Agenzia per la Cybersicurezza Nazionale

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 7/23

(Certificate No.)

Prodotto: **Huawei NetEngine 8000 Series Routers' Software V800R022C00SPC600**
(Product)

Sviluppato da: **Huawei Technologies Co., Ltd.**
(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL2+
(ALC_FLR.2)

p. il Direttore Generale
dell'ACN

Il Capo Servizio
Certificazione e Vigilanza
(Andrea Billet)

Roma, 13 giugno 2023

[ORIGINAL SIGNED]

Common Criteria

SOGIS IT SECURITY CERTIFIED

This page is left intentionally blank

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Huawei NetEngine 8000 Series Routers' Software V800R022C00SPC600

OCSI/CERT/ATS/13/2022/RC

Version 1.0

13 June 2023

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	13/06/2023

2 Table of contents

1 Document revisions 5
2 Table of contents 6
3 Acronyms 8
3.1 National Scheme 8
3.2 CC and CEM 8
3.3 Other Acronyms 8
4 References 10
4.1 Normative references and national Scheme documents 10
4.2 Technical documents 11
5 Recognition of the certificate 12
5.1 European recognition of CC certificates (SOGIS-MRA) 12
5.2 International recognition of CC certificates (CCRA) 12
6 Statement of certification 13
7 Summary of the evaluation 14
7.1 Introduction 14
7.2 Executive summary 14
7.3 Evaluated product 14
7.3.1 TOE architecture 15
7.3.2 TOE security features 16
7.4 Documentation 17
7.5 Protection Profile conformance claims 17
7.6 Functional and assurance requirements 18
7.7 Evaluation conduct 19
7.8 General considerations about the certification validity 20
8 Evaluation outcome 21
8.1 Evaluation results 21
8.2 Recommendations 22
9 Annex A – Guidelines for the secure usage of the product 23
9.1 TOE delivery 23
9.2 Identification of the TOE 24
9.3 Installation, initialization, and secure usage of the TOE 25

10 Annex B – Evaluated configuration 26

11 Annex C – Test activity 27

11.1 Test configuration 27

11.2 Functional tests performed by the Developer 27

11.2.1 Testing approach 27

11.2.2 Test coverage 27

11.2.3 Test results 28

11.3 Functional and independent tests performed by the Evaluators 28

11.3.1 Testing approach 28

11.3.2 Test results 28

11.4 Vulnerability analysis and penetration tests 28

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
cPP	collaborative Protection Profile
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	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol

CLI	Command Line Interface
DP	Data Plane
DRBG	Deterministic Random Bit Generator
ECC	Elliptic Curve Cryptography
GCP	General Control Plane
HMAC	Hash-Based Message Authentication Code
IP	Internet Protocol
MITM	Man In The Middle
NTP	Network Time Protocol
OS	Operating System
RADIUS	Remote Authentication Dial-In User Service
RSA	Rivest Shamir Adleman
SCP	Service Control Plane
SHA	Secure Hashing Algorithm
SMP	System Manage Plane
SSH	Secure Shell
SSP	System Service Plane
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UI	User Interface
VRP	Versatile Routing Platform

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. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

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

4.2 Technical documents

[CPP_ND] "collaborative Protection Profile for Network Devices", version 2.2e, 23 March 2020

[ETRv2] "Final Evaluation Technical Report Huawei NetEngine 8000 Series Routers' Software", version 2, date 2023-03-16

[ETRv3] "Final Evaluation Technical Report Huawei NetEngine 8000 Series Routers' Software", version 3, date 2023-04-26

[OPE] "Huawei NetEngine 8000 Series Routers' Software V800R022C00 Operational User Guidance", issue 1.3, date 2023-03-13

[PRE] "Huawei NetEngine 8000 Series Routers' Software V800R022C00 Preparative Procedures", issue 1.6, date 2023-03-13

[SIG_VER] "OpenPGP V100R001C00 Signature Verification Guide", issue 04, date 2020-10-09

[SOF_UPG] "Huawei NetEngine 8000 Series Routers' Software V800R022C00 Upgrade Guide", issue 1.2, date 2022-11-29

[ST] "Huawei NetEngine 8000 Series Routers' Software Security Target", version 1.4, date 2023-05-25

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 recognized under the terms of this agreement by signatory nations.

This certificate is recognized under SOGIS-MRA for all declared assurance components.

