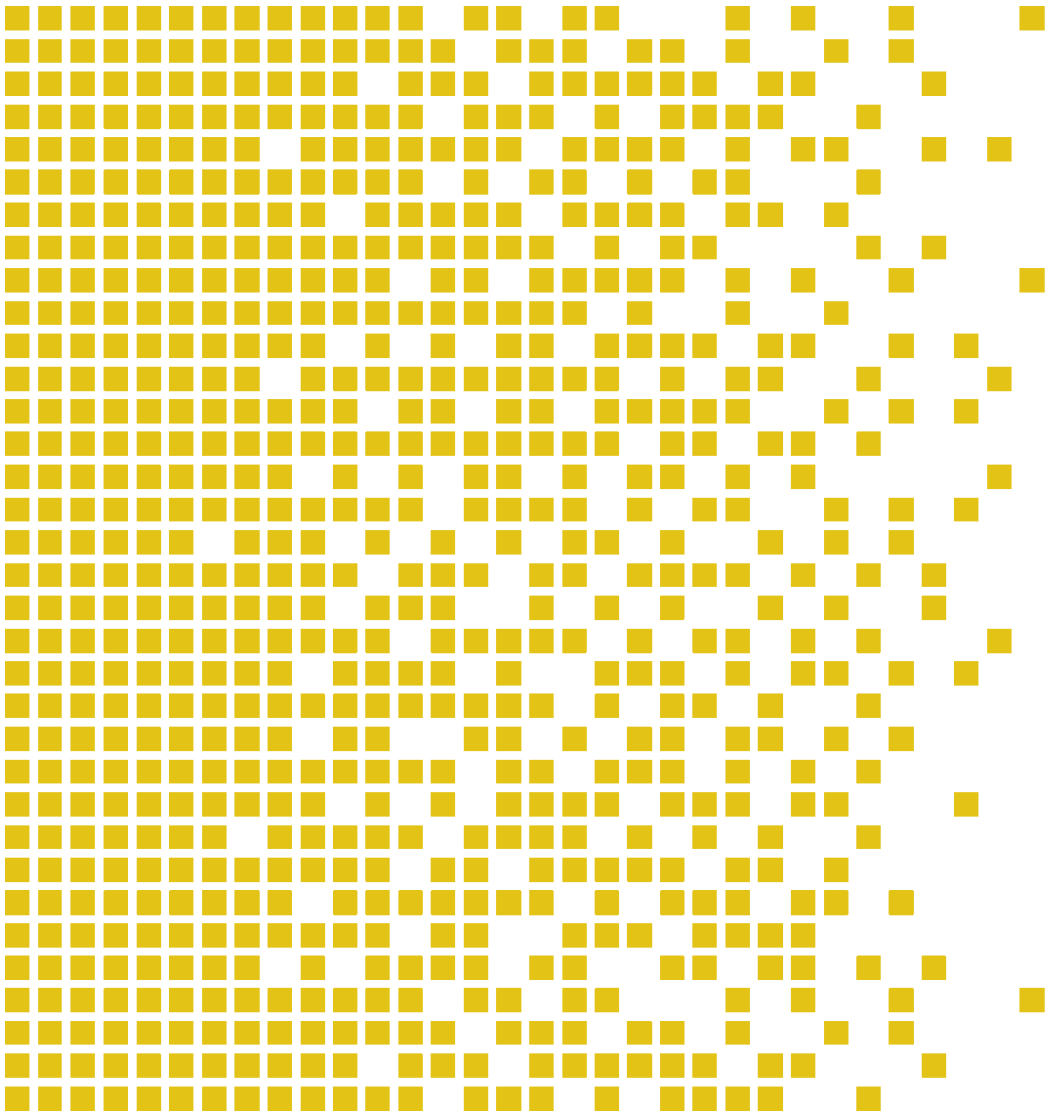
SERTIT-067 CR Certification Report

Issue 1.0 4 June 2015

Huawei iManager U2000 V100R009C00SPC301



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 July 2nd 2014. The recognition under CCRA is limited to cPP related assurance packages or EAL 2 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 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 iManager U2000 is a software system which provides centralized operation and maintenance for Huawei's fixed network element management solution.

Huawei iManager U2000 version V100R009C00SPC301 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 and ALC_FLR.2 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

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
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
NE	Network Element
OM	Operation and Maintenance
OSS	Operations Support System
POC	Point of Contact
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] Huawei iManager U2000, version V100R009C00SPC301 Security Target, Version 1.6, 2014-12-04.

