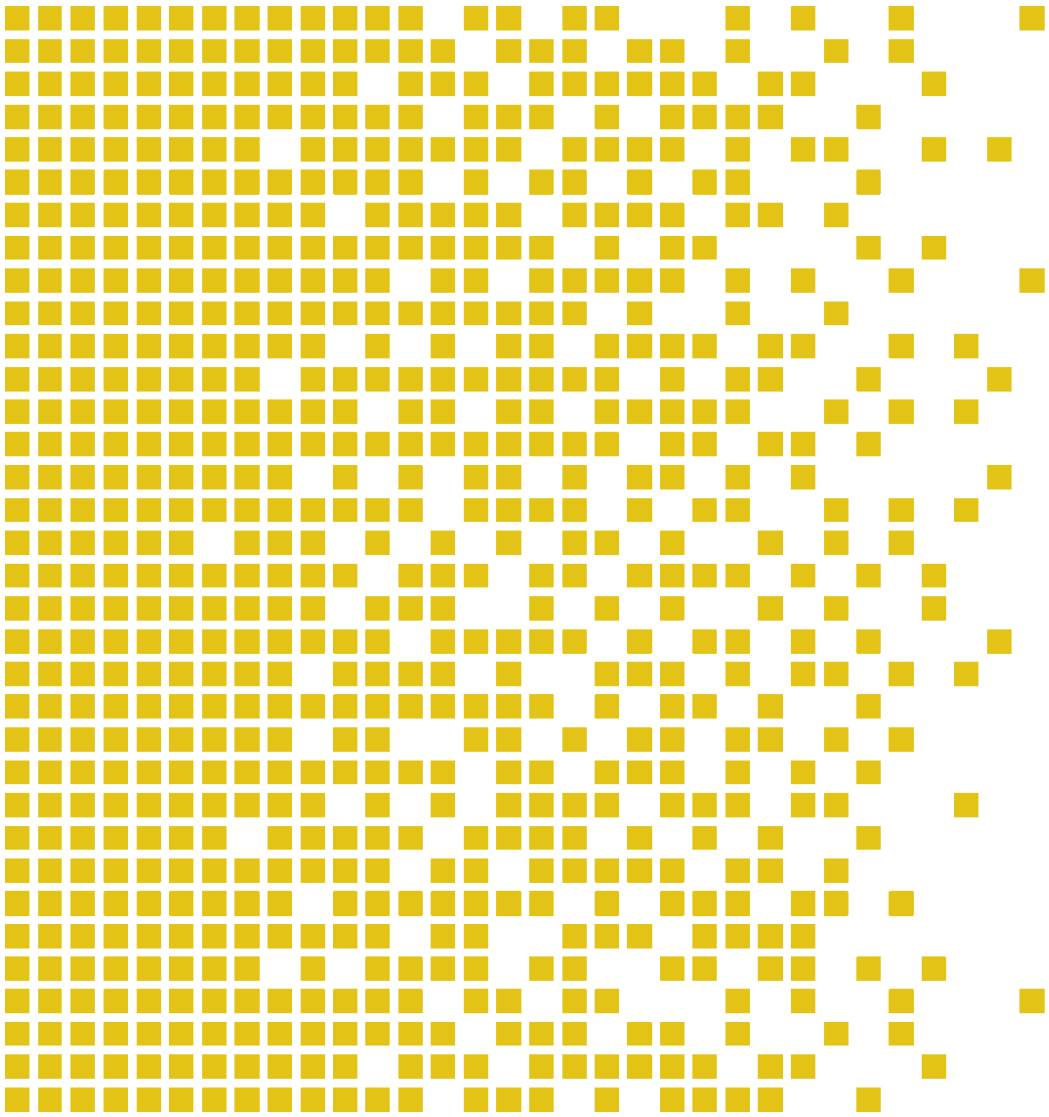
SERTIT-061 CR Certification Report

Issue 1.0 4 June 2015

Huawei NetEngine5000E Core Router V800R006 build C00SPC200



SERTIT, Postboks 814, 1306 Sandvika, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of the CCRA May 23rd 2000. The recognition under the CCRA is limited to EAL 4 and ALC_FLR CC part 3 components.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Agreement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Agreement and is the Party's claim that the certificate has been issued in accordance with the terms of this Agreement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. **

** Mutual Recognition under the SOGIS MRA recognition agreement applies to EAL 3

Contents

1 Certification Statement

Huawei Technologies Huawei NetEngine5000E Core Router is a core router developed to meet the requirement of carrier-class reliability.