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 for all declared assurance components.

6 Statement of certification

The Target of Evaluation (TOE) is the product “NetEngine 8000 Series Routers' Software version V800R022C00SPC600”, also referred to in the following as “NetEngine 8000 Series Routers’ Software”, developed by Huawei Technologies Co., Ltd.

The TOE is a part of the software running on the NetEngine 8000 Series Routers. These routers consist of both hardware (non-TOE) and software. The software running on the routers is named Versatile Routing Platform (VRP) running on the routers’ OS. VRP provides extensive security features, including services for administrators, enforcing authentications prior to establishment of administrative sessions, auditing of security relevant management activities.

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 also review 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 v 3.1 for the assurance level EAL2, 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 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 ”Huawei NetEngine 8000 Series Routers' Software V800R022C00SPC600” 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 NetEngine 8000 Series Routers' Software V800R022C00SPC600
Security Target	Huawei NetEngine 8000 Series Routers' Software Security Target Version 1.4 [ST]
Evaluation Assurance Level	EAL2 augmented with ALC_FLR.2
Developer	Huawei Technologies Co., Ltd.
Sponsor	Huawei Technologies Co., Ltd.
LVS	atsec information security s.r.l.
CC version	3.1 Rev. 5
PP conformance claim	No conformance declared
Evaluation starting date	5 August 2022
Evaluation ending date	16 March 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.

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 TOE is a part of the software named “Versatile Routing Platform” (VRP) running on the NetEngine 8000 Series Routers and part of the routers OS Huawei. VRP provides security features including authentication prior to establishment of administrative sessions and auditing of security relevant events.

7.3.1 TOE architecture

Figure 1 shows the logical scope of the TOE and TOE boundaries.

