Agenzia per la Cybersicurezza Nazionale

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti
ISO/IEC 15408 Common Criteria (CC) v.3.1 rel. 5

Certificato n. *(Certificate No.)*	01/2024
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/TCN/15/2022/RC, v1.0
Decorrenza *(Date of 1st Issue)*	12 gennaio 2024
Nome e Versione del Prodotto *(Product Name and Version)*	HUAWEI Software V100R022C00SPC100 for EA5800, EA5801E, EA5801S series devices
Sviluppatore *(Developer)*	Huawei Technologies Co., Ltd
Tipo di Prodotto *(Type of Product)*	Rete e Dispositivi e Sistemi relativi alla rete
Livello di Garanzia *(Assurance Level)*	EAL3 (ALC_FLR.2) conforme a CC Parte 3
Conformità a PP *(PP Conformance)*	Nessuna
Funzionalità di sicurezza *(Conformance of Functionality)*	TDS specifico per il prodotto conforme a CC Parte 2

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR
(CCRA recognition for components up to EAL2 and ALC_FLR only)

Riconoscimento SOGIS MRA per componenti fino a EAL4
(SOGIS MRA recognition for components up to EAL4)

Roma, 12 gennaio 2024

p. il Direttore Generale
dell’ACN

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

[ORIGINAL SIGNED]

Il prodotto IT (*Information Technology*) identificato nel presente certificato è stato valutato presso un LVS (Laboratorio per la Valutazione della Sicurezza) accreditato e abilitato/approvato utilizzando la Metodologia Comune per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5. Questo certificato si applica solo alla versione e al rilascio specifici del prodotto nella sua configurazione valutata e unitamente al Rapporto di certificazione completo. La valutazione è stata condotta in conformità alle disposizioni dello Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004) e le conclusioni dell'LVS nel Rapporto di Fine Valutazione sono coerenti con le evidenze addotte. Il presente Certificato non costituisce un sostegno o promozione del prodotto IT da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosca o dia effetto a questo certificato, e nessuna garanzia del prodotto IT, da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosce o dà effetto a questo certificato, è espressa o implicita.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using Common Methodology for Information Technology Security Evaluation version 3.1 release 5 for conformance to *Common Criteria for Information Technology Security Evaluation version 3.1 release 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of the National scheme for the evaluation and certification of the security in the sector of information technology (Prime Ministerial Decree of 30 October 2003 - Official Journal no. 93 of 27 April 2004) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product, by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.*

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

HUAWEI Software V100R022C00SPC100 for EA5800, EA5801E, EA5801S series devices

OCSI/CERT/TCN/15/2022/RC

Version 1.0

12 January 2024

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	12/01/2024

2 Table of contents

3 Acronyms

3.1 National scheme

DPCM	Decreto del Presidente del Consiglio dei Ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Agreement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other acronyms

AAA	Autentication Authorization and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
BIOS	Basic Input/Output System

CLI	Command Line Interface
CPLD	Complex Programmable Logic Device
cPP	collaborative Protection Profile
FPGA	Field Programmable Gate Array
HMAC	Hash-based Message Authentication Code
HTTPS	Hyper Text Transfer Protocol Secure
IP	Internet Protocol
IPC	Inter-Process Communication
IT	Information Technology
LMT	Local Management Terminal
NG PON	Next-Generation Passive Optical Network
NTP	Network Time Protocol
OLT	Optical Line Terminal
PC	Personal Computer
RMT	Remote Management Terminal
RSA	Rivest Shamir Adleman
SSH	Secure Shell
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VRP	Versatile Routing Platform
VTYs	Virtual Terminals

4 References

4.1 Normative references and national Scheme documents

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 agosto 2023

[SOGIS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3, January 2010

4.2 Technical documents

[CC_PRE] HUAWEI Software V100R022C00SPC100 for EA5800/EA5801E/EA5801S Series Devices - AGD_PRE, version 0.6 December 4th 2023

[CC_OPE] HUAWEI Software V100R022C00SPC100 for EA5800/EA5801E/EA5801S Series Devices - AGD_OPE, version 0.4 December 4th 2023

