SERTIT
Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

SERTIT-057 CR Certification Report

Issue 1.0 23.05.2014

Huawei CloudEngine Series Switch V100R002

CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009 VERSION 2.1 11.11.2011

SERTIT, P.O. Box 14, N-1306 Bærum postterminal, 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. *

* Mutual Recognition under the CC recognition arrangement applies to EAL 3.

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 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 CloudEngine Series Switch is a series of high-performance core switches designed for data center networks and high-end campus networks.

Huawei CloudEngine Series Switch version V100R002 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and have met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL3 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	Kvassnes, Kjartan Jæger Certifier
Quality Assurance	Arne Høye Rage Quality Assurance Arne H. Rage
Approved	Kjell W. Bergan Head of SERTIT Kjell W. Bergan
Date approved	23.05.2014

2 Abbreviations

ACL	Access Control List
AES	Advanced Encryption Standard
CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
GUI	Graphical User Interface
LMT	Local Maintenance Terminal
LPU	Line Process Unit
MCU	Main Control Unit
MD5	Message-Digest Algorithm 5
NTP	Network Time Protocol
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
SFR	Security Functional Requirement
SFU	Switching Fabric Unit
SNMP	Simple Network Management Protocol
SOGIS	Senior Officials Group Information Systems Security

SPM	Security Policy Model
SPU	Service Process Unit
SRU	Switch Router Unit
ST	Security Target
STP	Spanning-Tree Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
VP	Virtual Path
VRP	Versatile Routing Platform

3 References

[1] Huawei CloudEngine Series Switch V100R002 Security Target, Version 0.8, 2013-11-13.

[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 Huawei CE-Series Switches V100R002, version 1.1, March 27 2014.

[8] CloudEngine 6800&5800 Product Documentation, V1.0

[9] CloudEngine 12800 Product Documentation, V1.0

[10] CloudEngine V100R002 Certified Configuration, V5.0.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Huawei CloudEngine Series Switch version V100R002 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 CloudEngine Series Switch version V100R002.

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

The CloudEngine series switches provide secure, and high-performance L2/L3 switching capabilities, helping build a scalable, virtualized, and converged network.

At the core of each switch is the Versatile Routing Platform Version 8 Release 6 (VRP), the software for managing and running the router's networking functionality. VRP provides extensive security features. These features include different interfaces with according access levels for administrators; 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 1.3

4.4 Protection Profile Conformance

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

4.5 Assurance Level

The assurance incorporated predefined evaluation assurance level EAL3, 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

The TOE security policies are detailed in ST[1], chapter 3.2.

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.UnwantedTraffic

Unwanted traffic sent to/through the TOE will:

  - cause the TOE and/or resources on the network to become too slow or unavailable, or
  - reach resources on the network that it is not allowed to reach.

- T.UnauthenticatedAccess

A user who is not an administrator gains access to the management interface of the TOE

- T.UnauthorizedAccess

An administrator authorized to perform certain actions and access certain information gains access to commands or information he is not authorized for

- T.Eavesdrop

An eavesdropper (remote attacker) is able to intercept, and potentially modify or re-use information assets that are exchanged between:

  - TOE and LMT/RMT (management traffic)
  - TOE and the SNMP Trap Server (SNMP Traps)
  - TOE and other routers/switches (routing information)

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 countered are described.

4.11 Environmental Assumptions and Dependencies

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

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

- A Radius server or TACACS+ server for external authentication/authorization decisions
- Peer router(s) for the exchange of dynamic routing information
- Remote entities (PCs) used for administration of the TOE
- An SNMP Server used for collecting SNMP traps

It is assumed that the ETH interface in the TOE will be accessed only through an independent local network. This network is separate from the networks that use the other interfaces of the TOE.

The authorized administrators are not careless, wilfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.

4.12 IT Security Objectives

- 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 shall protect the network communication between:

  - the TOE and LMT/RMT (management information)
  - the TOE and the SNMP trap server (SNMP Traps)
  - the TOE and other switches/routers (routing information)
- O.Authorization

  The TOE shall allow different authorization levels to be assigned to administrators in order to restrict the functionality that is available to individual administrators.