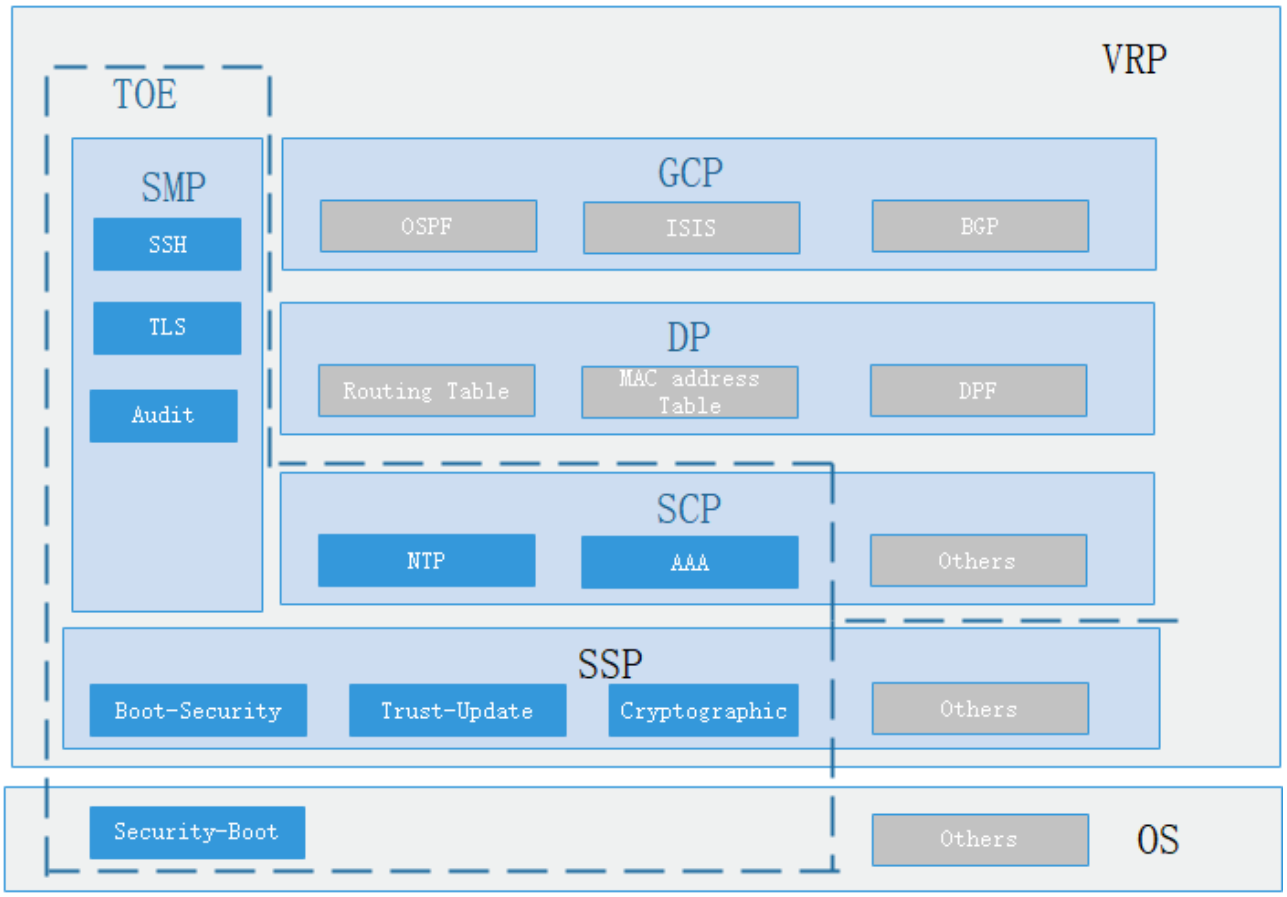

Figure 1 - TOE logical scope and boundaries

The TOE, that is part of the VRP and OS, is a network operating platform, which has a distributed, multi-process, and component-based architecture. VRP is responsible for functional management, routing information generation, receiving generated routing information and formatting them into hardware-specific data to direct traffic forwarding.

6 logical planes are defined for the complete software architecture of the routers:

- System Manage Plane (SMP), implements management for external access, management for system configuration, information output on VRP.
- Service Control Plane (SCP), implements authentication, authorization, accounting and other serviceable functionality on VRP.
- System Service Plane (SSP), implements system internal scheduling, communication, management of signals, events, timers, etc.
- Operating System (OS), provides hardware and software resource management.

- General Control Plane (GCP), implements routing information learning, ARP table entry learning, STP (Spanning Tree Protocol) topology management, and functionalities related to TCP/IP stack on VRP (out of TOE logical boundaries).

- Data Plane (DP), implements traffic forwarding. Forwarding related information, e.g. routing information, ARP table entry, static MAC table entries are generated in GCP and downloaded via communication channel provided by SSP (out of TOE logical boundaries).

The whole TOE consist of a single security domain based on the software running on the routers.

The TOE stores data in form of files in the non-TOE hardware device on which the TOE is running. These files include not only the overall configuration profile, but also TSF data and non-TSF data. In order to secure these files, access is provided through Command Line Interface (CLI) (Serial interface) or SSH (SSH interface). No matter what type of accesses the user adopts, authentication must be enforced prior to any action. TOE defines several user levels with different privileges: only trusted “level 15 administrator” has the access to all the security configurations.
For a detailed description of the TOE, consult the section 1.4 of Security Target [ST].

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats, and organizational security policies, is defined in sect. 3 of the Security Target [ST].

The TOE security functions are described in detail in section 7 of the Security Target [ST]. The most significant aspects are summarized below:

- **Security audit**: The log module records operations and events that occur on the appliance where the TOE runs. Key elements of log messages are timestamp, host name, Huawei identity, version, module name, severity, brief description. Information hierarchy is designed to help the user roughly differentiate between information about normal operation and information about faults.

- **Cryptographic support**: The TOE provides cryptography in support of secure connections that includes remote administrative management:

    - (Deterministic Random Bit Generator) DRBG – Used in session establishment of TLS and SSH.

    - (Rivest-Shamir-Adleman) RSA – Used for signature verification and generation in session establishment of TLS and SSH.

    - (Secure Hash Algorithm) SHA – Used to provide cryptographic hashing services.

    - (Hash Based-Message Authentication Code) HMAC-SHA – Used to provide integrity verification and authentication.

    - (Advanced Encryption Standard) AES – Used to encrypt traffic transmitted through TLS and SSH.

  - (Elliptic Curve Cryptography) ECC – Used for signature verification and generation in session establishment of (Secure Shell) SSH.

- **Identification and authentication**: The authentication functionality provides validation by user's account name and password. Public key authentication is supported for SSH users. Detailed functionalities, for example max idle-timeout period, max log-in attempts, UI lock, user kick out, can be configured by only an administrator according to networking environment, customized security considerations.

