Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1053-2018

for

Huawei NE40E Series Software Consisting of VRP and the Underlying OS, V800R010C00SPC200, V800R010SPH220T

from

Huawei Technologies Co., Ltd.

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1053-2018 (*)

Network Device

Huawei NE40E Series Software Consisting of VRP and the Underlying OS
V800R010C00SPC200, V800R010SPH220T

from	Huawei Technologies Co., Ltd.
PP Conformance:	collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 2018-03-14, NDFW-iTC (Exact conformance)
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations and by Common Criteria Supporting Document: Evaluation Activities for Network Device cPP, version 2.0 + Errata 20180314 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) 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 and Notification. For details on the validity see Certification Report part A chapter 4

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) 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 the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement

Bonn, 26 October 2018

For the Federal Office for Information Security

Bernd Kowalski
Head of Division

L.S.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

Certification....6

1. Preliminary Remarks....6
2. Specifications of the Certification Procedure....6
3. Recognition Agreements....7
4. Performance of Evaluation and Certification....8
5. Validity of the Certification Result....8
6. Publication....9

B. Certification Results....10

1. Executive Summary....11
2. Identification of the TOE....12
3. Security Policy....14
4. Assumptions and Clarification of Scope....14
5. Architectural Information....15
6. Documentation....16
7. IT Product Testing....16
8. Evaluated Configuration....18
9. Results of the Evaluation....19
10. Obligations and Notes for the Usage of the TOE....20
11. Security Target....20
12. Definitions....20
13. Bibliography....22

C. Excerpts from the Criteria....24

D. Annexes....25

Certification

1. Preliminary Remarks

Under the BSIG1 Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

2 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

3 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045.
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogisportal.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

[4] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

This certificate is recognized under CCRA-2014 for all assurance components selected.

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Huawei NE40E Series Software Consisting of VRP and the Underlying OS, V800R010C00SPC200, V800R010SPH220T has undergone the certification procedure at BSI.

The evaluation of the product Huawei NE40E Series Software Consisting of VRP and the Underlying OS, V800R010C00SPC200, V800R010SPH220T was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 25 October 2018. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Huawei Technologies Co., Ltd.

The product was developed by: Huawei Technologies Co., Ltd.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 26 October 2018 is valid until 25 October 2023. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product Huawei NE40E Series Software Consisting of VRP and the Underlying OS, V800R010C00SPC200, V800R010SPH220T has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Huawei Technologies Co., Ltd.

Bantian Longgang
Shenzhen 518129
P.R. China

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is defined as Huawei NE40E Series Software Consisting of VRP and the Underlying OS, version “V800R010C00SPC200” and patch version “V800R010SPH220T”, running on hardware models NE40E-X3A and NE40E-X16A. The TOE is a network device that is connected to the network and has an infrastructure role within the network.

The usage of the TOE is the following:

- The TOE supports username/password, or public-key authentication mode. Only users that are authenticated can access the TOE and its command line interface.
- The TOE is accessed by CLI locally or by a Network Management Server (NMS) remotely over SSH so that a secure channel is established to protect the data between TOE and NMS.
- For secure transmission of audit information between the TOE and the Syslog server a secure TLS channel is used.
- The TOE supports digital signature verification for software. Each of the software package or patch package released by Huawei includes a unique digital signature. When an NMS distributes the package to NE40E, the TOE will verify the online digital signature before updating. The verification of the digital signature demonstrates the integrity and authenticity of the package. The package is only processed further after successful verification of the digital signature, otherwise the package will be discarded without processing.

The TOE provides security services onto a single and secure device.

The TOE is part of the overall NE40E series routers product and is deployed at the edge of IP backbone networks, IP metropolitan area networks (MANs), and other large-scale IP networks. It consists of both hardware and software, providing network traffic processing capacity. The TOE is software only and consists of the Versatile Routing Platform (VRP) and the underlying Operating System (OS). Network traffic is processed and forwarded by the underlying hardware according to routing decisions downloaded from VRP. The NE40E runs with the VRP developed by Huawei. VRP provides extensive security features. These features include different interfaces with according access levels for administrators, enforcing authentications prior to establishment of administrative sessions, auditing of security-relevant management activities.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 2018-03-14, NDFW-iTC [8].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1, as well as ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_SPD.1, ASE_TSS.1.