- O.Authentication

  The TOE shall authenticate users before allowing them access to its management interface

- O.Audit

  The TOE shall generate audit records for security-relevant administrator actions.

4.13 Non-IT Security Objectives

- OE.NetworkElements

The operational environment shall provide secure and correct working network devices as resources that the TOE needs to cooperate with, such as: (when required):

  - A Radius server or TACACS+ server for external authentication/authorization decisions;
  - Peer router(s) for the exchange of dynamic routing information;
  - Remote entities (PCs) used for administration of the TOE.
  - An SNMP Server used for collecting SNMP traps

- OE.Physical

The operational environment shall protect the TOE against unauthorized physical access.

- OE.NetworkSegregation

The operational environment shall ensure that hat the ETH interface in the TOE will be accessed only through an independent local network. This network is separate from the networks that use the other interfaces of the TOE.

- 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/ECC 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/ECC 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/ECC 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
- FPT_FLS.1 Fail secure
- FTA_SSL.3 TSF-initiated termination
- FTA_TSE.1 TOE session establishment
- FTP_TRP.1 Trusted path
- FTP_ITC.1 Trusted channel
- FRU_PRS.1 Limited priority of service
- FRU_RSA.1 Maximum quotas
- FRU_FLT.1 Degraded fault tolerance

4.15 Security Function Policy

The functional host system is composed of the system backplane, MPU/LPU/SFU, SFU/MPU are the boards hosting the VRP which provides control and management functionalities. MPU also embeds a clock module as a source of system time. LPU is the board containing the forwarding engine and responsible for network traffic processing.

The functional host system processes data. In addition, it monitors and manages the entire system, including the power distribution system, heat dissipation system.

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 these Arrangements.

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].

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 on 27.03.2014. 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	Implementation representation 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_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	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

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 in the Operational User Guidance documents[8][9] provided by the developer. The [10] CloudEngine V100R002 Certified Configuration document[10] 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. Developers should 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, each containing between 1 and 13 tests. The categories are based on major groupings of security functionality, and in combination cover all SFRs and TSFIs.

5.7 Evaluators’ Tests

For independent testing it was decided to sample one test of each category to be repeated in his presence, thereby guaranteeing a good spread of these tests over the SFRs/TSFIs. The evaluator has also made sure that there is no overlap between these tests and the tests in the ATE IND, thereby maximizing coverage.

The evaluator also analysed the Developer Test Plan to see where additional tests could be performed, and selected 13 additional tests.

All of these tests were performed at the Huawei premises in Shenzhen in late February 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 CloudEngine Series Switch version V100R002 meet the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL3 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 CloudEngine Series Switch version V100R002 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 0 "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

There is no special hardware requirement. Since the TOE already includes the hardware components. The configuration of the hardware and software are listed below:

Hardware

Series name	Model name	Description
CloudEngine 12800 Series Switch 	Huawei CloudEngine 12800 Series 12-Slot Chassis (Also referred to as the 12812 Switch)	The Huawei CloudEngine 12800 Series 12812 support 12 LPU(Line Process Unit) . 12812 provides 2 Tbit/s per-slot bandwidth (can be increased to 4 Tbit/s) and a maximum of 48 Tbit/s switching capacity. 12812 chassis support 2 MPU/6 SFU/2 CMU/12 LPU/12 PM/17 FAN.
	Huawei CloudEngine 12800 Series 8-Slot Chassis (Also referred to as the 12808 Switch)	The Huawei CloudEngine 12800 Series 12808 support 8 LPU(Line Process Unit) . 12808 provides 2 Tbit/s per-slot bandwidth (can be increased to 4 Tbit/s) and a maximum of 32 Tbit/s switching capacity. 12808 Switch chassis support a maximum of 2 MPU/6 SFU/2 CMU/8 LPU/8 PM/13 FAN.
	Huawei CloudEngine 12800 Series 4-Slot Chassis (Also referred to as the 12804 Switch)	The Huawei CloudEngine 12800 Series 12804 support 4 LPU (Line Process Unit) . 12804 provides 2 Tbit/s per-slot bandwidth (can be increased to 4 Tbit/s) and a maximum of 16 Tbit/s switching capacity. 12804 Switch chassis support a maximum of 2 MPU/6 SFU/2 CMU/8 LPU/4 PM/9 FAN.
	Huawei CloudEngine 12800 Series Main Processing Unit MPUA (including master and slave, plugs into either the 12-Slot or 8-Slot or 4-slot chassis)	CE-MPUA is the main control unit of the CloudEngine 12800 series switches and is responsible for system control and management. The CE series switches can be configured with double CE-MPUAs to implement 1:1 hot backup. This configuration improves system reliability.
	Huawei CloudEngine 12800 Series Centralized Monitoring Unit CMUA (plugs into either the 12-Slot or 8-Slot or 4-slot chassis)	The CE-CMUA is the Centralized Monitoring Unit of the CloudEngine 12800 series switches and provides highly reliable device monitoring, management, and energy saving functions. The CE series switches can be configured with double CE-CMUAs to implement 1:1 hot backup. This configuration improves system reliability.
	Huawei CloudEngine 12800 Series Switch Fabric Unit (plugs into either the 12-Slot or 8-Slot or 4-slot chassis)	The CE-SFUs are switch fabric units of the CE series switches that complete line-speed switching on the data plane. A maximum of six CE-SFUs can be installed in a chassis and work in load balancing and redundancy mode to improve system reliability.
	CE-L48GT-EA (48-Port 10/100/1000BASE-T	The CE-L48GT-EA provides forty-eight GE electrical ports for data access and processing.

	Interface Card (EA, RJ45))	which can be installed in any slot of the CE12804/12808/12812 chassis.
	CE-L48GS-EA (48-Port 100/1000BASE-X Interface Card (EA, SFP))	The CE-L48GS-EA provides forty-eight GE optical ports for data access and processing. which can be installed in any slot of the CE12804/12808/12812 chassis.
	CE-L48GT-EC (48-Port 10/100/1000BASE-T Interface Card (EC, RJ45))	The CE-L48GT-EC provides forty-eight GE electrical ports for data access and processing. which can be installed in any slot of the CE12804/12808/12812 chassis.
	CE-L48GS-EC (48-Port 100/1000BASE-X Interface Card (EC, SFP))	The CE-L48GS-EC provides forty-eight GE optical ports for data access and processing. which can be installed in any slot of the CE12804/12808/12812 chassis.
	CE-L24XS-BA (24-Port 10GBASE-X Interface Card (BA, SFP+))	The CE-L24XS-BA provides twenty-four 10GE optical ports for data access and processing. which can be installed in any slot of the CE12804/12808/12812 chassis.
	CE-L24XS-EA (24-Port 10GE Optical Interface Card (EA, SFP+))	The CE-L24XS-EA provides twenty-four 10GE optical ports for data access and processing. which can be installed in any slot of the CE12804/12808/12812 chassis.
	CE-L48XS-BA (48-Port 10GBASE-X Interface Card (BA, SFP+))	The CE-L48XS-BA provides forty-eight 10GE optical ports for data access and processing. which can be installed in any slot of the CE12804/12808/12812 chassis.
	CE-L48XS-EA (48-Port 10GBASE-X Interface Card (EA, SFP+))	The CE-L48XS-EA provides forty-eight 10GE optical ports for data access and processing. which can be installed in any slot of the CE12804/12808/12812 chassis.
	CE-L24LQ-EA (24-Port 40G Interface Card (EA, QSFP+))	The CE-L24LQ-EA provides twenty-four 40GE optical ports for data access and processing. which can be installed in any slot of the CE12804/12808/12812 chassis.
CloudEngine 5800 Series Switch	CE5850-48T4S2Q-EI	CE5850-48T4S2Q-EI: Provides forty-eight 10/100/1000BASE-T Ethernet ports, four 10G SFP+ Ethernet optical ports, and two 40G QSFP+ Ethernet optical ports.
	CE5810-24T4S-EI	CE5810-24T4S-EI ：Provides twenty-four 10/100/1000BASE-T Ethernet ports, four 10G SFP+ Ethernet optical ports.
	E5810-48T4S-EI	CE5810-48T4S-EI ：Provides forty-eight 10/100/1000BASE-T Ethernet ports, four 10G SFP+ Ethernet optical ports.
CloudEngine 6800 Series Switch	CE6850-48S4Q-EI	CE6850-48S4Q-EI: Provides forty-eight 10G SFP+ Ethernet optical ports and four 40G QSFP+ Ethernet optical ports