- **Secure Management**: The TOE restricts the ability to determine the behaviour of and modify the behaviour of the function's transmission of audit data to the security administrator. Only the security administrator can manage the cryptographic keys. Only the security administrator has the right of opening/closing the security services and creation/deletion/modification of the user accounts.

- **Protection of the TSF**: The TOE protects the pre-shared keys, symmetric keys, and private keys from reading them by an unauthorized entity. The TOE stores the users or administrator passwords in non-plaintext and non-reversible form preventing them from reading. The TOE verifies the packet before their installation and uses the digital signature. The TOE provides Reliable Time-stamps functionality for internal use (e.g., for associating a time stamp to a log) and synchronize its time using a NTP server as a reliable source of time. The TOE performs self-test for integrity of the software and the cryptographic functions upon each boot. The TOE supports installation of software updates by administrators after a successful verification of their authenticity using secure and strong cryptographic algorithms based on digital signatures.

- **TOE access**: The TOE supports to terminate the session when a session is inactive for the configured period of time. Administrators can use a command to terminate their interactive session in the TOE. The TOE provides default access banners, after the user login the TOE.

- **Trusted path and channels authentication**: The TOE supports the trusted connections using TLS for the communication with the audit (syslog) server. The TOE supports the trusted connections using SSH for the communication with the remote users.

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 of 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].

The ST includes the following extended functional requirements:

- **FAU_STG_EXT.1**: This component is a member of a new family (FAU_STG_EXT – Security audit event storage) which exists within an existing CC Part 2 class (FAU – Security Audit). FAU_STG_EXT is described as specification for securely transmitting audit data between the TOE and an external IT entity.

- **FCS_RBG_EXT.1**: This component is a member of a new family (FCS_RBG – Random Bit Generation) which exists within an existing CC Part 2 class (FCS – Cryptographic Support). FCS_RBG_EXT is described as specification for random bit/number generation.

- **FCS_SSHC_EXT.1**: This component is a member of a new family (FCS_SSHC – SSH Client Protocol) which exists within an existing CC Part 2 class (FCS – Cryptographic Support). FCS_SSHC_EXT is described as specification for a client to offer SSH to protect data between a client and the server using the SSH protocol.

- **FCS_SSHS_EXT.1**: This component is a member of a new family (FCS_SSHS – SSH Server Protocol) which exists within an existing CC Part 2 class (FCS – Cryptographic Support). FCS_SSHS_EXT is described as specification for a server to offer SSH to protect data between a client and the server using the SSH protocol.

- **FCS_TLSC_EXT.1, FCS_TLSC_EXT.2**: These components are members of a new family (FCS_TLSC – TLS Protocol) which exists within an existing CC Part 2 class (FCS – Cryptographic Support). FCS_TLSC_EXT is described as specification for a client to use TLS to protect data between the client and a server using the TLS protocol.

- **FIA_PMG_EXT.1**: This component is a member of a new family (FIA_PMG – Password Management) which exists within an existing CC Part 2 class (FIA – Identification and Authentication). FIA_PMG_EXT is described as specification for ensuring that strong passwords and passphrases can be chosen and maintained by administrative users.

- **FIA_UIA_EXT.1**: This component is a member of a new family (FIA_UIA – User Identification and Authentication) which exists within an existing CC Part 2 class (FIA – Identification and Authentication). FIA_UIA_EXT is described as specification of displaying a warning banner in accordance with FTA_TAB.1 prior to the user being authenticated and allowing TSF-mediated actions after the user being authenticated.

- **FIA_X509_EXT.1, FIA_X509_EXT.2**: These components are a member of a new family (FIA_X509 – Authentication using X.509 Certificates) which exists within an existing CC Part 2 class (FIA – Identification and Authentication). FIA_X509_EXT is described as specification of the behaviour, management, and use of X.509 certificates for functions to be performed by the TSF.

- **FIA_UAU_EXT.2**: This component is a member of a new family (FIA_UAU_EXT – User Authentication) within an existing CC Part 2 class (FIA – Identification and Authentication). FIA_UAU_EXT is described as specification for a locally based authentication mechanism to administrative users.

- **FPT_SKP_EXT.1**: This component is a member of a new family (FPT_SKP – Protection of TSF Data (for reading all pre-shared, symmetric and private keys)) which exists within an existing CC Part 2 class (FPT – Protection of the TSF)). FPT_SKP_EXT is described as specification for managing and protecting TSF data, such as cryptographic keys.