Huawei NetEngine5000E Core Router version V800R006 build C00SPC200 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL 3 augmented with ALC_CMC.4 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality in the specified environment when running on the platforms specified in Annex A.

Author	Kjartan Jæger Kvassnes Certifier
Quality Assurance	Arne Høye Rage Quality Assurance
Approved	Øystein Hole Head of SERTIT
Date approved	4 June 2015

2 Abbreviations

AES	Advanced Encryption Standard
CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCC	Cluster Central Chassis
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
CF	Compact Flash
CLC	Cluster Line-card Chassis
CLI	Command Line Interface
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETH	Ethernet
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
GUI	Graphical User Interface
IS-IS	Intermediate System to Intermediate System
LMT	Local Maintenance Terminal
LPU	Line Process Unit
MD5	Message-Digest Algorithm 5
MPU	Main Process Unit
NE	NetEngine
NMS	Network Management Sub-system
OFC	Optical Flexible Card
POC	Point of Contact
PP	Protection Profile
QP	Qualified Participant

RMT	Remote Maintenance Terminal
RSA	Rivest Shamir Adleman
SERTIT	Norwegian Certification Authority for IT Security
SFE	Switch Fabric Extend unit
SFR	Security Functional Requirement
SFU	Switching Fabric Unit
SPM	Security Policy Model
SPU	Service Process Unit
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] Huawei NetEngine5000E Core Router V800R006 Security Target, version 1.6, 28 August 2014.

[2] Common Criteria Part 1, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[3] Common Criteria Part 2, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[4] Common Criteria Part 3, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[7] Evaluation Technical Report Common Criteria EAL3+ Evaluation of the Huawei NetEngine5000E Core Router V800R006, version 1.1, 25 August 2014

[8] NE5000E V800R006C00 Product Manual, v1.0, 15th April, 2014

[9] Common Criteria Security Evaluation – Certified Configuration, v1.3, 5th June 2014

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Huawei NetEngine5000E Core Router version V800R006 build C00SPC200 to the Sponsor, Huawei Technologies, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The version of the product evaluated was Huawei NetEngine5000E Core Router and version V800R006 build C00SPC200.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Huawei Technologies.

Huawei NetEngine5000E Core Router V800R006, which has large capacity and high performance, is developed to meet the requirement of carrier-class reliability. Based on the powerful versatile routing platform (VRP), the NE5000E provides strong switching capabilities, dense ports, and high reliability. NE5000Es mainly serve as super-core nodes on carriers' backbone networks, core nodes on metropolitan area networks (MANs), egresses in large-scale Internet data centres (IDCs), or core nodes on large-scale enterprise networks. NE5000E clusters are positioned as super-core nodes on backbone networks, supporting Layer 3 routing and Multiprotocol Label Switching (MPLS) forwarding. The TOE consists of both hardware and software.

At the core of each chassis is the Versatile Routing Platform (VRP), the software for managing and running the router's networking functionality. VRP provides extensive security features. These features include assigning different privileges to administration users with different privilege levels; enforcing authentications prior to establishment of administrative sessions with the TOE; auditing of security-relevant management activities; as well as the correct enforcement of routing decisions to ensure that network traffic gets forwarded to the correct interfaces.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

The TOE scope is described in the ST[1], chapter 1.4.2 and 1.4.3.

4.4 Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.

4.5 Assurance Level

The assurance incorporated predefined evaluation assurance level EAL 3, augmented by ALC_CMC.4. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

There are no Organizational Security Policies or rules with which the TOE must comply.