[ETRv1.1] “Final Evaluation Report for HUAWEI V100R022C00SPC100 for EA5800/EA5801E/EA5801S Series Devices, Version 1.1, Tecninf S.p.A., October 23th 2023

[ETRv1.2] “Final Evaluation Report for HUAWEI V100R022C00SPC100 for EA5800/EA5801E/EA5801S Series Devices, Version 1.2, Tecninf S.p.A., November 29th 2023

[ST] HUAWEI Software V100R022C00SPC100 for EA5800, EA5801E, EA5801S series devices - Security Target, Huawei Technologies Co., Ltd., version 1.0, September 18th 2023

[CRYPTO] SOGIS Agreed Cryptographic Mechanisms, version 1.3, February 2023

5 Recognition of the certificate

5.1 European recognition of CC certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT -Products. A higher recognition level for evaluations beyond EAL4 is provided for IT -Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under SOGIS-MRA up to EAL4.

5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] was ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA up to EAL2 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the product named "**HUAWEI Software V100R022C00SPC100 for EA5800, EA5801E, EA5801S series devices**", developed by Huawei Technologies Co., Ltd.

The TOE is responsible for managing and controlling the communication and security functionalities of the optical multiservice access nodes that provide a unified transport platform for multiple services over a fiber network, such as broadband, wireless, video and monitoring.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body "Organismo di Certificazione della Sicurezza Informatica (OCSI)", established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC version 3.1 Revision 5 for the assurance level EAL3, augmented with ALC_FLR.2, according to the information provided in the Security Target [ST] and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report.

The TOE certified configuration consists of the TOE operating on the hardware models selected for evaluation. Namely, the TOE has been installed, configured and tested on the following hardware during the evaluation: EA5800-X2, EA5800-X7, EA5800-X15, EA5800-X17, EA5801E-GP08-H3, EA5801E-GP16-H2, EA5801E-GP04-H2, EA5801E-FL16-H1, EA5801S-GP16-H2.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product named “HUAWEI Software V100R022C00SPC100 for EA5800, EA5801E, EA5801S series devices” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should also review the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	HUAWEI Software V100R022C00SPC100 for EA5800, EA5801E, EA5801S series devices
Security Target	HUAWEI Software V100R022C00SPC100 for EA5800, EA5801E, EA5801S series devices - Security Target, Huawei Technologies Co., Ltd., version 1.0, September 18th 2023
Evaluation Assurance Level	EAL3 augmented with ALC_FLR.2
Developer	Huawei Technologies Co., Ltd.
Sponsor	Huawei Technologies Co., Ltd.
LVS	Tecninf S.p.A.
CC version	3.1 Rev. 5
PP conformance claim	No conformance claimed
Evaluation starting date	17 November 2022
Evaluation ending date	26 October 2023

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled and in the configuration shown in “Annex B – Evaluated configuration” of this Certification Report.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description, please refer to the Security Target [ST].

The Target of Evaluation (TOE) is the product named “HUAWEI Software V100R022C00SPC100 for EA5800, EA5801E, EA5801S series devices”, developed by Huawei Technologies Co., Ltd.

The EA5800, EA5801E, EA5801S series devices are next generation Optical Line Terminal (OLT) for NG PON (Figure 1).

The TOE, i.e. the Software V100R022C00SPC100, is responsible for managing and controlling the communication and security functionalities of the optical multiservice access nodes that provide a unified transport platform for multiple services over a fiber network, such as broadband, wireless, video and monitoring.

