SERTIT

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

SERTIT-054 CR Certification Report

Issue 1.0 7 March 2014

Huawei USN9810 Unified Service Node V900R012

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.

Contents

Certification Statement

Huawei Technologies, Co., Ltd Huawei USN9810 Unified Service Node provides the functions of the serving GPRS support node (SGSN) and mobility management entity (MME) and can be used as a separate SGSN, separate MME, or combined SGSN/MME. The USN9810 can also be used as a single network element (NE) to manage other USN 9810s.

Huawei USN9810 Unified Service Node version V900R012 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) augmented requirements of Evaluation Assurance Level EAL3+ 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	Lars Borgos Quality Assurance
Approved	Kjell W. Bergan Head of SERTIT Kjell W. Bergan
Date approved	7 March 2014

1 Abbreviations

ACL	Access Control List
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
EAL	Evaluation Assurance Level
ECU	Enhanced Control Plane
EOR	Evaluation Observation Report
EPU	Enhanced Packet Forward Unit
ETI	E1/T1 Interface board
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
GPRS	General Packet Radio Service
GUI	Graphical User Interface
LMT	Local Maintenance Terminal
MME	Mobility Management Entity
NE	Network Element
NTP	Network Time Protocol
OMU	Operation and Maintenances Unit
PFI	Packet Forward Interface
POC	Point of Contact
PP	Protection Profile
QP	Qualified Participant
SDM	Shelf Data Module
SERTIT	Norwegian Certification Authority for IT Security
SFR	Security Functional Requirement

SGSN	Serving GPRS Support Node
SPM	Security Policy Model
ST	Security Target
SWU	Switch Unit
TMI	Time Master Interface
TOE	Target of Evaluation
TSF	TOE Security Functions
TSI	Time Slave Interface
TSP	TOE Security Policy

2 References

[1] Huawei USN9810 Version 900 Release 12 Security Target, 1.5, 2014-02-17

[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 USN9810 Unified Service Node V900R012, v 1.2, Febuary 17 2014.

[8] USN9810 Product Documentation V900R012C00, 2013/08/05

[9] Common Criteria Security Evaluation – Certified Configuration V1.2, 2013-11-12.

3 Executive Summary

3.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Huawei USN9810 Unified Service Node version V900R012 to the Sponsor, Huawei Technologies, Co., Ltd, 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 components.

3.2 Evaluated Product

The version of the product evaluated was Huawei USN9810 Unified Service Node version V900R012.

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

The USN9810 is a unified service node that can be used in GPRS, UMTS, and EPC networks. The USN9810 provides the functions of the serving GPRS support node (SGSN) and mobility management entity (MME) and can be used as a separate SGSN, separate MME, or combined SGSN/MME. The USN9810 can also be used as a single network element (NE) to manage other USN 9810s.

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

3.3 TOE scope

The TOE scope is described in the ST[1], chapter 1.4.

3.4 Protection Profile Conformance

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

3.5 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].

3.6 Security Policy

The TOE security policies are detailed in are specified in the ST[1], chapter 3.

3.7 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.

3.8 Threats Countered

- T.AccountabilityLoss:
  TA.ROGUE_USER performs undesirable actions that he is allowed to perform, or attempts to perform actions he is not allowed to, and this cannot be traced back to TA.ROGUE_USER.
- T.UnauthenticatedAccess:
  TA.ROGUE_USER or TA.ROGUE_SYSTEM gains access to the TOE.
- T.UnauthorizedAccess:
  TA.ROGUE_USER gains access to commands or information he is not authorized to access.

3.9 Threats Countered by the TOE's environment

- T.Eavesdrop:
  TA.NETWORK is able to intercept, and potentially modify or re-use, information assets that are exchanged between the TOE client (LMT) and the TOE server part (OMU).

3.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

3.11 Environmental Assumptions and Dependencies

It is assumed that the server part of the TOE and the workstation that is hosting the client part of the TOE are protected against unauthorized physical access.

It is assumed that the organization responsible for the TOE and its operational environment has measures in place to establish trust into and train users of the TOE commensurate with the extent of authorization that these users are given on the TOE. (For example, super users and users that are assigned similar privileges are assumed to be fully trustworthy and capable of operating the TOE in a secure manner abiding by the guidance provided to them.).

It is assumed that the customer`s configurations of connections to other trusted devices are correct.

It is assumed the operational environment provides reliable time stamps for the generation of audit records and a database to store the audit records.

It is assumed that the Telecommunication Service networks are trusted.

It is assumed that the systems in the Telecommunication Service networks and the EMS are trusted.