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats which these objectives meet and security functional requirements and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered

- T.UnwantedNetworkTraffic

  Unwanted network traffic sent to the TOE will not only consume the TOE's processing capacity for incoming network traffic thus fails to process traffic expected to be processed, but an internal traffic jam might happen when those traffic are sent to MPU from LPU within the TOE. This may cause denial of service of TOE.

  This may further cause the TOE fails to respond to system control and security management operations.

  Routing information exchanged between the TOE and peer routes may also be affected due to the traffic overload.

- T.UnwantedNetworkTraffic

  A user who is not a user of the TOE gains access to the TOE.

- T.UnauthorizedAccess

  A user of the TOE authorized to perform certain actions and access certain information gains access to commands or information he is not authorized for. This threat also includes data leakage to non-intended person or device

- T.Eavesdrop

  An eavesdropper (remote attacker) in the management network served by the TOE is able to intercept, and potentially modify or re-use information assets that are exchanged between TOE and LMT/RMT.

4.9 Threats Countered by the TOE's environment

There are no threats countered by the TOE's environment.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

It is assumed that the TOE (including any console attached, access of CF card) is protected against unauthorized physical access.

The environment is supposed to provide supporting mechanism to the TOE:

- A Radius server or TACACS+ server for external authentication/authorization decisions;
- NMS, logging server and alarm server used for administration of the TOE

In addition, it is assumed the Radius server, and TACACS+ server, and the NMS are all trusted and will not be used to attack the TOE.

- Peer router(s) for the exchange of dynamic routing information;

A remote entities (PCs) used for administration of the TOE.

It is assumed that the ETH interface on MPU in the TOE will be accessed only through sub-network where the TOE hosts. The sub-network is separate from the application (or, public) networks where the interfaces on LPU in the TOE are accessible.

The authorized 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.

4.12 IT Security Objectives

The following objectives must be met by the TOE:

- O.DeviceAvail
  The TOE shall ensure its own availability.
- O.UserAvail
  The TOE shall ensure authorized users can access network resources through the TOE.
- O.DataFilter
  The TOE shall ensure that only allowed traffic goes through the TOE.
- O.Communication
  The TOE must implement logical protection measures for network communication between the TOE and LMT/RMT from the operational environment.

- O.Authorization
  The TOE shall implement different authorization levels that can be assigned to administrators in order to restrict the functionality that is available to individual administrators.
- O.Authentication
  The TOE must authenticate users of its user access.
- O.Audit
  The TOE shall provide functionality to generate audit records for security-relevant administrator actions.

4.13 Non-IT Security Objectives

- OE.NetworkElementsThe operational environment shall provide securely and correctly working network devices as resources that the TOE needs to cooperate with. Behaviors of such network devices provided by operational environment shall be also secure and correct. For example, other routers for the exchange of routing information, PCs used for TOE administration, and Radius and TACACS+ servers for obtaining authentication and authorization decisions.
- OE.Physical The TOE (i.e., the complete system including attached peripherals, such as a console, and CF card inserted in the MPU) shall be protected against unauthorized physical access.
- OE.NetworkSegregation The operational environment shall provide segregation by deploying the Ethernet interface on MPU in TOE into a local sub-network, compared to the interfaces on LPU in TOE serving the application (or public) network.
- OE.Person Personnel working as authorized administrators shall be carefully selected for trustworthiness and trained for proper operation of the TOE.

4.14 Security Functional Requirements

- FAU_GEN.1 Audit data generation
- FAU_GEN.2 User identity association
- FAU_SAR.1 Audit review
- FAU_SAR.3 Selectable audit review
- FAU_STG.1 Protected audit trail storage
- FAU_STG.3 Action in case of possible audit data loss
- FCS_COP.1/AES Cryptographic operation
- FCS_COP.1/3DES Cryptographic operation
- FCS_COP.1/RSA Cryptographic operation
- FCS_COP.1/MD5 Cryptographic operation
- FCS_COP.1/HMAC-MD5 Cryptographic operation
- FCS_COP.1/DHKeyExchange Cryptographic operation
- FCS_COP.1/DSA Cryptographic operation
- FCS_CKM.1/AES Cryptographic key generation
- FCS_CKM.1/3DES Cryptographic key generation
- FCS_CKM.1/RSA Cryptographic key generation