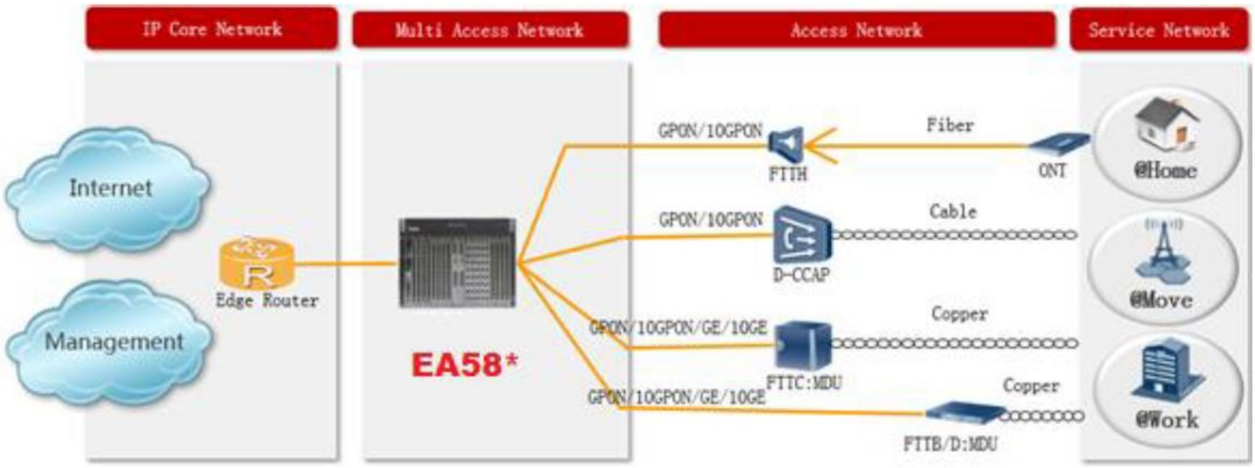

Figure 1 - Typical usage of the optical multiservice access node

For a detailed description of the TOE, refer to sections 1.3, 1.4 and 1.5 of the Security Target [ST].

7.3.1 TOE architecture

The TOE boundary is represented in Figure 2 with a red line encompassing the two components Versatile Routing Platform (VRP) and TCP/IP stack. The Operating System and the hardware platforms are not part of the TOE.

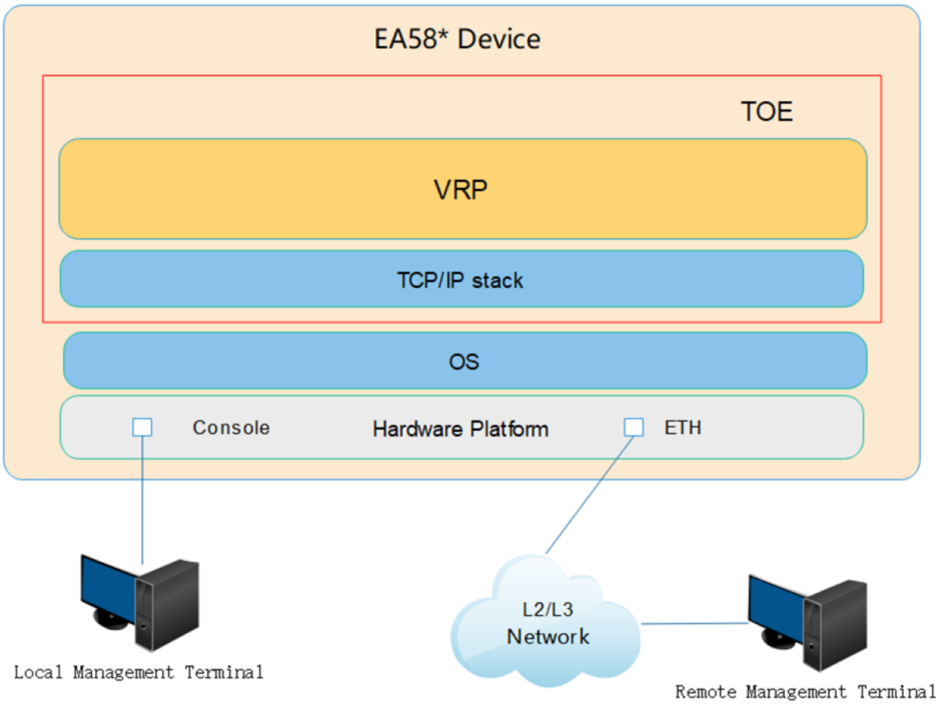

Figure 2 - V100R022C00SPC100 subsystems and TOE boundary

The VRP is responsible for managing and controlling the whole device in terms of communication, and security features. The VRP provides different interfaces with access levels for administrators, guarantees authentication prior to establishment of administrative sessions and performs auditing of security relevant management activities.

The OS is responsible for processes scheduling management, file system management, memory management, IPC module (Inter Process communication), and drivers etc.