- **FPT_APW_EXT.1**: This component is a member of a new family (FPT_APW – Protection of Administrator Password) which exists within an existing CC Part 2 class (FPT – Protection of the TSF). FPT_APW_EXT is described as specification for protecting plaintext credential data such as passwords from unauthorized disclosure.

- **FPT_TST_EXT.1**: This component is a member of a new family (FPT_TST_EXT – TSF Self Test) within an existing CC Part 2 class (FPT – Protection of the TSF). FPT_TST_EXT is described as specification for self-testing the TSF.

- **FPT_TUD_EXT.1:** This component is a member of a new family (FPT_TUD – Trusted Update) which exists within an existing CC Part 2 class (FPT – Protection of the TSF). FPT_TUD_EXT is described as specification for updating the TOE firmware and/or software.

- **FPT_STM_EXT.1:** This component is a member of a new family (FPT_STM_EXT – Time Stamps) which exists within an existing CC Part 2 class (FPT – Protection of the TSF). FPT_STM_EXT is described as specification for extending FPT_STM requirements by describing the source of time used in timestamps.

- **FTA_SSL_EXT.1:** This component is a member of a new family (FTA_SSL_EXT – TSF-initiated Session Locking) which is based on an existing family from CC Part 2 (FTA_SSL – Session Locking and Termination) within an existing CC Part 2 class (FTA – TOE Access). FTA_SSL_EXT is described as specification for TSF-initiated and user-initiated locking, unlocking, and termination of interactive sessions.

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 (Laboratorio per la Valutazione della Sicurezza, LVS) atsec information security s.r.l.

The evaluation was completed on 16 March 2023 with the issuance by LVS of the Evaluation Technical Report (ETR) [ETRv2], which was approved by the Certification Body on 14 April 2023.

An additional ETR ([ETRv3]) was delivered on 27 April 2023 including minor editorial 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. 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; it remains a probability (the smaller, the higher the assurance level) 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 [ETRv2] issued by the LVS atsec information security s.r.l. and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE Huawei NetEngine 8000 Series Routers' Software V800R022C00SPC600 meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL2, 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 1 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 EAL2, augmented with ALC_FLR.2.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
ST introduction	ASE_INT.1	Pass
Conformance claims	ASE_CCL.1	Pass
Security problem definition	ASE_SPD.1	Pass
Security objectives	ASE_OBJ.2	Pass
Extended components definition	ASE_ECD.1	Pass
Derived security requirements	ASE_REQ.2	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Security-enforcing functional specification	ADV_FSP.2	Pass
Basic design	ADV_TDS.1	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
Use of a CM system	ALC_CMC.2	Pass
Parts of the TOE CM coverage	ALC_CMS.2	Pass
Delivery procedures	ALC_DEL.1	Pass
Flaw reporting procedures	*ALC_FLR.2*	*Pass*
Test	**Class ATE**	Pass
Evidence of coverage	ATE_COV.1	Pass

Assurance classes and components		Verdict
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 1 - 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 NetEngine 8000 Series Routers' Software V800R022C00SPC600 are suggested to properly understand the specific purpose of certification 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 the Organizational Security Policies and the Assumptions described, respectively, in section 4.3.2 and 4.3.3 of the Security Target [ST] are respected.

This Certification Report is valid for the TOE in its evaluated configuration: Annex A – Guidelines for the secure usage of the product includes a number of recommendations related to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([PRE], [OPE]). It is worth highlighting that the LVS recommends to include in the operational environment a firewall with a rule to filter traffic towards/from the TOE, as discussed in section 11.4.

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

The following table contains the items that comprise the different elements of the TOE and non-TOE components, including software and hardware.