3.12 IT Security Objectives

- O.Authentication:
  The TOE shall authenticate management users of its user interfaces.
- O.Authorization:
  The TOE must implement an access control mechanism to differentiate between different authorities for TOE users.
- O.AccessControl:
  The TOE shall refuse access by invalid devices or users.
- O.Communication:
  The TOE shall implement logical protection measures for network communication between the server part of the TOE and the client part of the TOE.
- O.Audit:
  The TOE shall be able to generate audit records for security-relevant events.

3.13 Non-IT Security Objectives

- OE.Administration:
  Those responsible for the operation of the TOE and its operational environment must ensure that only authorized users have access to the management plane, and in particular to the part of the TOE and its data that is running in management plane. This includes ensuring that audit records stored in the database in the operational environment are protected against unauthorized access, and that cryptographic keys and certificates are properly managed to support the communications security mechanisms implemented by the TOE. This also includes the restriction of physical access to the server part of the TOE and the workstation hosting the client, making the TOE unavailable to access from the consumer/application networks served by the network device, and ensure that devices and networks the TOE assumes to be trusted are indeed trustworthy.
- OE.Support:
  Those responsible for the operation of the TOE and its operational environment must ensure that the operational environment provides reliable time stamps for the generation of audit records and a database to store these records.
- OE.Users:
  Those responsible for the operation of the TOE and its operational environment must be trustworthy, and trained such that they are capable of securely managing the TOE and following the provided guidance.
- OE.Devices:
  Those responsible for the operation of the TOE must ensure that the configuration of connections to trusted devices in the TOE environment is correct.

3.14 Security Functional Components

- FAU_GEN.1
- FAU_GEN.2
- FAU_SAR.1
- FAU_SAR.3
- FDP_ACC.1
- FDP_ACF.1
- FIA_AFL.1
- FIA_ATD.1
- FIA_SOS.1
- FIA_UAU.2
- FIA_UID.2
- FMT_MSA.1
- FMT_MSA.3
- FMT_SMF.1
- FMT_SMR.1
- FPT_ITT.1
- FTA_TSE.1
- FTP_ITC.1/EMS

3.15 Security Function Policy

The TOE security policies are detailed in are specified in the ST[1], chapter 6.

3.16 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 SD001E[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 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].

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 17.02.2014. SERTIT then produced this Certification Report.

3.17 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.

4 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

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

4.1 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.

4.2 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.

4.3 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 Common Criteria Security Evaluation – Certified Configuration document[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.

4.4 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.

4.5 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.

4.6 Developer's Tests

The Developer Test Plan consists of 25 different categories. Each category contains between 1 and 9 tests. However, only parts of sub-categories are related to security functionality. The relevant tests in combination cover all SFRs and TSFIs.

4.7 Evaluators' Tests

For independent testing it was decided to sample one test of each SFR relevant category

This approach guaranteed 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 next section, thereby maximizing coverage.

The evaluator also analysed the Developer Test Plan to see where additional ATE tests could be performed, and selected 9 additional tests.

All of these tests were performed at the Huawei premises in Shenzhen between 8th October and 11th October 2013.

5 Evaluation Outcome

5.1 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 USN9810 Unified Service Node version V900R012 meet the Common Criteria Part 3 extended 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.

5.2 Recommendations

Prospective consumers of Huawei USN9810 Unified Service Node version V900R012 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 3.3 “TOE Scope” and Section 4 “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

Name	Version	Description
OMU	CN21UPBA2/ CN22UPBA6	The operation & maintenance unit (OMU) performs the operations and maintenance of the system.
USI	USIA7	• Serving as the interface board of the UPB, the USIA7 provides various external interfaces, including: • Six gigabit Ethernet interfaces (10/100/1000M auto-sensing) to other network devices • Standard VGA interface to the KVMS • USB interface to the keyboard and mouse • Hot swapping
ECU	CN21UPBA3/ CN22UPBA3	The enhanced control plane unit (ECU) performs the service processing and charging functions related to the control plane.
EPU	MSPB0	The Enhanced Packet forward Unit (EPU) board processes the services related to the user plane.
ETI	ETIA0/SSIA0 /SSIA2	Functioning as the rear board of the enhanced control plane unit (ECU), the E1/T1 interface board (ETI) is generally used together with matching sub-boards.
PFI	PFIA0	Packet Forward Interface (PFI) as the rear board of the broadband interface processing board and the rear board of the EPU board.
SWU	SWUA1/SWUB1	The SWU is a switch unit. It consists of an exchange carrier board and a time division multiplexing (TDM) daughter board. The SWU supports layer-2 network switching, TDM narrowband switching, device management, configuration restoration and hot swap.
TSI	SWIA0/SWIB	The Time Slave Interface (TSI) board is used in the extended sub rack supporting cascading between