The assurance requirements ASE_OBJ.2 and ASE_REQ.2 are not part of the ST and of this certificate, in order to claim exact conformance to the NDcPP [8]. However they were considered during the evaluation by refering to an addendum to the ST "Huawei NE40E

Series Software Consisting of VRP and the Underlying OS, Security Target - ASE_OBJ.2, ASE_REQ.2 Addendum" [9].

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality / ST chapter	Addressed issue
7.1	Security Audit (FAU)
7.2	Cryptographic Support (FCS)
7.3	Identification and Authentication (FIA)
7.4	Security management (FMT)
7.5	Protection of the TSF (FPT)
7.6	TOE Access (FTA)
7.7	Trusted path/channels (FTP)

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1 . Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3 and 4.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

Huawei NE40E Series Software Consisting of VRP and the Underlying OS,
V800R010C00SPC200, V800R010SPH220T

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	TOE / : Huawei NE40E Series Software Consisting of VRP and the Underlying OS	SW: V800R010C00SPC200 Filename: V800R010C00SPC200-OC-NE-X3A.cc SHA256 value: 3f3f7cdf2fc34e9409833fdba57644ced01859324ab3776a60f901ce7f5bb73d HPV: V800R010SPH220T Filename: NE40EV800R010SPH220T.PAT SHA256 value: 9f52bc0e01c94cff5a322c013bcfe8ee1571a92fcd4f9afbd3c4e490100f2450	Download
2	DOC	PD / NE40E Product Documentation Procduct Version: V800R010C00SPC200 [10]	Version 0.2 Filename: NE40E V800R010C00SPC200 Product Documentation 02.chm SHA256 value: 48ad0c9693099ce4df2430276e6247d3070d2ca2784435ece0e0576ad36ca1de	Download
3	DOC	PRE / Huawei NE40E Series Product V800R010C00SPC200 Preparative Procedures Product Version: V800R010C00SPC200 [11]	Version 0.7	Secure Shipping
4	DOC	OPE / Huawei NE40E Series Product V800R010C00SPC200 Operational user Guidance Product Version: V800R010C00SPC200 [12]	Version 0.6	Secure Shipping
5	DOC	C&R / NDcPP Universal Service Router NE40E V800R010C00SPC200 Configuration and Reference [13]	Version 0.4	Secure Shipping

Table 2: Deliverables of the TOE

Please note: The Preparative Procedures Guidance document [11] gives information on the Delivery Interfaces and Acceptance Procedures at delivery but Assurance Family Delivery was not within the scope of the evaluation.

For TOE identification, the TOE supports the command "*Display version*" on the command prompt to show the TOE version and the patch version information. The command can be entered in the status after the secure installation. The command is registered at command level 1.

The response of the TOE to the command starts as follows:

Huawei Versatile Routing Platform Software

*VRP (R) software, Version 8.160 (**NE40E V800R010C00SPC200**)*

[…]

*Patch Version: **V800R010SPH220T***

For identification of the TOE the user shall only consider the information that is highlighted in bold in the above example printout. The version information given in bold is the detailed version information that reflects the unique TOE reference.

The unique reference for the TOE is *V800R010C00SPC200* with Patch Version *V800R010SPH220T*.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the issues as described in detail in the ST, chapter 7 as functional security policies enforced by the TOE and can be summarized as

- Security Audit,
- Cryptographic Support,
- Identification and Authentication,
- Security Management,
- Protection of the TSF,
- TOE Access,
- Trusted Path/Channels.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The list of objectives which have to be met by the environment is to be found in the Security Target [6], chapter 4.1. For convenience, the list is reproduced here:

- OE.PHYSICAL: Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

- OE.NO_GENERAL_PURPOSE: There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- OE.NO_THRU_TRAFFIC_PROTECTION: The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
- OE.TRUSTED_ADMIN: Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
- OE.UPDATES: The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- OE.ADMIN_CREDENTIALS_SECURE: The Administrator’s credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
- OE.RESIDUAL_INFORMATION: The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5. Architectural Information

The TOE is composed of two parts: VRP and the underlying OS.