- FCS_CKM.1/HMAC_MD5 Cryptographic key generation
- FCS_CKM.1/DHKey Cryptographic key generation
- FCS_CKM.1/DSA Cryptographic key generation
- FCS_CKM.4/3DES-AES Cryptographic key destruction
- FCS_CKM.4/RSA Cryptographic key destruction
- FCS_CKM.4/HMAC_MD5 Cryptographic key destruction
- FCS_CKM.4/DHKey Cryptographic key destruction
- FCS_CKM.4/DSA Cryptographic key destruction
- FDP_ACC.1 Subset access control
- FDP_ACF.1 Security attribute based access control
- FDP_DAU.1 Basic Data Authentication
- FDP_IFC.1(1) Subset information flow control- CPU-defend
- FDP_IFC.1(2) Subset information flow control- Data plane traffic control
- FDP_IFF.1(1) Simple security attributes - CPU-defend
- FDP_IFF.1(2) Simple security attributes – Data plane traffic control
- FIA_AFL.1 Authentication failure handling
- FIA_ATD.1 User attribute definition
- FIA_SOS.1 Verification of secrets
- FIA_UAU.1 Timing of authentication –Administrator Authentication
- FIA_UAU.5 Multiple authentication mechanisms
- FIA_UID.1 Timing of identification – Administrator Identification
- FMT_MOF.1 Management of security functions behaviour
- FMT_MSA.1 Management of security attributes
- FMT_MSA.3 Static attribute initialization
- FMT_SMF.1 Specification of Management Functions
- FMT_SMR.1 Security roles
- FPT_STM.1 Reliable time stamps
- FTA_SSL.3 TSF-initiated termination
- FTA_TSE.1 TOE session establishment
- FTP_TRP.1 Trusted path
- FTP_ITC.1 Trusted channel

4.15 Security Function Policy

At the core of each chassis is the Versatile Routing Platform (VRP), the software for managing and running the router's networking functionality. VRP provides extensive security features. These features include assigning different privileges to administration users with different privilege levels; enforcing authentications prior to establishment of administrative sessions with the TOE; auditing of security-relevant management activities; as well as the correct enforcement of routing decisions to ensure that network traffic gets forwarded to the correct interfaces.

The Main Processing Units (MPU) integrate the main control unit and the system maintenance unit. The MPU controls and manages the system in a centralized way and is responsible for data exchange.

The Line Processing Units (LPU) are the actual hardware providing network traffic processing capacity. Network traffic is processed and forwarded according to routing decisions downloaded from VRP.

Besides the MPUs and LPUs, there are other types of boards on TOE, such as Switch Fabric Unit (SFU), Switch Fabric Extend unit (SFE), ICU, ECU and OFC. Only MPU and LPU are security relevant.

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the Senior Officials Group Information Systems Security (SOGIS) and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6]. [Note any significant use of Interpretations[7]].

SERTIT monitored the evaluation which was carried out by the Brightsight B.V. Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR)[7] to SERTIT in 25 August 2014. SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3[4]. These classes comprise the EAL 3 assurance package augmented with ALC_CMC.4.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.3	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the guidance listed in the ST[1] chapter 1.4.2 and Preparative Procedures documents [8] provided by the developer. The Common Criteria Security Evaluation – Certified Configuration [9] describes all necessary steps to configure the TOE in the certified configuration.

These documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner.

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. The user should always follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

The evaluators assessed which potential vulnerabilities were already tested by the developer and assessed the results.

The remaining potential vulnerabilities were tested by Brightsight on the final version of the TOE.

5.6 Developer's Tests

The Developer Test Plan consists of 12 different categories of tests of 1-25 tests. The categories are based on major groupings of security functionality, and, in combination cover all SFRs and TSFIs.

