Certification Report

Huawei HSM 2.0 Management Firmware version B006

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, P.R.C

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

Report number:	**NSCIB-CC-2200028-01-CR**
Report version:	**1**
Project number:	NSCIB-**2200028-01**
Author(s):	**Wim Ton**
Date:	**18 November 2023**
Number of pages:	**11**
Number of appendices:	**0**

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.

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 HSM 2.0 Management Firmware version B006. The developer of the Huawei HSM 2.0 Management Firmware version B006 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 the run-time firmware for the HSM functionality that will be integrated in a SoC. This certificate concerns only the management functions for said HSM, such as access control, remote attestation, secure update, and key management. The actual cryptographic operations are out of scope as these are provided by the underlying hardware.

Although the smartcard rating methodology was most applicable and thus used for this certification, the TOE type does not include the hardware in the scope and thus does not fall under the technical domain of smartcards and similar devices.

The main consumers of this TOE will be Huawei SoC developers.

This TOE is critically dependent on the operational environment to provide countermeasures against specific attacks as described in chapter 2 of the *[UG]* and chapter 3.4 of the *[ST].* As such it is vital that meticulous adherence to the user guidance of both the software and the hardware part of the TOE is maintained.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 2023-11-18 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 HSM 2.0 Management Firmware version B006, 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 HSM 2.0 Management Firmware version B006 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_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).

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 HSM 2.0 Management Firmware version B006 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 HSM 2.0 Management Firmware	B006

To ensure secure usage a set of guidance documents is provided, together with the Huawei HSM 2.0 Management Firmware version B006. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.3.3.

2.2 Security Policy

- Digest/message **encoding/decoding** and **access control** to cryptographic services.
- Key management.
- Dynamic measurement of the external memory contents
- Provide the device identity information stored in the hardware environment to the requesting user
- Secure update of the second-stage bootloader image or the TOE image.
- Communication with the user for securely accessing the HSM service and access control based on role-based authentication.
- Remote attestation service.
- Audit of security-relevant actions.

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 3.4 of the *[ST]*.

2.3.2 Clarification of scope

It is assumed that the SoC which the TOE is integrated into is used on network devices such as firewalls and routers for which the working environment is a physically secure environment, i.e., no unauthorized person has physical access to the device.

It is assumed that the TOE is integrated with secure boot firmware into a CC EAL4+ ALC_DVS.2 and AVA_VAN.5 certified hardware SoC. The hardware shall protect the TOE against:

- Physical attacks, such as probing or physical manipulation.
- Malfunction attacks, where environmental stress is applied to cause a malfunction.
- Side-channel attacks, where sensitive information leaks as a result of leakage.

It is assumed that the HSM-agent, TEE OS, and AP BIOS outside of the TOE are trusted.