The underlying OS is the Windriver Linux and the Real Time Operating System (RTOS).

The OS provides basic services including memory management, scheduling management, file management, and device management.

The VRP is a new-generation network operating platform, which has a distributed, multiprocess, and component-based architecture. It builds upon the hardware development trend and will meet carriers' exploding service requirements for the next five to ten years.

The VRP software is responsible for functional management, routing information generation, receiving generated routing information and formatting them into hardwarespecific data to direct traffic forwarding.

Figure 1-2 of the Security Target [6] depicts the detailed TOE Software Architecture.

In that figure one can see that six logical planes are defined for the Software Architecture. They are:

- 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.
- 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.
- System Service Plane (SSP), implements system internal scheduling, communication, management of signals, events, timers, etc. Communication with Virtual Path is also implemented at this plane.

- Data Plane (DP), implements traffic forwarding. Forwarding related information, e.g. routing information, ARP table entry, static MAC table entry are generated in GCP and downloaded via communication channel provided by SSP.
- Operating System (OS), provides hardware and software resource management. The underlying OS is the Windriver Linux and the Real Time Operating System (RTOS). The Real Time Operating System (RTOS) manages underlying hardware resources, such as the CPU, memory, storage devices, network devices, and other hardware. The RTOS is developed by Huawei.

Please note that VRP consists of SMP, SCP, GCP, DP and SSP.

SMP, SCP, SSP and OS are in the scope of the TOE. GCP and DP are not in the scope of the TOE. SMP, SCP, GCP are hosted in the MPU. DP is hosted in the LPU. SSP and OS are hosted in the both MPU and LPUs. Please see also the Security Target [6], chapter 1.4.1.

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

Independent Evaluator Testing

The independent testing was partially performed using the developer's testing environment, partially using the test environment of the ITSEF. The overall test result is that no deviations were found between the expected and the actual test results.

The evaluator examined the test coverage achieved by Network Device cPP Supporting Document (NDcPP/SD) testing and focused on the functional areas that were not fully covered by the NDcPP/SD testing efforts. Moreover, the evaluator devised and conducted further functional tests on a pre-release version of the TOE running on the X16A platform in the developer's test environment.

The TOE has also been tested on the X3A platform. A selection of standard test tools has been used, including:

- SSH clients,
- Packet capture tool,
- Cryptographic key generator,
- C Compiler and Linker.

The functional tests on the X3A platform have been mainly focused on the following TOE functionalities:

- SSH server behavior when processing large packets,
- SSH configuration,

- SSH rekeying,
- User identification & authentication,
- User authorization,
- Audit.

The overall test result is that no deviations were found between the expected and the actual test results.

Penetration Testing

The penetration testing was partially performed on the X16A platform in the developer's test environment, and partially on the X3A platform in the test environment of the ITSEF. The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential Basic was actually successful.

The evaluator examined public information to identify potential vulnerabilities in the TOE. As a result from this analysis, the evaluator devised penetration tests and performed these tests on the TOE running on the X3A platform using the test environment of the ITSEF. Further penetration tests were performed on a pre-release version of the TOE running on the X16A platform.

The TOE has been tested on the X3A platform, and supplemental tests have been performed on a pre-release version of the TOE on the X16A platform. A selection of standard test tools has been used, including:

- SSH clients,
- Port scanner,
- Packet capture tool,
- Packet generation tool, and
- Exploit framework.

The attack scenarios that have been tested target the following TOE properties:

- Available network services and protocols provided by the TOE in its certified configuration,
- Configuration and robustness of the SSH server, and
- Configuration of user accounts and privileges.