5.7 Evaluators' Tests

Since the evaluator has evaluated similar devices from the same developer three times before under supervision of SERTIT, the test plan of the developer has considerably improved and covered all SFRs/TSFIs, and also included all the penetration tests the evaluator has performed form the previous TOEs. As a result, the limited number of the general security functionality tests (such as authentication, authorization, managing) has been sampled, and several penetration tests also has been sampled to ensure the developer performed them correctly. The evaluator also analysed the Developer Test Plan to see where additional ATE tests could be performed, and selected 3 additional tests.

All of these tests were performed at the Huawei premises in Beijing in end May 2014.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Huawei NetEngine5000E Core Router version V800R006 build C00SPC200 meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 3 augmented with ALC_CMC.4 for the specified Common Criteria Part 2 conformant functionality, in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of Huawei NetEngine5000E Core Router version V800R006 build C00SPC200 should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under Section 4.3 “TOE Scope” and Section 5 “Evaluation Findings”.

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

Hardware:

Product Name	Board Name for Order	Description
NE5000E CLC	CR52K-BKPC-36U-8KW	**Feil! Hyperkoblingsreferansen er ugyldig.**
	CR52-MPUB	Main Processing Unit B
	CR5DSFEBA06B	**Feil! Hyperkoblingsreferansen er ugyldig.**
NE5000E CCC	CR55C-BKPA/CR55C-BKPB	**Feil! Hyperkoblingsreferansen er ugyldig.**
	CR5D0MPUA450	**Feil! Hyperkoblingsreferansen er ugyldig.**
	CR55C-MPUA	**Feil! Hyperkoblingsreferansen er ugyldig.**
	CR5DSFUIA050	**Feil! Hyperkoblingsreferansen er ugyldig.**
	CR55C-ICUA	**Feil! Hyperkoblingsreferansen er ugyldig.**
	CR5DECUFA050	**Feil! Hyperkoblingsreferansen er ugyldig.**
	CR5D00FCA060	**Feil! Hyperkoblingsreferansen er ugyldig.**
NE5000E CCC-A	CR5D0MPUB550	Main Processing Unit B550
	CR5D00ICUB50	Internal Communication Unit B50
	CR5DSFUFK050	**Feil! Hyperkoblingsreferansen er ugyldig.**
	CR5M00FCK050	Optical Flexible Card
	CR5B0BKPCD50	NE5000E-CCC-A Integrated Chassis Components DC
	CR5B0BKPCA50	NE5000E-CCC-A Integrated Chassis Components DC

NE5000E-X16	CR5B0BKP1660	**Feil! Hyperkoblingsreferansen er ugyldig.**
	CR5D0MPUB461	**Feil! Hyperkoblingsreferansen er ugyldig.**
	CR5DSFUFA06B	**Feil! Hyperkoblingsreferansen er ugyldig.**
	CR5D0SFUK06B	**Feil! Hyperkoblingsreferansen er ugyldig.**
NE5000E-X16A	CR5B0BKP166A	**Feil! Hyperkoblingsreferansen er ugyldig.**
	CR5B0BKP166B	**Feil! Hyperkoblingsreferansen er ugyldig.**
	CR5D0MPUB560	**Feil! Hyperkoblingsreferansen er ugyldig.**
	CR5DSFUFA06C	**Feil! Hyperkoblingsreferansen er ugyldig.**
	CR5DSFUIK06A	**Feil! Hyperkoblingsreferansen er ugyldig.**
	CR5DSFUIK06B	400G Switch Fabric Unit A for Cluster Chassis Access
NE5000E-X16B	CR5BBKP6BD60	NE5000E-X16B Integrated Chassis Components DC
	CR5BBKP6BA60	NE5000E-X16B Integrated Chassis Components AC
	CR5D0MPUB560	**Feil! Hyperkoblingsreferansen er ugyldig.**
	CR5DSFUIT060	1T Switch Fabric Unit A for Single Chassis
	CR5D00EFMB60	1T 24*40Gbps QSFP+ Interface Board
	CR5D00E8NC60	1T 8*100Gbps CFP2 Interface Board

Software:

Type	Name	Version
Software	Product software	V800R006 build C00SPC200
	VRP	Version 8 Release8 build C00SPC200
	Linux	Version: WRlinux4.1.0.0(CR5D0MPUA450,

		CR5D0MPUB550,CR5D0MPUB461, CR5D0MPUB560) /WRlinux3.0.3.0(CR52-MPUB, CR55C-MPUA)

TOE Documentation

The supporting guidance documents evaluated were:

[a] NE5000E V800R006C00 Product Manual, V1.0

[b] Common Criteria Security Evaluation – Certified Configuration, V1.3

Further discussion of the supporting guidance material is given in Section 5.3 "Installation and Guidance Documentation".