#	Type	Identifier	Release	Form of Delivery
Huawei NetEngine 8000 Series Routers' Software version V800R022C00SPC600				
1	TOE Software	NetEngine8000-Series-X_V800R022C00SPC600.cc	X_V800R022C00SPC600	Digital Delivery
2	Non-TOE hardware	NetEngine 8000	NetEngine 8000 X4, X8, X16	Express Shipping

Table 2 – Scope of supply

The TOE contains the following English-guidance documentation reference:

- [OPE] Huawei NetEngine 8000 Series Routers' Software V800R022C00 Operational User Guidance V1.3.
- [PRE] Huawei NetEngine 8000 Series Routers' Software V800R022C00 Preparative Procedures V1.6.
- [SOF_UPG] - Huawei NetEngine 8000 Series Router's Software Upgrade Guide 1.2.pdf. This document provides instructions on how to upgrade the router's software, including guidance on precautions, preparation process, verification process, rollback process, troubleshooting, etc.
- [SIG_VER] - Signature Verification Guide. This document describes OpenPGP signature tools, and verification process.

Since the TOE is entirely composed of software, a cryptographic signature verification is employed to ensure that tampering or masquerading can be detected.

The information provided for the acceptance procedures clearly states that users always need to download the TOE software from the support website (1), check the integrity when installing the product (2) and verify the software version (section 9.2).

In [PRE], chapter 3 “Secure Acceptance by User”, subsection "Software Identification” the developer provided the following two-phase procedure:

(1) Downloading the Software Package

This phase listed the steps that the users have to follow to download the software package from the Huawei Support website: https://support.huawei.com/carrierindex.

(2) Verification of integrity and authenticity of the Software Package

This phase states that, to prevent network security threats caused by malicious tampering or damage during installation package transfer, the users have to verify the integrity of an installation package after obtaining it. Deployment can be started only after the package passes the verification. The procedure is summarized as follow:

1. Obtain the PGPVerify tool
2. Obtain the public key file
3. Import the public key
4. Run the # *gpg —fingerprint* command to check the public key is successfully imported
5. Verify the public key
6. Obtain the software package and signature file Huawei support website
7. Verify the signature
8. Verify the SHA256 values of the TOE software file with the values stated in the section 1.4.3 TOE Physical Scope of the [ST].

The installer will verify the digital signature on the package and the product version. The software package that fails verification is deemed as an illegal package and cannot be used by the system. PGPVerify proprietary tool is used by the installer to simplify the verification the digital signature.

More information on this can be found also in [SIG_VER] where step by step guides for using GnuPG (Linux), Gpg4Win (Windows) and PGPVerify (Windows&Linux) exist, each with "Background", "Prerequisites" and "Verifying the Signature" sections.

9.2 Identification of the TOE

Identification of the TOE version is performed at the end of the installation procedure reported in section 9.3 and described in detail in [PRE].

Users must ensure that the product software which has been downloaded and installed is the correct version under which the TOE has been evaluated. For this purpose, in [PRE] regarding Software Version Identification the user is provided with the following advice:

"*You can obtain the product software version by running the **display version** [**slot** slot-id] command to view the version information. See "Reference/Commands Reference/User*

Commands Manual/System Management Commands/Update and Maintenance Commands/display version" for further details about this command.

*The returned value must be **V800R022C00SPC600** matching with that version of the TOE in the ST*."

9.3 Installation, initialization, and secure usage of the TOE

TOE installation, configuration and operation should be done 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]:

- Huawei NetEngine 8000 Series Routers' Software V800R022C00 Operational User Guidance V1.3.pdf [OPE].
- Huawei NetEngine 8000 Series Routers' Software V800R022C00 Preparative Procedures V1.6.pdf [PRE].

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product Huawei NetEngine 8000 Series Routers' Software with Huawei NetEngine 8000 Series version V800R022C00SPC600, developed by Huawei Technologies Co., Ltd.

The TOE has been tested on the supporting hardware NetEngine 8000 X4 upgraded to the TOE version of the software. The model tested represents the TOE system firmware supported by all the hardware platform models, that is Huawei NetEngine 8000 X4/X8/X16 Routers. All TOE models use the same V800R022C00SPC600 TOE version.

The evaluator, supported by an equivalency analysis, determines that the test of TSFs performed on the X4 model are representatives of tests performed on X8 and X16 models.

The TOE works in an operational environment where the following components are available:

- **Management Server**: any Management workstation with an SSH client installed that is used to establish a protected channel with the TOE.
- **Local Console** any Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
- **NTP Server**: the TOE supports secure communications with an NTP server. In the evaluated configuration the TOE operates only as NTP Client to obtain a reliable source of time from the non-TOE NTP Server located in the operational environment to support the internal timestamp function. The TOE provides timestamps for internal use only.
- **Syslog Server:** any syslog server to which the TOE transmits syslog messages.