The main security features of the TOE, provided by the VRP, are:

- Identification and authentication of administrative users;
- Authorization;
- Auditing;
- Communication security;
- Management traffic flow control;
- Security functionality management.

The detailed description of these security features is in section 1.5.2 of the Security Target [ST].

The TOE has been evaluated on the hardware platforms identified in Table 1.

Series devices	Hardware platform identification
EA5800	EA5800-X2 EA5800-X7 EA5800-X15 EA5800-X17
EA5801E	EA5801E-GP04-H2 EA5801E-GP08-H3 EA5801E-GP16-H2 EA5801E-FL16-H1
EA5801S	EA5801S-GP16-H2

Table 1 - Hardware model identification

The external entities which may communicate with the TOE are shown in Figure 3. The CLI interface of the TOE can be accessed either through Local Maintenance Terminal (LMT) via the Console port on the control board, or through Remote Maintenance Terminal (RMT) via a secure SSHv2 channel based on the ETH port located on the control board.

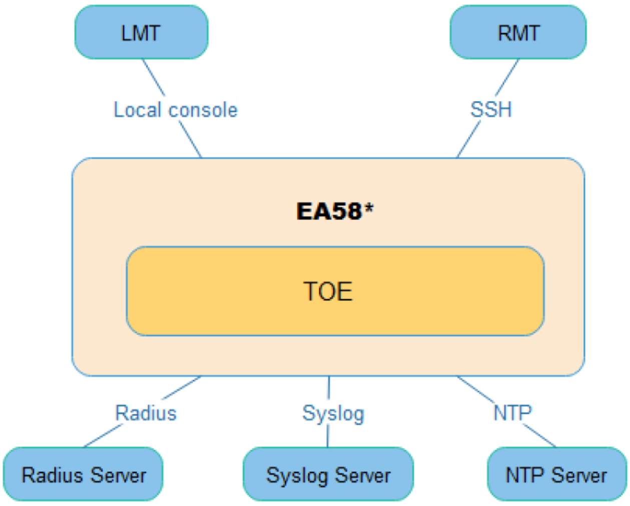

Figure 3 - External entities communication with the TOE

The TOE supports local authentication with username and password using local database, or remote authentication using RADIUS server.

The TOE sends report audit information to SYSLOG Server and supports time synchronization using NTP server.

7.3.2 TOE security features

Assumptions, threats and security objectives are defined in section 3 and 4 of the Security Target [ST].

For a detailed description of the TOE Security Functions, refer to sections 1.5.2 and 6 of the Security Target [ST]. The most significant aspects are summarized in the following sections.

7.3.2.1 Identification and authentication of administrative users

The CLI interface of the TOE can be accessed either through LMT (i.e. the 'console') or RMT (i.e. via virtual terminals, 'VTYs'). The LMT can only access the TOE via the physical console port of the appliance, it is authenticated by username and password. The RMT accesses the TOE via SSH and it is authenticated by username and password or public key, and the possible authentication modes include password only, public key only, password and public key, password or public key. Only authenticated users can execute commands of the TOE. The password policy requires 12 characters at least and the password can be composed of uppercase letters, lowercase letters, numbers and special characters. The password must contain at least one uppercase letter, one lowercase letter, one number and one special character.

The TOE provides a local authentication mode or can optionally enforce authentication decisions obtained from a AAA server in the IT environment.

In local authentication mode, accounts and passwords are saved on the local equipment and authenticated using the local account and password by the local equipment during login. In remote authentication mode, accounts and passwords are saved on the AAA server and authenticated by the AAA server. During login, the accounts and passwords are forwarded to the AAA server, using the RADIUS protocol and the AAA server checks the validity of accounts and passwords.

User authentication is always enforced for virtual terminal sessions via SSH sessions and for local terminal sessions via the console. The use of SSH connection is always required for accessing the TOE via RMT. For LMT no logically secured communication channel is required.

7.3.2.2 Authorization

Through authorization devices assign operation permissions to accounts according to their profile.

The TOE manages user privileges by access level. There are 3 hierarchical access levels ranging from 0 to 2. The bigger is the number, the higher is the privilege. Correspondingly, levels from 0 to 2 can be assigned to all commands provided by the TOE. A user can access a command if the command's access level is lower or equal to the user's access level. By default, commands are registered with level 0~2.