	0	sub-racks and provides the clock receive function.
TMI	SWIA1/SWIB1	The Time Master Interface (TMI) board is used in the extended sub rack supporting cascading between sub racks and provides the clock receive function.
SMM	SMMD/SMME	The SMM board is used to manage all hardware in the OSTA 2.0 sub rack including the sub rack, boards of all types, fan tray to implement the device management, event management, asset management, power management, remote maintenance, configuration restoration, and power saving control.
SDM	SDM	The SDM (Shelf Data Module) stores the sub rack asset information, such as sub rack name, bar code, vendor, and delivery date.

Software

Name	Version
USN9810	V900R012C00SPC300
OS	SUSE Linux Enterprise Server 10 SP2

TOE Documentation

The supporting guidance documents evaluated were:

[a] USN9810 Product Documentation V900R012C00, 2013/08/05

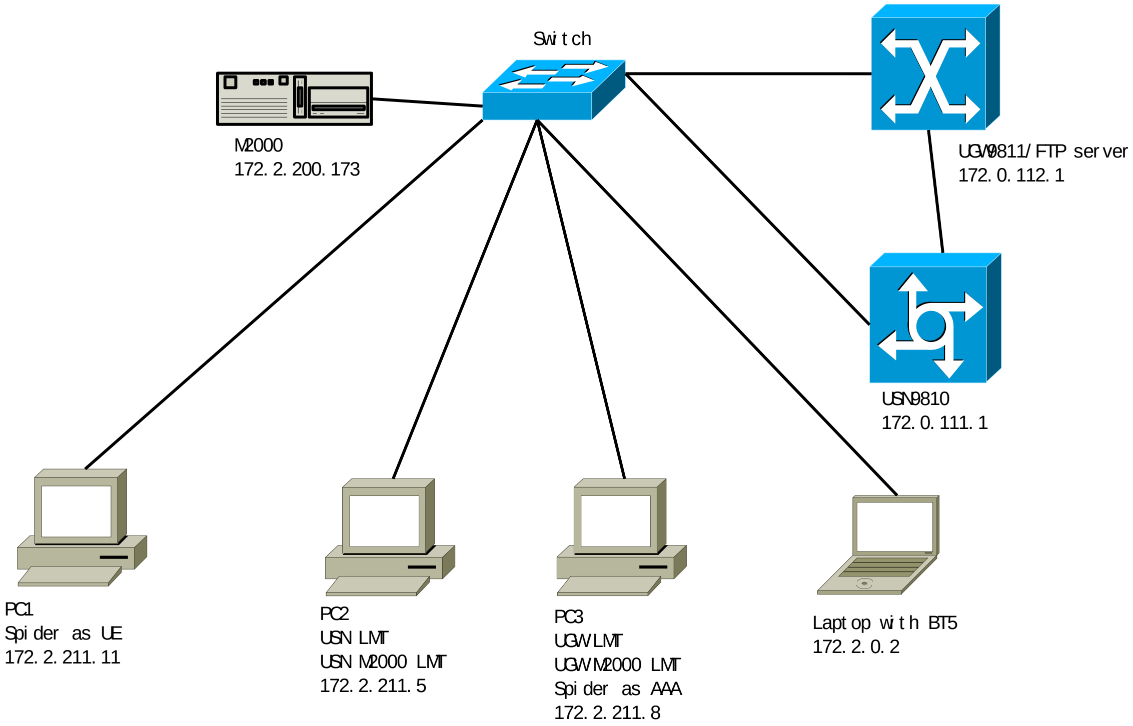
[b] Common Criteria Security Evaluation – Certified Configuration V1.2, 2013-11-12

Further discussion of the supporting guidance material is given in Section 4.3 "Installation and Guidance Documentation".

TOE Configuration

The TOE is tested by the evaluator on USN9810 V900R012C00SPC300.

The following configuration was used for testing:



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 USN9810

Type of Product: Unified Service Node

Version and Release Numbers: Version V900R012

Build: C00SPC300

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-054 CR, issue 1.0, 7 March 2014

Certificate Identifier: SERTIT-054 C

Date Issued: 7 March 2014

Kjartan Jæger Kvassnes
Certifier

Lars Borgos
Quality Assurance

Kjell W. Bergan

Kjell Werner Bergan
Head of SERTIT

SERTIT
Norwegian Certification Authority for IT Security