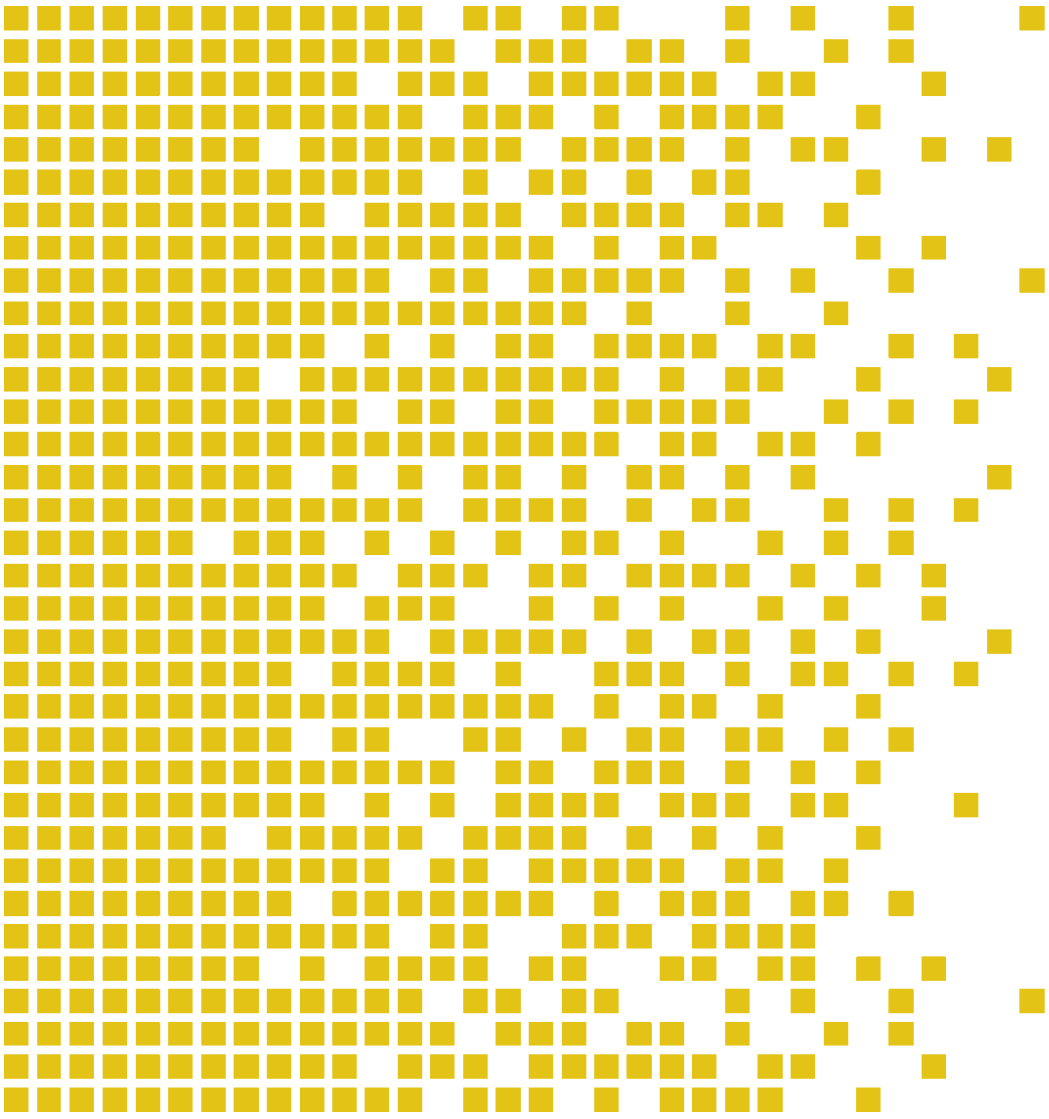
# SERTIT-053 CR Certification Report

Issue 1.0 13 December 2013

## Huawei UGW9811 V900R010ENGC00SPC200





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 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 but not to ALC_CMC.4.

Contents

# 1 Certification Statement

Huawei Technologies Co., Ltd. Huawei UGW9811 is a unified packet gateway that can be used in GPRS, UMTS, and EPC networks.