The three hierarchical access control levels are listed in the Table 2.

User level	Level name	Authority
0	Common user	Perform basic system operations and simple query operations.
1	Operator	Perform basic configuration operations for the service and device.
2	Administrator	Perform all configuration operations. Maintain and manage the device, perform security management, create other user including administrator, operator and common user accounts.

Table 2 - TOE user level.

All authenticated users with an access level equal or higher to the access level of the command (also referred to as *command level*) are allowed to execute the corresponding command.

7.3.2.3 Auditing

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 functionality is activated by default and cannot be deactivated.

TOE supports writing the audit records in local storage or sending the audit records to external audit servers via SYSLOG protocol. When writing into the local storage, audit records are written into log buffer first and then moved to log files located in Flash memory.

7.3.2.4 Communication security

The TOE provides communication security by implementing the SSHv2 protocol. The TOE can act as both STELNET server and STELNET client. When the RMT accesses the TOE, the TOE acts as STELNET server, and when the users who login the TOE access other SSH server via STELNET, the TOE acts as STELNET client.

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.

TOE does not offer cryptographic services, but uses cryptographic mechanisms in the implementation of its communication security functions (SSH) and Identification and Authentication functions (SSH public key authentication). The TOE is capable of generating the necessary keys (AES, RSA).

7.3.2.5 Management traffic flow control

For administration of the TOE, network packets 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 List (ACL) 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. Packet flows matching a deny rule in the ACL are dropped. If no rule is specified for an incoming packet, it is forwarded by default. Through this mechanism the TOE provides network filtering based on ACLs for the management network as a security function.

Users with sufficient access rights can create, delete, and modify rules for ACL configuration to filter, prioritize, rate limit the information flow destined to TOE or other network devices through interfaces by matching information contained in the headers of connection oriented or connectionless packets against ACL rules specified. Ethernet protocol type, Source IP address, destination IP address, IP protocol number, source port number if TCP/UDP protocol, destination port number if TCP/UDP protocol, TCP flag if TCP protocol, etc., can be used for ACL rule configuration.

7.3.2.6 Security functionality management

Security functionality management includes not only authentication, access level, but also managing security related data consisting of configuration profile and runtime parameters. According to security functionality management, customized security is provided.

Security functionalities include:

- 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.

7.4 Documentation

The guidance documentation specified in "Annex A – Guidelines for the secure usage of the product" is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration, and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in section 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

All the SFRs have been selected or derived by extension from CC Part 2 [CC2].

Please refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme

Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) Tecninf S.p.A..

The evaluation was completed on 26 October 2023 with the issuance by LVS of the Evaluation Technical Report [ETRv1.1], which was approved by the Certification Body on 14 November 2023. An additional ETR ([ETRv1.2]) was delivered on 2 December 2023 including minor changes. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in “Annex B – Evaluated configuration” (see also [CC_PRE] and [CC_OPE]).

Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; there is a probability, however small, that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to regularly check the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETRv1.1] issued by the LVS Tecninf S.p.A. and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE named "HUAWEI Software V100R022C00SPC100 for EA5800, EA5801E, EA5801S series devices" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL3 augmented with ALC_FLR.2, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in "Annex B – Evaluated configuration".

Table 3 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL3 augmented with ALC_FLR.2.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Functional specification with complete summary	ADV_FSP.3	Pass
Architectural design	ADV_TDS.2	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Authorizations Control	ALC_CMC.3	Pass
Implementation representation CM coverage	ALC_CMS.3	Pass
Delivery procedures	ALC_DEL.1	Pass
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
Flaw reporting procedures	*ALC_FLR.2*	*Pass*

Assurance classes and components		**Verdict**
Test	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Vulnerability analysis	AVA_VAN.2	Pass

Table 3 Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in section 6 (Statement of Certification).