Even if the TOE also supports the integration with a RADIUS AAA server providing user authentication to administrators, such setup is not covered by the evaluated configuration.

In evaluated configuration the administrators only authenticate against the TOE without relying on an external RADIUS AAA server.

For more details, please refer to section 1.3.4 of the Security Target [ST].

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities. For the assurance level EAL2, augmented with ALC_FLR.2, such activities include the following three steps:

- evaluation of the tests performed by the Developer in terms of coverage;
- execution of independent functional tests by the Evaluators;
- execution of penetration tests by the Evaluators.

11.1 Test configuration

For the execution of test activities a test environment was set up at the LVS site.

The evaluator verified the system configuration according to the documentation provided by the developer ([PRE]) and the test plan. The evaluator then concluded that the test configuration is consistent with [ST].

The hardware platform used for testing is the Huawei NetEngine 8000 X4 Router with V800R022C00SPC600 TOE version.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The evaluator noted that for the choice of tests to be performed on the TOE, the developer used the approach of taking [CPP_ND] as a blueprint, thus choosing threats, assumptions, and policies, using security objectives, and consequently using SFR. [CPP_ND] provides for specific test for each SFR included in [ST]. The evaluator checked that the tests performed by the Developer are the same of those listed in [CPP_ND].

This approach of the developers ensures the repeatability and reproducibility of the actions performed by the evaluator.

The tests suite was designed to ensure the TOE fulfils the security objectives for the TOE as established in [ST] section 4.1 "Security objectives for the TOE". This is evidenced in the test descriptions provided throughout the test case guides which not only include the expected test results but also test results and evidence. All the tests were executed successfully according to the expected tests results. The test systems were configured according to the ST and the instructions in [PRE].

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 developer provided tests results which were generated using the TOE in its evaluated configuration as stated in [PRE]. All test results from the tested environment show that the expected test results are identical to the actual test results, therefore all tests can be deemed to have expected outcome.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Testing approach

In addition to running the chosen subset of the developer tests, the evaluator devised a test subset with some test derived from the Developer test set and other that are completely independents.

The evaluator has chosen the following test cases:

- variants of a cryptographic-test case to verify the management of maximum length of packets, to verify the correct implementation of the cipher suite of TLS,
- a variant of a cryptographic operation test cases by performing various tests with vectors generated by LVS,
- a variant of identification and authentication test case to test passwords management and X.509 certificates validation,
- a variation of the TOE access test case.

11.3.2 Test results

During the evaluator's review of the test cases provided by the developer, the evaluator gained confidence in the developer testing effort and the depth of test coverage in the developer supplied test cases. The analysis has shown a very wide coverage of the TSF, therefore the evaluator devised only a small number of developer test cases.

All tests passed successfully.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked on the same TOE sample already used for the functional test activities, verifying that the test configuration was consistent with the version of the TOE under evaluation.

Multiple public searches were conducted between 2023-01-23 and 2023-01-26, with different keyword combinations (e.g. Huawei NetEngine Router and VRP, SSH, TLS, NTP service, etc.) to identify the publicly available bugs and vulnerabilities for the TOE. For this phase public vulnerability databases and research papers were reviewed as well.

The following list shows the areas of closer examination the evaluator focused on:

- SSH MITM (Man In The Middle).

- SSH Fuzzing using different tools.
- Port Scan against TOE.
- UDP Fuzzing.

The evaluator considering the type of product set up a TCP and UDP port scan via Nmap. The obtained results are as follows:

- TCP port 22 open for SSH service as expected, no other ports open.
- UDP ports 7, 13, 19 and 56304.

Regarding UDP, the evaluator considered the first three ports as known ports:

- 7 - Echo Protocol.
- 13 - Daytime Protocol.
- 19 - CHARGEN (Character Generator Protocol).

The port scan resulted in 3 unexpected UDP open|filtered ports. The Evaluator wrote scripts for each port, with the aim to use the well-known associated service. No response was observed, and traffic was discarded. However, LVS recommends to include in the operational environment a firewall with a rule to filter traffic towards/from the identified ports as a preventive measure.

The Evaluator performed penetration testing to try to bypass security functionalities of the TOE using the tests defined by the above attack scenarios.

Based on the analysis above the evaluator determined that there are 2 residual known vulnerability, that could be exploited only by an attacker with attack potential beyond Basic.