Huawei UGW9811 version V900R010ENGC00SPC200 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 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 | Kjartan Jæger Kvassnes<br>Certifier |
| Quality Assurance | Lars Borgos<br>Quality Assurance |
| Approved | Kjell W. Bergan<br>Head of SERTIT |
| Date approved | 13 December 2013 |

# 2 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 |
| EOR | Evaluation Observation Report |
| EPC | Evolved Packet Core |
| ETR | Evaluation Technical Report |
| EVIT | Evaluation Facility under the Norwegian Certification Scheme for IT Security |
| EWP | Evaluation Work Plan |
| GGSN | Gateway GPRS Support Node |
| GPRS | General Packet Radio Service |
| GUI | Graphical User Interface |
| LIG | Lawful Interception Gateway |
| LMT | Local Maintenance Terminal |
| LPU | Line Process Unit |
| MME | Mobility management entity |
| MPU | Main Processing Unit |
| NTP | Network Time Protocol |
| PDN | Packet Data Network |
| P-GW | PDN Gateway |
| POC | Point of Contact |
| PP | Protection Profile |
| QP | Qualified Participant |
| RNC | Radio network controller |
| SERTIT | Norwegian Certification Authority for IT Security |
| SFR | Security Functional Requirement |
| SFU | Switching Fabric Unit |

| | |
|---|---|
| SGSN | Serving GPRS support node |
| S-GW | Serving Gateway |
| SNMP | Simple Network Management Protocol |
| SPM | Security Policy Model |
| SPU | Service Process Unit |
| SRU | Switch Router Unit |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |
| UMTS | Universal Mobile Telecommunications Service |
| VP | Virtual Path |
| VRP | Versatile Routing Platform |

# 3 References

[1] Security Target for Huawei UGW9811 V900R010, Version 1.5, 2013-11-07.

[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 UGW9811 Unified Packet Gateway V900R010, 13-RPT-316, Version 1.1, December 09, 2013.

[8] HUAWEI UGW9811 Unified Gateway V900R010C00 Product Documentation 06(GGSN&S-GW&P-GW), version V900R010C00, 2013/06/08

[9] UGW9811 NPE Solution Documentation, version V900R009C01, 2011/12/15

[10] Common Criteria Security Evaluation – Certified Configuration, version 1.2, 2013/11/07.

# 4 Executive Summary

## 4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Huawei UGW9811 version V900R010ENGC00SPC200 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 requirements.

## 4.2 Evaluated Product

The version of the product evaluated was Huawei UGW9811 version V900R010ENGC00SPC200.

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

The UGW9811 is a unified packet gateway that can be used in GPRS, UMTS, and EPC networks. The UGW9811 can function as a gateway GPRS support node (GGSN), serving gateway (S-GW), PDN gateway (P-GW), or any combination of these three roles, and can be managed individually.

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.

## 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 EAL3, augmented with 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 are specified in the ST[1], chapter 3.

## 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.UNAUTHORIZED:
  TA.ROGUE_USER tries to access the TOE management function that he/she is not authorized to
- T.UNKNOWN_USER:
  TA.NETWORK_T or TA.NETWORK_M gains unauthorized access to the TOE and is able to perform actions on the TOE
- T.NETWORK_M:
  TA.NETWORK_M is able to modify/read external network traffic originating from / designated for the TOE and thereby:
  - Perform actions on the TOE
  - Gain unauthorized knowledge about the traffic between the LMT and the server
- T.NETWORK_T:
  TA.NETWORK_T is able to modify/read external network traffic originating from designated for the TOE and thereby gain unauthorized knowledge about the traffic between the server and LIG, SGSN, MME, RNC, eNodeB, PGW, SGW, PCRF, OCS, 3GPP-AAA server, AAA server, DHCP server, Report server, CHR server, BM-SC, HSGW, ICAP server
- T.UnwantedTraffic:
  TA.NETWORK_T, TA.ROGUE_MS_USER or TA.ROGUE_SYSTEM sends unwanted network traffic to the TOE which consumes the TOE's processing capacity for incoming network traffic, thus fails to process traffic expected to be processed. This may further causes the TOE fails to respond to system control and security management operations.

## 4.9 Threats Countered by the TOE's environment

- T.UNAUTHORIZED_MS:
  TA.ROGUE_MS_USER tries to access the telecommunication service network/PDN that he/she is not authorized to
- T.AUTHORIZED:
  TA.ROGUE_USER performs actions on the TOE that he/she is allowed to but not desired and these actions cannot be traced back to that specific user
- T.PHYSICAL:
  TA.PHYSICAL gains physical access to the TOE (either LMT or UGW9811 Server) and is able to perform actions on the TOE.

## 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 network interfaces that allow access to the TOE's user interfaces are in a management network that is separate from the application (or, public) networks that the network device hosting the TOE serves.

