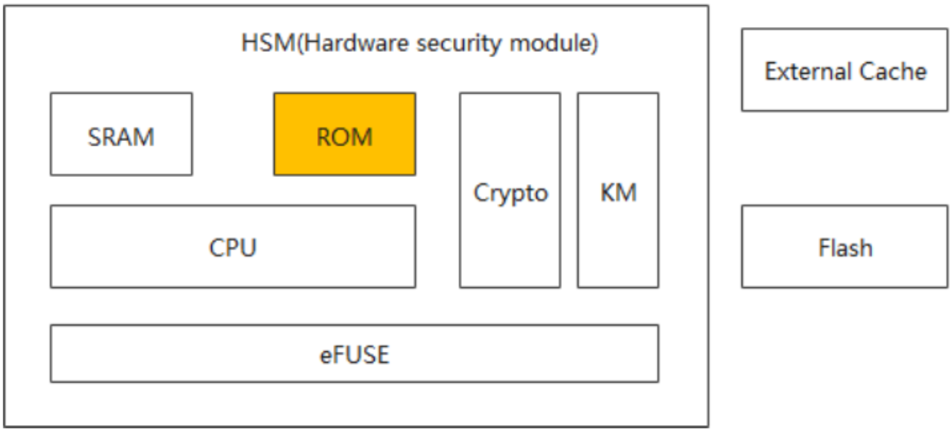
2.3.2 Clarification of scope

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 TOE is a BSBC which is a secure bootloader, it is the first piece of software code that is used in the start-up process of an IT security product a secure embedded hardware product, such as an integrated secure element or SoC, to ensure the product securely initializes into a secure state.

The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows:



The TOE as indicated by the orange colour is located in HSM (hardware security module), 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 the ROM of HSM. The TOE also relies on two components (External Cache and Crypto) which are not part of the HSM, but they are still part of the same hardware that comprises the operational environment of the TOE. Figure 1 shows the TOE in its operational environment. The following summarises the role of the various components:

- External Cache and SRAM are used by the TOE as volatile memory.
- KM and Crypto are used for image decryption and image authentication (signature verification).
- eFUSE is used as one-time programmable memory.
- CPU executing the TOE.
- Flash are used to store the image.

The TOE is intended to run specifically on the Huawei HSM product range.

2.5 Documentation

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

Identifier	Version
Huawei BSBC 2.0 Guidance Document, date 25 October 2021	V1.1

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

The evaluators have 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 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 was performed on the TOE. During this attack oriented analysis the protection of the TOE was analysed using the knowledge gained from all previous evaluation classes. This resulted in the identification of (additional) potential vulnerabilities. This analysis was performed according to the attack methods in [JIL-AM].
- 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 the potential vulnerabilities are not exploitable.

The total test effort expended by the evaluators was 1 week. During that test campaign, 100% of the total time was spent on logical tests. This corresponds to the total duration of the single logical software attack test, no attacks including exploitation of test features were defined. No perturbation and side-channel attacks were defined as the TOE does not claim to be resistant against these types of attacks.

2.6.3 Test configuration

The developer tested the TOE in the following configuration

- TOE version “BSBC B003” corresponds to the final TOE version. “BSBC B003” is the internal name corresponding to BSBC 2.0 for external use; hence the same configuration as stated in the [ST] was applied.

The evaluator-defined test is performed on a test chip, which is part of the Huawei HSM product range. The test chip used is a high-performance multi-core processor designed for the communications field. Its frequency is up to 2GHz and it integrates two 72-bit DDR4/5 interfaces, provides a speed of 3200/3600 MT/s, and integrates multiple acceleration engines. 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 next stage bootloader software as well as other software to be used in case of failure occurs for test robustness. There are two UARTs in this test board UART1 and UART2.

The following test tools were used:

- MobaXterm v20.2
- VSCode-huaweiv1.43.2
- gcc7.5.0
- gcov7.5.0.

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.

For composite evaluations, please consult the *[ETRfC]* for details.

2.7 Reused Evaluation Results

There has been reuse of the ALC aspects for one of the sites involved in the development and production of the TOE, by use of the results of one site audit as reported in NSCIB-CC-0209053-CR *[CR_0209053]*.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Huawei BSBC 2.0 version B003.

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 sites *[STAR Hangzhou]*, *[STAR Suzhou]* and *[STAR Dongguan]* [2]. To support composite evaluations according to *[COMP]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that must be considered when this TOE is used as platform in a composite evaluation.

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

Based on the above evaluation results the evaluation lab concluded the **Huawei BSBC 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 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

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).

[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 BSBC 2.0 Security Target v1.1, 26 October 2021 *[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:

BSBC	Boot-rom Secure Boot Code
IT	Information Technology
ITSEF	IT Security Evaluation Facility
HSM	Hardware Security Module
JIL	Joint Interpretation Library
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

[COMP] Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018

[CR_0209053] Certification Report Huawei BSBC V1.5, NSCIB-CC-0209053-CR, version 1.0, 30 October 2020

[ETR] Evaluation Technical Report BSBC 2.0 – EAL5+, 21-RPT-1092, Version 4.0, 04 February 2022

[ETRfC] Evaluation Technical Report for Composition BSBC 2.0 EAL5+, 21-RPT-1235, v2.0, 03 January 2022

[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 BSBC 2.0 Security Target v1.1, 26 October 2021

[STAR Dongguan] Site Technical Audit Report Huawei BSBC 2.0, STAR Huawei Dongguan Data Center site, 21-RPT-1058, Version 2.0, 03 January 2022

[STAR Hangzhou] Site Technical Audit Report Huawei BSBC 2.0, STAR Huawei Hangzhou site, 21-RPT-828, Version 2.0, 03 January 2022

[STAR Suzhou] Site Technical Audit Report Huawei BSBC 2.0, STAR Huawei Suzhou Data Centre, 21-RPT-1057, Version 2.0, 03 January 2022

(This is the end of this report.)