[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 iManager U2000, version V100R009C00SPC301, 14-RPT-361, December 17, 2014

[8] iManager_U2000_V100R009C00_Product_Documentation_03(hdx)-C, Issue 03

[9] U2000_V100R009C00SPC301_Patch_Installation_Guide_03-A , issue 03

[10] Common Criteria Security Evaluation - Certified Configuration, v1.2

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Huawei iManager U2000 version V100R009C00SPC301 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 iManager U2000 and version V100R009C00SPC301.

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

Huawei's iManager U2000 (U2000) Element Management system is a software system which provides centralized operation and maintenance for Huawei's fixed network element management solution. The U2000 manages the fixed network element including the Transport, Access and IP equipment, and provides external interfaces for interoperability with other systems. The core of Huawei iManager U2000 is the iMAP Platform, U2000 V100R009C00SPC301 is based on the iMAP Platform.

The iMAP Platform provides extensive security features, including account based system access control that enforces only authenticated users can access authorized system features; auditing of security-relevant user activities; as well as the enforcement of network transmission security against data peeking.

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 1.4.1.

4.4 Protection Profile Conformance

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

4.5 Assurance Level

The Security Target[1] specified the assurance requirements for the evaluation. Predefined evaluation assurance level EAL 3 was used, augmented by ALC_CMC.4 and ACL_FLR.2. 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.UnauthenticatedAccess

  An attacker who is not a user of the TOE, gains access to the TOE, modifies and compromises the confidentiality of the TSF data and the OM data.

- T.UnauthorizedAccess

  An unauthorized user may gain unauthorized accesses to the TOE and compromises the confidentiality and the integrity of the TSF data and OM data. Also perform non-authorized operations in the NEs.

- 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 NEs, between the client and server of the TOE and between the server and the OSS client.

4.9 Threats Countered by the TOE's environment

- T.UnauthenticatedAccess is partly countered by OE.Physical and OE.Database;
- T.UnauthorizedAccess is partly countered by OE.Database.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

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

- A PC that is suitable to run the client part of the TOE (see ST[1] chapter 1.3.3);
- A server that is suitable to run the server part of the TOE (see ST[1] chapter 1.3.3)
- Firewall to protect the server part of the TOE;

- NEs that are managed by the TOE shall support SSL/SNMPv3/SSH/SFTP/HTTPS, and will not perform any harmful operation to the TOE;
- A NTP server to provide accurate time.

4.12 IT Security Objectives

The following objectives must be met by the TOE:

- **O.Communication** The TOE must implement logical protection measures for network communication between the server of TOE and network elements from the operational environment, also for the communication between the GUI and the server of the TOE and between the server and the OSS .
- **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, including limitations to the session establishment. Also limitation to the actions that may be performed in a Network Element.
- **O.Authentication** The TOE must authenticate users of its user access; The TOE shall provide configurable system policy to restrict user session establishment.
- **O.Audit** The TOE shall provide functionality to generate and review audit records for security-relevant administrator actions.

4.13 Non-IT Security Objectives

The following objectives must be met by the operational environment:

- **OE.NetworkElements** The operational environment shall ensure that the managed network elements are trusted can support the SSL /SNMPv3/SSH/SFTP/HTTPS connection with the TOE, and the private interface defined by Huawei .
- **OE.Physical** The TOE (i.e., the complete system including attached peripherals, such as Sun workstation, Suse Linux workstation, windows Server workstation, disk array, client PC) shall be protected against unauthorized physical access.
- **OE.NetworkSegregation** The operational environment shall provide protection to the network in which the TOE hosts by separating it from the application (or public) network. A firewall shall be installed between the server of TOE and non-trust domain, filter the unused communication port.
- **OE.Database** The operational environment shall protect the database against unauthorized physical access and data file damage.
- **OE.AdministratorBehaviour** The super user admin and the users that belong to the SMManagers and Administrator groups will behave correctly and will not perform any harmful operation to the TOE. Also, the users of the underlying operating system will not perform any harmful operation to the TOE.