TOE Configuration

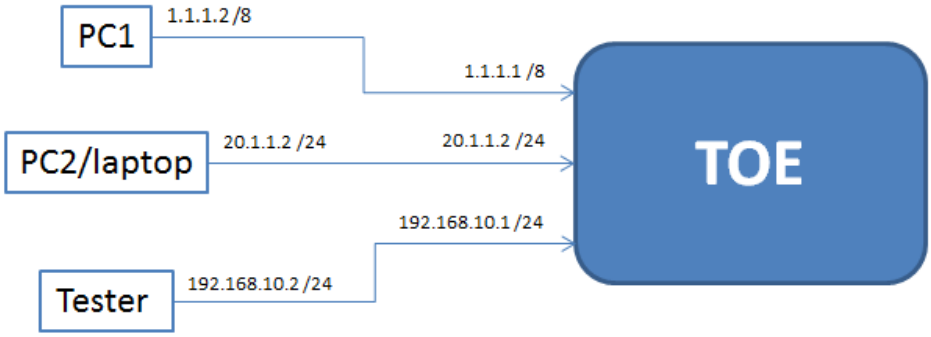
ITEM	IDENTIFIER
HARDWARE	NE5000E-X16A NE5000E-X16 NE5000E CCC-2 with 2 CCCs and four CLCs The LPU used are • 48-port 10GBase LAN/WAN – SFP Integrated Line Process Unit (NE5000E LPUI – 480) • 10-port 10GBase LAN/WAN – XFP Integrated Line Processing Unit (NE5000E LPUI – 100)
SOFTWARE	NE5000E V800R006C00SPC200T[1] and other software (VRP, Linux) listed in section "TOE Identification" configured according to [b].
MANUAL	The appropriate guidance document in section "TOE Documentation"

Environmental Configuration

The following configuration was used for testing:

The TOE is tested mainly in the following test set-up:

[1] The suffix "T" indicates it is the testing version. "T" is removed and the final release version is "V800R006C00SPC200"



The tester is the Spirent Test centre.

Certificate

The IT product identified in this certificate has been evaluated at the Norwegian evaluation facility described on this certificate using Common Methodology for IT Security Evaluation, according to the version number described on this certificate, for conformance to the Common Criteria for IT Security Evaluation according to the version number described on this certificate. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunctionwith the complete Certification report. The evaluation has been conducted in accordance with the provisions of The Norwegian Certification Authority for IT Security (SERTIT) and the conclusions of the evaluation technical report are consistent with the evidence adduced. Certification does not guarantee that the IT product is free from security vulnerabilities. This certificate only reflects the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown of this certificate. This certificate is not an endorsement of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.

Product Manufacturer: Huawei Technologies

Product Name: NetEngine 5000E Core Router

Type of Product: Router

Version and Release Numbers: Version V800R006

Build: C00SPC200

Assurance Package: EAL 3 augmented with ALC_ CMC.4

Evaluation Criteria: Common Criteria version 3.1R4 (ISO/IEC 15408)

Name of IT Security Evaluation Facility: Brightsight B.V.

Name of Certification Body: SERTIT

Certification Report Identifier: SERTIT-061 CR, issue 1.0, 4 June 2015

Certificate Identifier: SERTIT-061 C

Date Issued: 4 June 2015

Kjartan Jæger Kvassnes
Certifier

Arne Høye Rage
Quality Assurance

Øystein Hole
Head of SERTIT

SERTIT
Norwegian Certification Authority for IT Security