Potential customers of the product “HUAWEI Software V100R022C00SPC100 for EA5800, EA5801E, EA5801S series devices” are suggested to properly understand the specific purpose of the certification by reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the “Security Objectives for the Operational Environment” specified in section 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all Assumptions described in section 3.3 of the Security Target [ST] shall be satisfied. It is worth mentioning that some potential vulnerabilities have been found during testing (Cfr. “Annex C – Test activity) and they are not exploitable provided that TOE users strictly abide by all assumptions on TOE environment. Evaluators and the Certification Body recommended the Developer correct found vulnerabilities even if they are currently not exploitable in the intended Operational Environment.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, “Annex A – Guidelines for the secure usage of the product” includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([CC_PRE], [CC_OPE]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE delivery

TOE and TOE documentation ([CC_PRE], [CC_OPE]) are delivered to customers using Huawei support website.

Alongside with the hardware components, Huawei provides TOE customers with instructions to access the support HTTPS website. Therefore, to download software and documentation:

1) Login at https://support.huawei.com;
2) Select the target version. The software and document list for the version are displayed. Click a file name and fill in the information as required to download it;
3) Choose product line (e.g. Enterprise);
4) Select the 'Documentation' tab and choose the correct TOE version (V100R022C00).

The software package containing the TOE software is digitally signed by Huawei. The signature files use the same filename as software packages, with the filename extension of "asc". For example, if the software package name is EA5800V100R022C00SPC100.zip, the corresponding verification file name is EA5800V100R022C00SPC100.zip.asc. The signature shall be verified using GnuPG (section 6 in [CC_PRE] document provides comprehensive description).

As the TOE is identified by V100R022C00SPC100, each family product has its own software package and verification file as in the following:

- For EA5800 series
  - EA5800V100R022C00SPC100.zip (software package name)
    SHA256 33FB0D3EA239D0AE8A8E14272390385941678D3CEC7FAE218BC81A75B4491AA0
  - EA5800V100R022C00SPC100.zip.asc (verification file name)
- For EA5801E series
  - EA5801EV100R022C00SPC100.zip (software package name)
    SHA256 AFBD467138C2D22605BAADFA7064D8A4107D5868AF263BD7AB26C0239E9C8C60
  - EA5801EV100R022C00SPC100.zip.asc (verification file name)
- For EA5801S series
  - EA5801SV100R022C00SPC100.zip (software package name)
    SHA256 87F4EFF7804BFFE254445B540308E7E0B593643C6FC844A23BE0782784A765F8
  - EA5801SV100R022C00SPC100.zip.asc (verification file name)

9.2 Identification of the TOE

The TOE user can identify TOE components as described below:

- **Software**: The user can verify TOE version by checking the installed version as described in [CC_PRE].
- **Guidance documentation**: the version number is printed in the documents.

Hardware model name is marked on the front of the device and the product number on the product label located on the case (back or top).

9.3 Installation, initialization, and secure usage of the TOE

TOE installation, configuration and operation should be done by following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the following documents contain detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure operation of the TOE in accordance with the security objectives specified in the Security Target [ST]:

[CC_PRE]	HUAWEI Software V100R022C00SPC100 for EA5800/EA5801E/EA5801S Series Devices - AGD_PRE, version 0.6 December 4th 2023
[CC_OPE]	HUAWEI Software V100R022C00SPC100 for EA5800/EA5801E/EA5801S Series Devices - AGD_OPE, version 0.4 December 4th 2023

10 Annex B – Evaluated configuration

The TOE consists of the Management Component Software used on the EA5800, EA5801E, EA5801S family of devices (hardware appliances are not part of the TOE), manufactured by Huawei Technologies Co., Ltd.

EA5800, EA5801E, EA5801S series hardware devices are optical multiservice access nodes that provide a unified transport platform for multiple services over a fiber network, such as broadband, wireless, video and monitoring.

Hardware, which is not part of the TOE, consists of the cabinet, chassis, power supply unit and boards. The TOE software is running on the device's control board and the TOE is only the management software components. The underlying operating system contained in the evaluated platforms (RTOS) is not part of the TOE. The TOE components provide the main control and management services for the hardware device.

The TOE evaluated configuration consists of the TOE running on one of the following optical multiservice access node, on which the TOE was installed, configured and tested during the evaluation:

- EA5800:
  - EA5800-X2
  - EA5800-X7
  - EA5800-X15
  - EA5800-X17
- EA5801E:
  - EA5801E-GP04-H2
  - EA5801E-GP08-H3
  - EA5801E-GP16-H2
  - EA5801E-FL16-H1
- EA5801S:
  - EA5801S-GP16-H2

Preparative procedures are described in [CC_PRE].