The penetration tests focus on the X3A platform was on the following Security Functional Requirements:

- FCS_SSHS_EXT.1 (SSH Server Protocol),
- FMT_MTD.1/CoreData (Management of TSF Data),
- FTP_TRP.1/Admin Trusted Path (Refinement).

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential Basic was actually successful in the TOE's operational environment as defined in the Security Target [6] provided that all measures required by the developer are applied.

The TOE has passed the evaluation tests. Overall, the tests confirm the TOE functions as described in the developer´s documents. With the result of the vulnerability analysis the evaluator has determined that the TOE is free of vulnerabilities, which can be exploited by an attacker with Basic attack potential.

8. Evaluated Configuration

This certification covers the TOE Huawei NE40E Series Software Consisting of VRP and the Underlying OS, V800R010C00SPC200, V800R010SPH220T of which “V800R010C00SPC200” is the TOE version and “V800R010SPH220T” is the patch version. The Preparative Procedures document [11] has identified only one possible configuration of the TOE under evaluation, which is the TOE being only one instance. The configuration as multiple instances was not included in the evaluation.

The operational environment of the TOE in its evaluated configuration can be summarized by the following hardware, software, and firmware components which are required in the operational environment of the TOE:

- NE40E-X3A, NE40E-X16A: The TOE runs on these hardware platforms.
- Network Management Server: This includes any Management workstation with a SSH client installed that is used to establish a protected channel with the TOE.
- Local Console: This includes 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.

The following hardware, software, and firmware components are optional based on the claims made in the Security Target:

- RADIUS AAA Server: This RADIUS AAA server provides user authentication. The TOE correctly leverages the services provided by this RADIUS AAA server to provide authentication to administrators.
- CRL Distribution Point: CRL should be downloaded from CRL Distribution Point. Then this downloaded CRL should be uploaded into the TOE.
- NTP: The TOE supports secure communications with an NTP server in order to synchronize the date and time on the TOE with the NTP server’s date and time. When the TOE acts as NTP server, it receives NTP request from client and send timestamp to the client.
- Syslog Server: This includes any syslog server to which the TOE would transmit syslog messages.

Please read the Security Target [6] chapter 1.3.3 for the description of Non TOE Hardware and Software, the Security Target [6] table 1-2 for the description of evaluated and not evaluated modules, Security Target [6] chapter 1.4.2 and 1.4.3 for the physical and logical scope of the TOE. The Security Target [6] chapter 1.4.4 defines the TOE as a standalone TOE, i.e. it is not a distributed TOE in the sense of the collaborative Protection Profile [8], chapter 3.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used, extended by Scheme Interpretations and by the assurance activities specified in Common Criteria Supporting Document: Evaluation Activities for Network Device cPP, version 2.0 + Errata 20180314 [8] and showed that the TOE is conformant to the collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018 [8], and that the assurance activities specified in the Supporting Document [8] had been performed appropriately.

For RNG assessment the scheme interpretations AIS 20 (see [4]) and [8] (for the entropy assessment) were used.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components claimed in the Security Target [6], chapter 2.2 and 6.2 and defined in the CC (see also part C of this report)

Please note that the ST [6] lists threats but the cPP [8] excludes an analysis if those threats have actually been countered by the TOE. Please also note that there have no objectives for the TOE been claimed. The cPP author chose an evaluation scope that excludes the analysis if and how SFRs are traced back to security objectives for the TOE and if they counter all threats, and if and how security objectives for the TOE are traced back to the threats and OSPs, and if security objectives for the TOE are defined. To include these aspects into this evaluation, the developer provided an addendum to the ST (in order to not interfere with the exact conformance of the ST to the NDcPP): "Huawei NE40E Series Software Consisting of VRP and the Underlying OS, Security Target - ASE_OBJ.2, ASE_REQ.2 Addendum" [9] with the required information that allow the evaluation of the aforementioned aspects, i.e. to consider the assurance families ASE_REQ.2 and ASE_OBJ.2 in the evaluation.