	CE6850-48T4Q-EI	CE6850-48T4Q-EI: Provides forty-eight 10G BASE-T Ethernet ports and four 40G QSFP+ Ethernet optical ports

Software

Type	Name	Version
Software	Product software	V100R002 build C00SPC200
	VRP	Version 8 Release 6 build C00SPC200
	Linux	Version: 2.6.34.12-WR4.3.0.0

TOE Documentation

The supporting guidance documents evaluated were:

[a] CloudEngine 6800&5800 Product Documentation, V1.0

[b] CloudEngine 6800&5800 V100R002C00 Alarm Handling, V1.0

[c] CloudEngine 6800&5800 V100R002C00 Hardware Description, V05

[d] CloudEngine 12800 Product Documentation, V1.0

[e] CloudEngine 12800 V100R002C00 Alarm Handling, V1.0

[f] CloudEngine 12800 V100R002C00 Hardware Description, V05

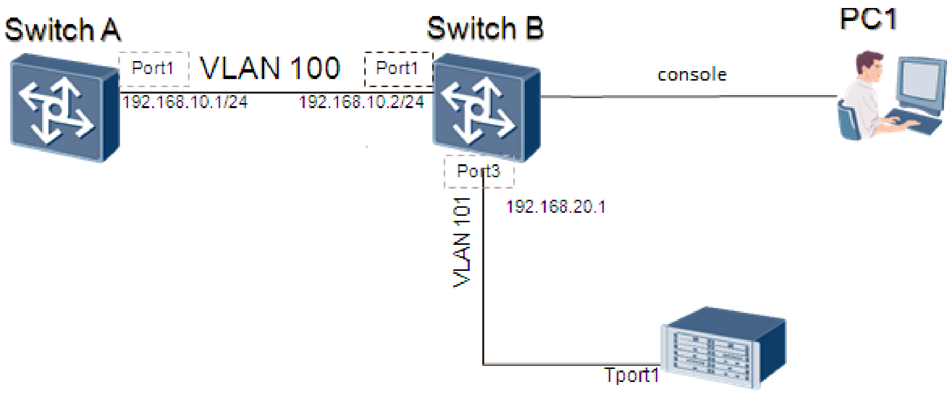
[g] CloudEngine 12800 V100R002C00 Log Reference 01, V1.0

[h] CloudEngine V100R002 Certified Configuration, V5.0

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

TOE Configuration

The TOE is tested mainly in the following test set-up (other setups were used for some tests, these were detailed in the test plan and results).



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.

Certificate

Product Manufacturer: Huawei Technologies

Product Name: Huawei CloudEngine Series Switch

Type of Product: Switch

Version and Release Numbers: Version V100R002

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-057 CR, issue 1.0, 23 May 2014

Certificate Identifier: SERTIT-057 C

Date Issued: 23 May 2014

Kjartan Jæger Kvassnes
Certifier

Arne H. Rage
Arne Høye Rage
Quality Assurance

Kjell W. Bergan
Kjell Werner Bergan
Head of SERTIT

SERTIT
Norwegian Certification Authority for IT Security

SOGIS