10.1 TOE operational environment

The following components are part of the TOE environment:

- Local PCs used by administrators for accessing TOE command line interface, either through local console interface or ETH interface via a secure channel enforcing SSH.
- Remote PCs used by administrators for accessing TOE command line interface, through ETH interface via a secure channel enforcing SSH.
- Radius server is optional and is used for centralized authentication via Radius protocol.
- Syslog server is optional and is used for receiving audit information from the TOE via SYSLOG protocol.

- NTP server is used for synchronizing time to the TOE.
- Physical networks, such as Ethernet subnets, interconnecting various networking devices.
- EA5800, EA5801E, EA5801S hardware, firmware and non-TOE software, including BIOS/OS/FPGA/CPLD of the control board.

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities.

11.1 Test configuration

Testing activities have been carried out in the LVS site.

The Evaluators verified the configuration of the test environment, including the TOE, and found it to be consistent with the Common Criteria Preparative Procedures [CC_PRE] and the Security Target [ST]. Hardware listed in section 10 Annex B "Evaluated configuration" was used for testing.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer used a testing approach that resulted in covering all the TSFIs with at least one test case. For each test case, the Developer's test documentation describes its purpose, the relevant TSFI(s) and SFR(s), test prerequisites, step-by-step test procedures, and expected test results.

11.2.2 Test coverage

The Evaluators have examined the test plan presented by the Developer and verified the complete coverage of the functional requirements (SFRs) and the TSFIs described in the functional specification.

11.2.3 Test results

The actual test results of all Developer's tests were consistent with the expected ones.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Test approach

Before initiating the testing activity, the Evaluators verified that the TOE was configured correctly. They also verified that the test environment was properly set up.

It has been verified that the encryption algorithms used to connect to the TOE are those conforming to the document "SOGIS Agreed Cryptographic Mechanisms" (Ref. [CRYPTO]).

11.3.2 Test results

All the actual test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked with the TOE on the same hardware already used for the functional test activities and verified that the TOE and the test environment were properly configured. Most recent vulnerability analysis was performed on July 9th, 2023.

The Evaluators could conclude that the TOE is resistant to a BASIC attack potential in its intended operating environment even if some potential vulnerabilities (i.e. vulnerabilities that cannot be exploited in the intended operational environment) have been identified.

Customers must be informed that potential vulnerabilities are not exploitable provided that TOE users strictly abide by assumptions on TOE environment, as described at chapter 3.3 in [ST] document and, in particular, the following:

- ***A.NetworkSegregation*** *- It is assumed that the operational environment provides segregation of networks by deploying the management interface in TOE into an independent local network.*
- ***A.NoEvil*** *- It is assumed that personnel working as authorized administrators and non-TOE administrators (administrators that have physical access to the TOE but do not operate the TOE) shall be carefully selected for trustworthiness and trained for proper operation of the TOE. These administrative users will be competent, and not careless or willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.*
- ***A.PhysicalProtection*** *- It is assumed that the TOE and its operational environment (i.e. the complete system including attached peripherals) are protected against unauthorized physical access. It is assumed that only administrators and non-TOE administrators (administrators that have physical access to the TOE but do not operate the TOE) with explicit approval by the administrator(s) are authorized to physically access the TOE and its operational environment. This assumption includes that the local management network, including the AAA server (RADIUS server), SYSLOG server, NTP server and locally attached management terminals (LMT) together with all related communication lines are operated in the same physically secured environment as the TOE. Remote management terminal (RMT) needs to be physically protected on the same level as the TOE but they do not necessarily have to be kept in the same physical environment. The communication lines between any RMT and the TOE are protected by cryptographic means and do not need any physical protection. It is assumed that all RMT as well as peripherals like AAA server, NTP server or SYSLOG server are connected to the TOE via the same segregated management network (see also A.NetworkSegregation).*

Evaluators and the Certification Body recommend the Developer to correct found vulnerabilities even if they are not exploitable in the intended operational environment, comprising the above assumptions.