## 4.12 IT Security Objectives

- O.IDAUTH:
  The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.
- O.IDAUTHMS:
  The TOE shall support MS user authentication, allowing the TOE to accept/reject the non-3GPP MS users based on the response of the 3GPP AAA servers, and accept/reject MS users accessing PDN networks based on the response of the PDN AAA servers.
- O.Resource:
  The TOE shall provide functionalities and management configuration to prevent traffic overload.
- O.Connect:
  The TOE shall provide functionality to limit other devices (e.g., MS, SGSN/MME/S-GW) from connecting to it
- O.Audit:
  The TOE shall provide functionality to generate audit records for security-relevant administrator actions.
- 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.Communication:
  The TOE must implement logical protection measures for network communication between the server and LMT part of the TOE, and the server part of the TOE and various devices in the telecommunication network .

## 4.13 Non-IT Security Objectives

The following security objectives, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

- OE.PHYSEC:
  The operator shall ensure the TOE is protected against unauthorized physical access.
- OE.Person:
  Personnel working as authorized administrators shall be carefully selected for trustworthyness and trained for proper operation of the TOE.

- OE.TrustedSystems:
  The operator shall correctly configure the TOE such that only trusted devices can connect to the TOE
- OE.NetworkElements:
  The operator shall provide:
  - At least two L3 switches to separate the management network and the telecommunication service network
  - 3GPP-AAA server to authenticate the non-3GPP MS user to use the 3GPP network
  - PDN AAA server to authenticate the MS user to the PDN network
  - Firewall between the server part of the TOE and the PDN networks
- OE.NetworkSegregation:
  The operational environment shall provide segregation by deploying the Ethernet interface on MPU/SRU in TOE into a local sub-network, compared to the interfaces on LPU in TOE serving the application (or public) network.
- OE.NetworkSecurity:
  The operational environment shall provide network security. Different security policies should be deployed for different security domains. In addition, the isolation of the management/control/end-user planes should be designed, in such a way that events on one Security Plane are kept totally isolated from the other Security Planes.

## 4.14 Security Functional Requirements

All the SFR's are described in full in the ST[1], chapter 5.2.

## 4.15 Security Function Policy

The UGW9811, a unified packet gateway independently developed by Huawei, can be used in GPRS, UMTS, and EPC networks. The UGW9811 can function as a gateway GPRS support node (GGSN), serving gateway (S-GW), PDN gateway (P-GW), or any combination of these three roles, and can be managed individually.

For a full description, see the ST[1], chapter 1.3.1.

## 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 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 on 9. December 2013. 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 |

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 in the Operational User Guidance documents[8][9] provided by the developer. The Common Criteria Security Evaluation – 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 3 major categories. Each category contains 2-10 sub categories, and each sub-category contains 1-9 tests. However, only parts of

sub-categories are related to security functionality. The relevant tests in combination cover all SFRs and TSFIs.

### 5.7 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 14 additional tests.

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

## 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 UGW9811 version V900R010ENGC00SPC200 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 UGW9811 version V900R010ENGC00SPC200 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.

The above "Evaluation Findings" include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

# 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 |
|---|---|---|
| SRU/MPU | V900R10C00 | Switch and Route Processing Unit/Main Processing Unit, which is the core circuit board for system management. The SRU/MPU collects routing information and generates routing tables. The SRU/MPU serves as the operation and maintenance agent of the system. |
| SFU | V900R10C00 | Switching Fabric Unit, which performs the data exchange function. The SFU switches service data in the entire system and works in 3+1 backup mode to share service data load. |
| SPU | V900R10C00 | Service Processing Unit, which performs the service processing function. The SPU processes all UGW9811 services, including GTP access, charging, and policy enforcement. |
| LPU | V900R10C00 | Line Processing Unit, which provides physical interfaces that connect the UGW9811 to NEs or external networks. |

## Software

| Name | Version |
|---|---|
| UGW9811 | V900R010ENGC00SPC200 |
| LMT GUI | V900R10C00 |

## TOE Documentation

The supporting guidance documents evaluated were:

[a] HUAWEI UGW9811 Unified Gateway V900R010C00 Product Documentation 06(GGSN&S-GW&P-GW), version V900R010C00, 2013/06/08

[b] UGW9811 NPE Solution Documentation, version V900R009C01, 2011/12/15

[c] Common Criteria Security Evaluation – Certified Configuration, version 1.2, 2013/11/07

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

## TOE Configuration

The TOE was tested on UGW9811 V900R010ENGC00SPC200.

The following configuration was used for testing: