Certification Report

Huawei MA5800 Software Management Component V100R019C10SPH211

Sponsor and developer:	***Huawei Technologies Co., Ltd.*** **Huawei Base, Bantian, Longgang District, Shenzhen, China.**
Evaluation facility:	***Brightsight*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0132616-CR**
Report version:	**1**
Project number:	**0132616**
Author(s):	**Andy Brown**
Date:	**02 December 2020**
Number of pages:	**12**
Number of appendices:	**0**

Headoffice:
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 Dutch Chamber of Commerce 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 license 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, in order 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 and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Huawei MA5800 Software Management Component V100R019C10SPH211. The developer of the Huawei MA5800 Software Management Component V100R019C10SPH211 is Huawei Technologies Co., Ltd. located in Shenzhen, 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 management component of the Versatile Routing Platform (VRP) that runs on the control board of the MA5800 series.

The MA5800 series (MA5800-X17, MA5800-X15, MA5800-X7 and MA5800-X2) are aggregation Optical-Line-Terminal (OLT) with a distributed architecture and with different user access interfaces such as Gigabit-capable-Passive-Optical-Network (GPON), 10-Gigabit-capable- Passive-Optical-Network (10G PON), and 10/1G Ethernet (10GE/1GE) protocols.

The MA5800 supports deployment on Fiber-To-The-Home (FTTH), Fiber-To-The-Door (FTTD), Fiber-To-The-Building (FTTB), Fiber-To-The-Cabinet (FTTC), and Distributed-Converged-Cable- Access-Platform (D-CCAP) networks.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 02 December 2020 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 MA5800 Software Management Component V100R019C10SPH211, 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 MA5800 Software Management Component V100R019C10SPH211 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 provides sufficient evidence that the TOE meets the EAL3 augmented (EAL3+) 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]*.

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. It should be noted that the certification results only apply 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 releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Huawei MA5800 Software Management Component V100R019C10SPH211 from Huawei Technologies Co., Ltd. located in Shenzhen, China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	Huawei MA5800 Software Management Component	V100R019C10SPH211

To ensure secure usage a set of guidance documents is provided together with the Huawei MA5800 Software Management Component V100R019C10SPH211. Details can be found in section 2.5 of this report.

2.2 Security Policy

To counter the security threats listed in the [ST], the TOE provides the following security features:

- Identification and authentication of administrative users
  - Users are identified by a username and authenticated by password piror to accessing services of the TOE. The TOE is accessed via CLI (console and SSH). The TOE provides local authentication and remote authentication via RADIUS.
- Authorization
  - The TOE maintains multiple administration roles. There are in total 4 hierarchical access levels ranging from 0 ~ 3. The bigger the number, the higher is the privilege. Only authenticated users can execute commands of the TOE.
- Auditing
  - The TOE generates audit records for security-relevant management actions. All audit records contain not only the information on the event itself but also a timestamp and – if applicable – additional information like user ID, source IP, etc. Audit records are writing to local flash storage. The TSF deletes the oldest log files if the audit trail exceeds the size of the storage device
- Communication security
  - The TOE provides communication security by implementing the SSHv2 protocol. To protect the TOE from eavesdrop and to ensure data transmission security and confidentiality, SSHv2 provides:
    - Authentication of client by password or RSA public key;
    - AES encryption algorithms;
    - HMAC integrity verification algorithms;
    - Secure cryptographic key exchange.
- Management traffic flow control
  - For administration of the TOE, network packages have to be sent to the TOE from the management network. When a network packet reaches the TOE from the management network, the TOE applies an information flow security policy in the form of Access Control Lists (ACLs) to the traffic before processing it. Network packets on Layer 3 from the management network arriving at a network interface of the TOE are checked to ensure that they conform to the configured packet filter policy.
- Security functionality management
  - The TOE provides the following management functionalities:
    - Management of user accounts and user attributes, including user credentials.
    - Management of authentication failure policy.

- Access control management, including the association of users and corresponding privileged functionalities.
- Enabling and disabling trusted channels for local and remote access to the TOE's management interfaces.
- Management of ACLs and ACL attributes and parameters like IP addresses or address ranges.
- Configuration of network addresses for services used by the TOE, like NTP, SYSLOG, SSH.
- Management of the TOE's time.
- All security management functions (i.e. commands related to security management) require sufficient user level for execution.

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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in 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

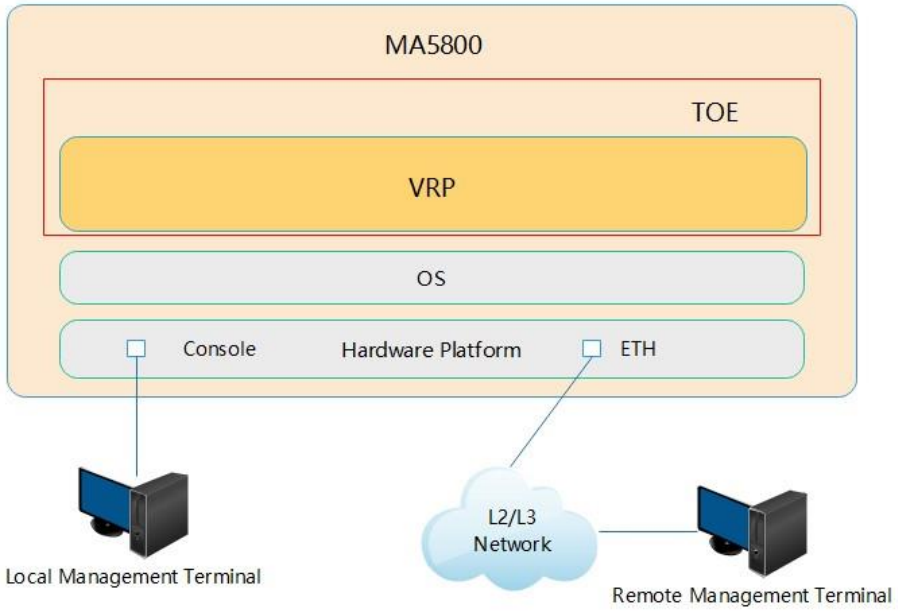
2.4 Architectural Information

The TOE is the management component of the Versatile Routing Platform (VRP) that runs on the control board of the MA5800 series.

The MA5800 series (MA5800-X17, MA5800-X15, MA5800-X7 and MA5800-X2) are aggregation Optical-Line-Terminal (OLT) with a distributed architecture and with different user access interfaces such as Gigabit-capable-Passive-Optical-Network (GPON), 10-Gigabit-capablePassive-Optical-Network (10G PON), and 10/1G Ethernet (10GE/1GE) protocols.

The MA5800 supports deployment on Fiber-To-The-Home (FTTH), Fiber-To-The-Door (FTTD), Fiber-To-The-Building (FTTB), Fiber-To-The-Cabinet (FTTC), and Distributed-Converged-CableAccess-Platform (D-CCAP) networks.

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



The VRP is responsible for managing and controlling the whole MA5800 software, communication, and security features in MA5800. The VRP is relying on the underlying OS. The OS is responsible for processes scheduling management, file system management, memory management, IPC module (Inter Process communication), and drivers etc. The security features of the TOE are all provided by the VRP.

2.5 Documentation

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

Identifier	Version
SmartAX MA5800 Product Documentation	V100R019C10_03
HUAWEI MA5800 Series Software V100R019C10 - AGD_OPE	1.0
HUAWEI MA5800 Series Software V100R019C10 - AGD_PRE	1.0
HUAWEI MA5800 Series Software V100R019C10 - ADV_C&R	0.4

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 focused on functional testing and manually tested all of the defined test cases. The developer grouped the 25 executed test cases into the following logical security functions:

- Authentication
- Authorization
- Auditing
- Access control
- Reliable time stamps
- Communication security

Each defined test case ran independently. There is no sequence dependency between test cases. The developer tested all the TSFIs.

The developer executed their test plan on a Huawei MA5800-X17 chassis with control board H901MPLB running V100R019C10SPH211. Figure 2 and Figure 3 shows the test configurations used by the developer.

