Certification Report

Common Criteria Protection Profile for Network Device Management (NDhPP), version 1.0, 2021-04-23

Sponsor and developer: ***Huawei Technologies Co., Ltd.***
Administration Building， Huawei Base, Bantian, Longgang District, Shenzhen
518129 Shenzhen
P.R.C.

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

Report number:	**NSCIB-PP-0335832-CR**
Report version:	**1**
Project number:	**0335832**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**1 July 2021**
Number of pages:	**10**
Number of appendices:	**0**

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

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.

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

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 Common Criteria Protection Profile for Network Device Management (NDhPP), version 1.0, 2021-04-23. The developer of the Common Criteria Protection Profile for Network Device Management (NDhPP), version 1.0, 2021-04-23 is Huawei Technologies Co., Ltd. located in Shenzhen, 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 Protection Profile *[PP]* address the network management of cloud-based networks and defines two classes of network device management components (A and B) each of which has slightly different requirements and objectives. The *[PP]* describes the security problem definition, security objectives and security requirements for both class A and class B. Class A devices may store information of a higher sensitivity level than class B. Therefore, an additional security objective and SFR´s for the TOE can be selected by the ST author to mitigate the additional threats.

The Protection Profile has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 7 May 2021 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 results documented in the evaluation technical report *[ETR]*[1]for this Protection Profile 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 and *[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. 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 Common Criteria Protection Profile for Network Device Management (NDhPP), version 1.0, 2021-04-23 from Huawei Technologies Co., Ltd. located in Shenzhen, P.R.C..

PP Title	Common Criteria Protection Profile for Network Device Management (NDhPP)
PP Version	Version 1.0, 2021-04-23
CC Version	3.1, revision 5
CC Conformance claim	Part 2 conformant, Part 3 conformant, EAL3 augmented with ALC_FLR.2
Required conformance	Conformance claims to this protection profile require **strict** conformance

2.2 Security Policy defined by the Protection Profile

The Protection Profile describes a set of security requirements for network management of telecommunication devices. The management and control layer of telecommunication devices are positioned as the brain of cloud-based networks and integrates functions such as network management, service control, and network analysis.

Therefore, the TOE has defined two classes of network device management components (Class A and Class B) each of which has slightly different requirements and objectives. Class A devices may store information of a higher sensitivity level than class B. Therefore, an additional security objective and SFR´s for the TOE can be selected by the ST author to mitigate the additional threats.

Class A

TheTOE-type is a software application that is located on the management and control layer of the cloud-based network. It can manage and control ubiquitous network devices, including transport, IP, and firewall devices. It provides open interfaces to quickly integrate with upper-layer application systems such as OSSs, service orchestrators and service applications. Various apps can be developed and customised to accelerate service innovation and achieve operations.

Class B

The TOE-type Management software installed on a service application/infrastructure device. Infrastructure devices such as Optical-Line-Terminal (OLT), optoelectronic OTN/WDM products transparently transmit client services from one place to another. In general these devices do not process client services transmitted from other equipment. These devices are generally managed by a EMS (Class A) device.

The major security features for the TOE-types listed in the TOE are:

Identification and authentication of administrative users.

- Only authenticated users can execute commands of the TOE.

Authorisation.

- The TOE manages user privileges by access level.

Auditing.

- The TOE generates audit records for security-relevant management actions.

Communication security.

- The TOE protects data integrity and confidentiality.

Management traffic flow control (Class B only)

- The TOE applies an information flow security policy before processing packets received from the management network.

Security functionality management.

- Management of user accounts and user attributes, access control management, management of authentication failure policy, enabling/disabling trusted channels, etc.

2.3 Security Functional Requirements

Based on the Security Objectives to be fulfilled by a TOE claiming conformance to the *[PP]* the security policy is expressed by the set of SFR´s to be implemented by the TOE.

The *[PP]* describe two classes of network device management, which differ from each other in various aspects. This chapter describes a number of security requirements, but not all security requirements are valid for both classes.

Security Functional Requirement		Class A	Class B
FAU_GEN.1	Audit event records generation	X	X
FAU_GEN.2	User identity association	X	X
FAU_SAR.1	Audit review	X	X
FAU_SAR.2	Restricted audit review	X	X
FAU_STG.1	Protected audit trail storage	X	X
FAU_STG.3	Action in case of possible audit data loss	X	X
FDP_ACC.2	Complete access control	X	X
FDP_ACF.1	Security attribute based access control	X	X
FDP_IFC.1	Subset information flow control		X
FDP_IFF.1	Simple security attributes		X
FIA_AFL.1	Authentication failure handling	X	X
FIA_ATD.1	User attribute definition	X	X
FIA_UAU.2	User authentication before any action	X	X
FIA_UAU.5	Multiple authentication mechanisms	X	X
FIA_UAU.7	Protected authentication feedback	X	X
FIA_UID.2	User identification before any action	X	X
FMT_MOF.1	Management of security functions behaviour	X	X
FMT_MSA.1/ACCESS	Management of security attributes	X	X
FMT_MSA.1/FILTER	Management of security attributes		X
FMT_MSA.3/ACCESS	Static attribute initialisation	X	X
FMT_MSA.3/FILTER	Static attribute initialisation		X
FMT_SMF.1	Specification of Management Functions	X	X
FMT_SMR.1	Security roles	X	X
FTA_SSL.3	TSF-initiated termination	X	X
FTA_TSE.1	TOE session establishment	X	X
FTP_TRP.1	Trusted path	X	X

FTP_ITC.1	Inter-TSF trusted channel	X	

2.4 Security Assurance Requirements

The TOE security assurance requirements claimed in the *[PP]* are based on the assurance components defined in part 3 of the Common Criteria for the Evaluation Assurance Level 3 package, augmented with ALC_FLR.2. Thus the SAR claim is called: **Common Criteria Part 3 conformant, EAL3 augmented with ALC_FLR.2.**

2.5 Results of the PP Evaluation

This evaluation was conducted using the methodology described in the *[CEM]* for the configuration defined in the *[PP]* using the APE class.

The evaluation lab documented their evaluation results in the *[ETR]* and determined that the claims as made in the *[PP]* are in conformance with the requirements for (standard) Protection Profiles as specified in class APE of the *[CC]*.

The certifier concluded that the evaluation lab has performed all APE work units in accordance with the APE section of the *[CEM]* and approved the *[ETR]* on 7 May 2021.

2.6 Comments/Recommendations

None

3 Protection Profile

The Common Criteria Protection Profile for Network Device Management (NDhPP), version 1.0, 23 April 2021 *[PP]* 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:

EMS	Enterprise Mobility Service
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
OLT	Optical-Line-Terminal
OSS	Operations Support System
OTN	Optical Transport Network
PP	Protection Profile
SAR	Security Assurance Requirement
TOE	Target of Evaluation
WDM	Wavelength Division Multiplexing

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] Common Criteria Protection Profile for Network Device Management (NDhPP) – Evaluation Technical Report APE, 21-RPT-259, Version 1.0, 23 April 2021.

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

[PP] Common Criteria Protection Profile for Network Device Management (NDhPP), version 1.0, 23 April 2021.

(This is the end of this report).