2.4 Architectural Information

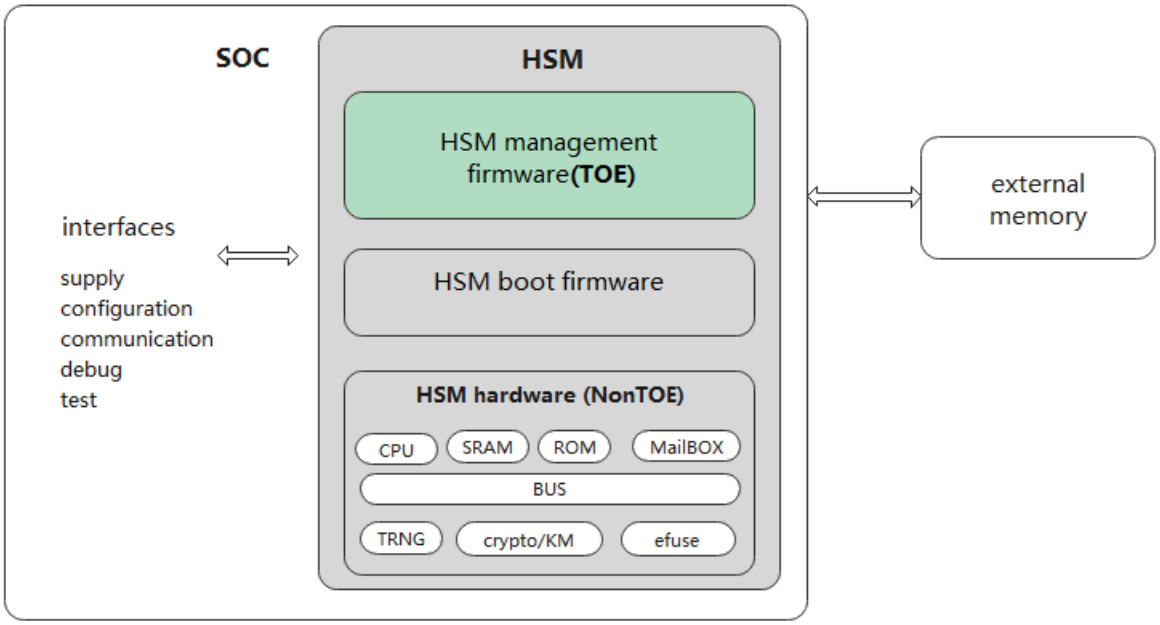

Figure 1 The TOE in its environment

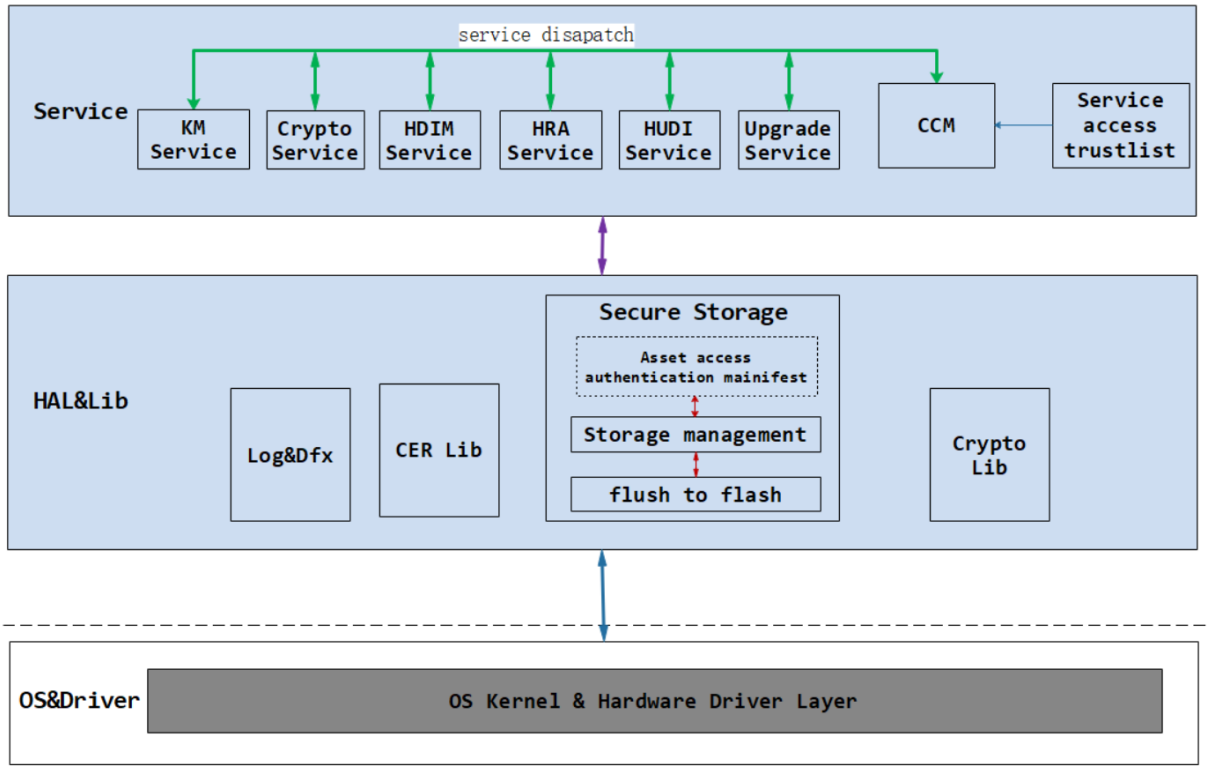

Figure 2 TOE architecture

The Communication Core Module (CCM) communicates securely with the TEE in the integrated product.