- **OE.NTP** The operational environment shall provide an accurate time source, in order to ensure the normal operation of the server of 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.2 Restricted audit review
- FAU_SAR.3 Selectable audit review
- FAU_STG.3 Action in case of possible audit data loss
- FDP_ACC.2 Complete access control
- FDP_ACF.1 Security attribute based access control
- FIA_AFL.1 Authentication failure handling
- FIA_ATD.1 User attribute definition
- FIA_SOS.1 Verification of secrets
- FIA_UAU.2 User authentication before any action
- 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_ITT.1 Basic internal TSF data transfer protection
- FTA_MCS.1 Basic limitation on multiple concurrent sessions
- FTA_SSL.1 TSF-initiated session locking
- FTA_TSE.1 TOE session establishment
- FTP_TRP.1 Trusted path
- FTP_ITC.1.OSS Inter-TSF trusted channel
- FTP_ITC.1.NE Inter-TSF trusted channel

4.15 Security Function Policy

The U2000 manages the fixed network element including the Transport, Access and IP equipment, and provides external interfaces for interoperability with other systems. The core of Huawei iManager U2000 is the iMAP Platform, U2000 V100R009C00SPC301 is based on the iMAP Platform.

The iMAP Platform provides extensive security features, including account based system access control that enforces only authenticated users can access authorized system features; auditing of security-relevant user activities; as well as the enforcement of network transmission security against data peeking.

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 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 17-12-2014. 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 and ALC_FLR.2.

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
	ALC_FLR.2	Flaw reporting procedures
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 1.4.1 and Preparative Procedures documents [8][9] provided by the developer. The Common Criteria Security Evaluation – Certified Configuration [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. 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 13 different categories, each containing several relevant 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, the evaluator has decided to sample a limit number of the general security functionality tests (such as authentication, authorization, managing), and to sample several penetration tests to ensure the developer performed them correctly. The evaluator also analyzed 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 Shenzhen in end October 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 iManager U2000 version V100R009C00SPC301 meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 3 augmented with ALC_CMC.4 and ALC_FLR.2 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 iManager U2000 version V100R009C00SPC301 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 the following software:

Application Software	Name and version
U2000 Client	Huawei iManager U2000 V100R009C00SPC301
U2000 Server	Huawei iManager U2000 V100R009C00SPC301

TOE Documentation

The supporting guidance documents evaluated were:

[a] iManager_U2000_V100R009C00_Product_Documentation_03(hdx)-C, Issue 03

[b] U2000_V100R009C00SPC301_Patch_Installation_Guide_03-A , Issue 03

[c] Common Criteria Security Evaluation - Certified Configuration, v1.2

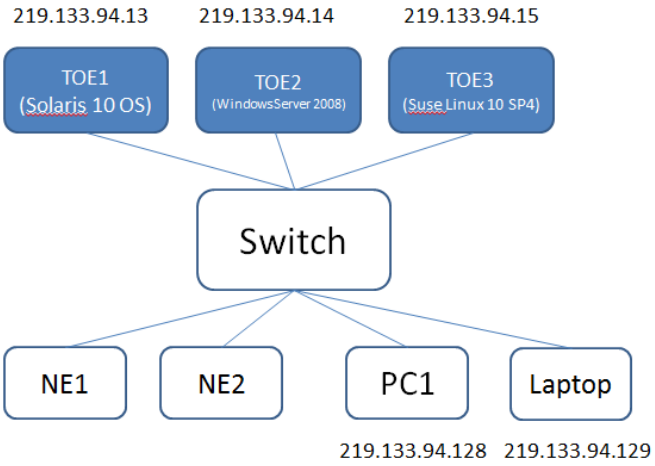
Further discussion of the supporting guidance material is given in Section 5.3 "Installation and Guidance Documentation".

TOE Configuration

Item	Identifier
HARDWARE	N/A as the TOE is software only.
SOFTWARE	The software listed in section "TOE Identification" configured according to [a] in section "TOE Documentation".
MANUAL	iManager_U2000_V100R009C00_Product_Documentation_03(hdx)-C, Issue 03 U2000_V100R009C00SPC301_Patch_Installation_Guide_03-A , Issue 03 Common Criteria Security Evaluation - Certified Configuration, v1.2

Environmental Configuration

The following configuration was used for testing:


219.133.94.13
219.133.94.14
219.133.94.15
TOE1
(Solaris 10 OS)
TOE2
(WindowsServer 2008)
TOE3
(Suse Linux 10 SP4)
Switch
NE1
NE2
PC1
Laptop
219.133.94.128
219.133.94.129