Certification Report

Huawei A800 Series Routers V800R022C00SPC600

Sponsor and developer: ***Huawei Technologies Co., Ltd.***
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-2200048-01-CR**

Report version: **1**

Project number: NSCIB-**2200048-01**

Author(s): **Kjartan Jæger Kvassnes**

Date: **05 July 2023**

Number of pages: **10**

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) logo on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA Mutual Recognition Agreement (CCRA 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.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Huawei A800 Series Routers V800R022C00SPC600. The developer of the Huawei A800 Series Routers V800R022C00SPC600 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 are used to satisfy the requirements for networks of various scales. They are deployed at the edge of Metropolitan Area Networks or at access sites that process heavy traffic to implement multi-service acces.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 05 July 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 A800 Series Routers V800R022C00SPC600, 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 A800 Series Routers V800R022C00SPC600 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 *[NDcPP]* assurance requirements for the evaluated security functionality.

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 A800 Series Routers V800R022C00SPC600 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
Hardware	A811	n/a
	A821	n/a
Software	A800 Router V800R022C00SPC600	V800R022C00SPC600

To ensure secure usage a set of guidance documents is provided, together with the Huawei A800 Series Routers V800R022C00SPC600. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE supports the following security functionality:

- The TOE supports username/password, or public-key authentication mode and only users that are authenticated can access the TOE and its command line interface.
- The TOE is accessed by CLI locally or a NMS remotely over SSH so that a secure channel is established to protect the data between TOE and NMS.
- For secure transmission of audit information between the TOE and the Syslog server a secure TLS channel is used.
- The TOE supports digital signature verification for software. Each of the software package or patch package released by Huawei includes a unique digital signature. When an NMS distributes the package to router, the TOE will verify the online digital signature before updating. The verification of the digital signature demonstrates the integrity and authenticity of the package. The package is only processed further after successful verification of the digital signature, otherwise the package will be discarded without processing.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

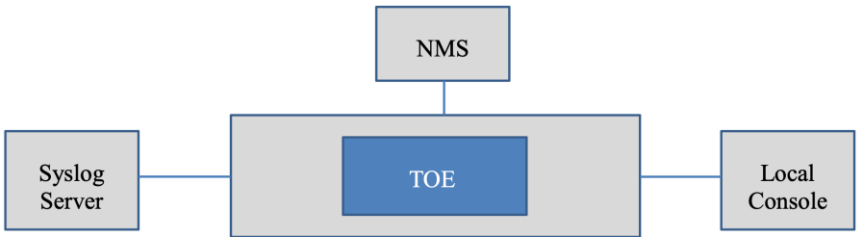
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.1 of the *[ST]*.

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 Security Target [ST] of the TOE can be depicted as follows:



The Huawei A800 Series Routers TOE are used to satisfy the requirements for networks of various scales. They are deployed at the edge of MANs or at access sites that process heavy traffic to implement multi-service access.

2.5 Documentation

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

Identifier	Version	Date
Huawei NetEngine A800 Series Routers, Preparative Procedures	V1.3	13 April 2023
Huawei NetEngine A800 Series Routers, Operational User Guidance	V1.3	08 June 2023
NetEngine A800 V800R022C00SPC600 Upgrade Guide	Issue 01	31 October 2022
NetEngine A821 E, A821, A811 M, A811 and A810 V800R022C00 Product Documentation	Issue 01	31 October 2022

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

All the evaluator defined tests are directly from the [NDcPP SD].

2.6.2 Independent penetration testing

The vulnerability assessment is performed following the guideline provided in [NDcPP] Appendix A, based on the following hypotheses:

- Type 1: Public – Vulnerability based
- Type 2: iTC Sourced
- Type 3: Evaluation-Team Generated
- Type 4: Tool Generated

Penetration tests were created based on the vulnerabilities that are applicable to an attacker possessing a Basic attack potential and according to *[NDcPP SD]* appendix A

The total test effort expended by the evaluators was 4.5 weeks. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The TOE was tested in the following configuration:

- Huawei A800 Series Routers V800R022C00SPC600 running on A821

The evaluator ran tests on the hardware model A821 only, and have verified that

- The hardware difference is not security relevant (e.g., port format)

- Only one software binary are in scope of the evaluation, thus all software security functionality of the TOE are identical for all models
- Some special crypto tests will be performed on a special crypto library build. It is verified the special crypto build and the crypto library used in the TOE software is identical.

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 evaluator 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 is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Huawei A800 Series Routers V800R022C00SPC600.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

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

Based on the above evaluation results the evaluation lab concluded the Huawei A800 Series Routers V800R022C00SPC600, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of ***[NDcPP]***. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'exact' conformance to the Protection Profile *[NDcPP]*.

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 Huawei A800 Series Routers Security Target, Version 1.4, Dated 08 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:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAN	Metropolitan Area Network
NSCIB	Netherlands Scheme for Certification in the area of IT Security
NSM	Network Management Server
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 “Huawei A800 Series Routers” – NDcPP, 23-RPT-013, Version 2.0, dated 12 June 2023
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[NDcPP]	Collaborative Protection Profile for Network Device, version 2.2e, dated 23 March 2020
[NDcPP SD]	Evaluation activities for Network Devices cPP, version 2.2, dated December 2019, registered under the reference CCDB-2019-12-004
[ST]	Huawei A800 Series Routers Security Target, Version 1.4, Dated 08 June 2023

(This is the end of this report.)