The Huawei Unique Device Identity (HUDI) Service provides the unique composite cryptographic identity of chips, boards, and devices.

The Huawei Dynamic Integrity Measurement (HDIM) service measures and compares software at different levels based on the hardware trust root provided by the hardware security module (HSM) to ensure that the code running in the memory is not tampered with.

The Huawei Remote Attestation (HRA) Service sends the device's status information (such as boot and runtime measurements) signed by the device's remote reporting trusted root securely to the customer's remote management server. Users can verify the validity of the uploaded device status information and check if the firmware and/or hardware of the device is tampered with or replaced.

Log&Dfx collects logs and device health status information.

The "crypto services" are out of scope for this certification.

2.5 Documentation

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

Identifier	Version
Huawei HSM 2.0 Management Firmware Guidance Document	1.7
Huawei HSM 2.0 Management firmware service command specification	1.6

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 uses 2 test approaches: "unit tests" and "high level" tests. The unit tests reach 100% code coverage and close to 100% function coverage.

The high-level tests are executed on an FPGA based emulation of the target platform.

2.6.2 Independent penetration testing

The evaluator defined 2 unit-tests that were executed on x86 hardware for performance reasons.

The total test effort expended by the evaluators was 1 week. During that test campaign, all time was spent on logical tests. The fuzz test ran for 2 days.

2.6.3 Test configuration

The test configuration for the repeated developer tests is the same as the developer's configuration for high-level tests. The tests were executed on the developer's system using secure remote access from the developer's Rijswijk office where they were witnessed by the evaluator.

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 TOE does not provide cryptographic functionality.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

There has been reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 4 Site Technical Audit Reports. The Shenzhen Bantian site was audited in the course of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Huawei HSM 2.0 Management Firmware version B006. Chapter 3.3 in the *[UG SVC]* describes how the user can query the TOE version.

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 in 4 Site Technical Audit Reports for the sites *[STAR]* [2].

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

Based on the above evaluation results the evaluation lab concluded the Huawei HSM 2.0 Management Firmware version B006, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 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.

This TOE is critically dependent on the operational environment to provide countermeasures against specific attacks as described in the *[UG]* chapter 2. Therefore, it is vital to maintain meticulous adherence to the user guidance of both the software and the hardware part of the TOE.

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.

[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 HSM 2.0 management firmware Security Target, Version 2.0, 2023-08-24 *[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:

AP	Application Processor
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
RNG	Random Number Generator
SHA	Secure Hash Algorithm
SoC	System on a Chip
TEE	Trusted Execution Environment
TOE	Target of Evaluation
TRNG	True Random Number Generator

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 HSM 2.0 Firmware, 23-RPT-049, 4.0, 16 November 2023
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	Huawei HSM 2.0 management firmware Security Target, Version 2.0, 2023-08-24
[STAR1]	Site Technical Audit Report - Huawei Shenzhen Bantian E1-2A-08 Development Site, 23-RPT-006, Version 1.0, 7 July 2023
[STAR2]	Site Technical Audit Report - Huawei Dongguan Data Center D1, 22-RPT-843, Version 1.0, 9 December 2022
[STAR3]	Site Technical Audit Report - Huawei Suzhou Data Center, 21-RPT-1057, Version 2.0, 03 January 2022
[STAR4]	Site Technical Audit Report - Huawei Hangzhou Development Site, 21-RPT-828, Version 2.0, 03 January 2022
[UG]	Huawei HSM 2.0 Management Firmware Guidance Document, Version 1.7, 24 August 2023
[UG SVC]	Huawei HSM 2.0 Management Firmware Service Command Specification, Version 1.6, 24 August 2023

(This is the end of this report.)