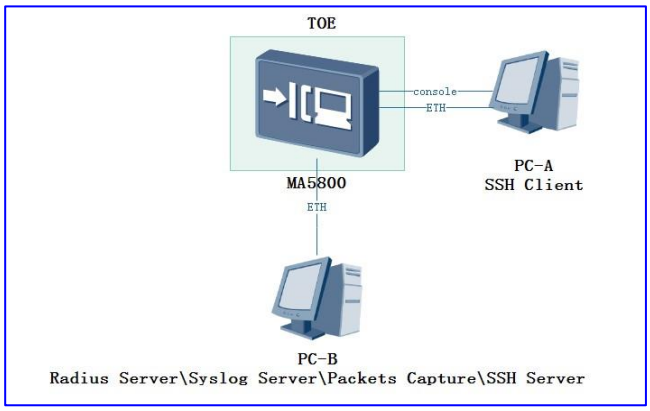


Figure 2 test configuration 1

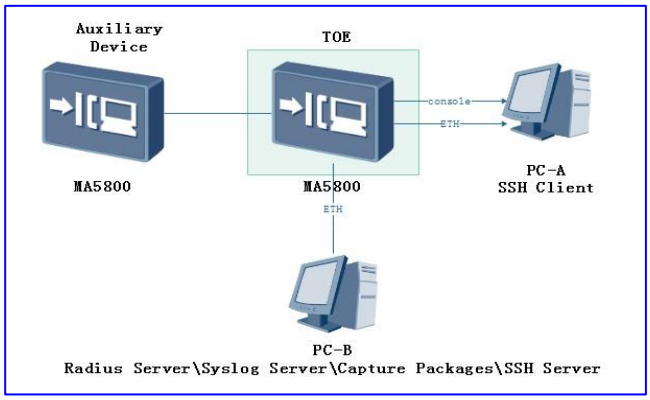


Figure 3 test configuration 2

The evaluator repeated 5 of the developer's test cases.

In addition, the evaluator devised 7 additional independent evaluator tests to further complement the coverage.

2.6.2 Independent Penetration Testing

To identify potential vulnerabilities the evaluator performed the following activities:

- SFR analysis
  - The evaluator applies their knowledge of attacks applicable to the TOE type.
- Public domain analysis
  - The evaluator performs a public domain vulnerability search for TOE specific items (TOE name, TOE-type, secure libraries, etc.)
  - The evaluator uses the websites provided by NSCIB as biases to perform the search.
- Network scanning tools
  - The evaluator runs vulnerability-scanning tools to identify potential vulnerabilities.

Penetration tests were created based on the vulnerabilities that are applicable to an attacker possessing Basic attack potential.

The evaluator devised seven (7) penetration tests were created to verify that the TOE, in its operational environment, is resistant to an attacker possessing a Basic attack potential.

2.6.3 Test Configuration

The test configuration is identical to that described in section 2.6.1.

2.6.4 Testing 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 overall conclusion is that the TOE is protected against attackers possessing a Basic attack potential, under the condition that the TOE user guidance is followed.

2.7 Re-used evaluation results

There is no re-use of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Huawei MA5800 Software Management Component V100R019C10SPH211.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*.

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

Based on the above evaluation results the evaluation lab concluded the Huawei MA5800 Software Management Component V100R019C10SPH211, to be **CC Part 2 extended, CC Part 3 conformant** and to meet the requirements of **EAL 3** augmented with ALC_FLR.2. 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 contains necessary information about the usage of the TOE.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE. The TOE needs to be operated in a segregated network that only allows for access via the remote interfaces and by physically protected interfaces (OE.NetworkSegration and OE.PhysicalProtection). Personnel working as authorized administrators are expected to be carefully selected for trustworthiness and trained for proper operation of the TOE (OE.NoEvil).

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

3 Security Target

The HUAWEI MA5800 Series Software Management Component V100R019C10, Issue 1.0, 2020-09-19 *[ST]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

CC	Common Criteria
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security CEM Common Methodology for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile
SSH	Secure Shell
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] Huawei MA5800 Software Management Component V100R019C10 ETR, 20-RPT-783, Version 3.0, 17 November 2020.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[ST] HUAWEI MA5800 Series Software Management Component V100R019C10, Issue 1.0, 2020-09-19.

(This is the end of this report).