The evaluation has confirmed:

- PP Conformance: collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 2018-03-14, NDFW-iTC [8]
- for the Functionality: Exact PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant

Please note that Exact Conformance, as a subset of Strict Conformance as defined by the CC, is defined as the ST containing all of the SFRs in section 6 of the NDcPP [8] (these are the mandatory SFRs), and potentially additional SFRs from Appendix A of the NDcPP [8] (these are optional SFRs) or Appendix B of the NDcPP [8] (these are selection-based SFRs, some of which will be mandatory according to the selections made in other SFRs). While iteration is allowed, no additional requirements (from the CC parts 2 or 3, or definitions of extended components not already included in the cPP) are allowed.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The table presented in chapter 8 of the Security Target [6] gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. All Cryptographic Functionality reach a *Security Level above 100 Bits.*

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

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

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a finalized version of the working version of the Security Target [6] that was used for the performed evaluation. Their contents are identical, only some formattings, version histories, and document classifications differ.

12. Definitions

12.1. Acronyms

AAA Authentication Authorization Accounting

AIS Application Notes and Interpretations of the Scheme

ARP Address Resolution Protocol

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CA	Certificate Authority
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
cPP	Collaborative Protection Profile
CRL	Certificate Revocation List
DP	Data Plane
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCP	General Control Plane
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LPU	Line Process Unit
MAC	Media Access Control
MAN	Metropolitan Area Network
MPU	Main Processing Unit
ND	Network Device
NMS	Network Management Server
NTP	Network Time Protocal
OS	Operating System
PP	Protection Profile
RTOS	Real Time Operating System
SAR	Security Assurance Requirement
SCP	Service Control Plane
SFP	Security Function Policy
SFR	Security Functional Requirement
SMP	System Manage Plane
SSH	Secure Shell
SSP	System Service Plane
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation

TSF TOE Security Functionality

VRP Versatile Routing Platform

12.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017,
http://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target of Huawei NE40E Series Software Consisting of VRP and the Underlying OS BSI-DSZ-CC-1053-2018, Version 2.5, Date 2018-10-23, Huawei Technologies Co., Ltd. (confidential working document) and Security Target Lite of Huawei NE40E Series Software Consisting of VRP and the Underlying OS BSI-DSZ-CC-1053-2018, Version 2.5, Date 2018-10-23, Huawei Technologies Co., Ltd. (public finalized document)

[7] Evaluation Technical Report for Huawei NE40E Series Software Consisting of VRP and the Underlying OS V800R010C00SPC200, V800R010SPH220T, BSI-DSZ-CC-1053-2018, Version 2.0, Date 2018-10-24, TÜV Informationstechnik GmbH, (confidential document)

[8] collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 2018-03-14, NDFW-iTC + Common Criteria Supporting Document: Evaluation Activities for Network Device cPP, version 2.0 + Errata 20180314

[9] Huawei NE40E Series Software Consisting of VRP and the Underlying OS, Security Target - ASE_OBJ.2, ASE_REQ.2 Addendum, Version 0.4, Date 2018-10-02, Huawei Technologies Co., Ltd.

[10] NE40E Product Documentation Procduct Version: V800R010C00SPC200, Version 0.2, Date 2018-04-10, Huawei Technologies Co., Ltd.

[11] Huawei NE40E Series Product V800R010C00SPC200 Preparative Procedures Product Version: V800R010C00SPC200, Version 0.7, Date 2018-10-02, Huawei Technologies Co., Ltd.

[12] Huawei NE40E Series Product V800R010C00SPC200 Operational user Guidance Product Version: V800R010C00SPC200, Version 0.6, Date 2018-10-02, Huawei Technologies Co., Ltd.

[13] NDcPP Universal Service Router NE40E V800R010C00SPC200 Configuration and Reference, Version 0.4, Date 2018-09-29, Huawei Technologies Co., Ltd.

[7] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at http://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report