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

SERTIT-065 CR Certification Report

Issue 1.0 2 June 2015

USP running on Huawei Transmission Equipment Series (WDM/OTN, SDH/MSTP, RTN) V100R013C00

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

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

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

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

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

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

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

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

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the 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 USP running on Huawei Transmission Equipment Series (WDM/OTN, SDH/MSTP, RTN) is an optical transmission system transparently transmit client services from one place to another. During the transmission, transmission equipment encapsulates client services into signals of certain rates, performs error control, and monitors the quality of the signals. To achieve transparent transmission, the transmission equipment does not process client services transmitted from other equipment.

The Optix OSN 1800(I/II) /1800V /3800 /3800A /6800 /6800A /8800(T16/T32/T64) /9600(U32/U64) /9800(U32/U64) are WDM/OTN products. The Optix OSN 500 /550 /580 /1500(A/B) / 3500 /7500 /7500II are SDH/MSTP products. The Optix RTN 360 /380 /905(1A/1C/1E/2A/2E) /950 /950A /980 /980L are RTN products. The USP is the software core of the transmission equipment. It is the software platform for managing and running communication networking functionalities.

USP running on Huawei Transmission Equipment Series (WDM/OTN, SDH/MSTP, RTN) version v100R13C00 have 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 and ALC_FLR.2 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality when running on the platforms specified in Annex A.

Author	Kjartan Jæger Kvassnes Certifier
Quality Assurance	Arne Høye Rage Quality Assurance Arne H. Rage
Approved	Øystein Hole Head of SERTIT Øystein Hole
Date approved	2 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
EMS	Element Management System
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
LCT	Local Craft Terminal
LMT	Local Maintenance Terminal
MSTP	Multi-Service Transmission Platform
NMS	Network Management System
OSN	Optical Switch Node
OTN	Optical Transport Network
POC	Point of Contact
PP	Protection Profile
QP	Qualified Participant
RADIUS	Remote Authentication Dial-In User Service
RMT	Remote Maintenance Terminal
RTN	Radio Transmission Node
SDH	Synchronous Digital Hierarchy
SERTIT	Norwegian Certification Authority for IT Security
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
SPM	Security Policy Model
SSH	Secure Shell
SSL	Secure Sockets Layer

ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
USP	Universal Software Platform
WDM	Wavelength Division Multiplexing

3 References

[1] Huawei USP running on Transmission Equipment Series (OptiX OSN 1800/3800/3800A/6800/6800A/8800/9600/9800, OptiX OSN 500/550/580, OptiX OSN 1500(A/B)/3500/7500/7500 II, and OptiX RTN 360/380/905(1A/1C/1E/2A/2E)/950/950A/980/980L) V100R13C00 Security Target, Version 1.7, 2014-12-12.

[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 USP running on Transmission Equipment Series (OptiX OSN 1800/3800/3800A/6800/6800A/8800/9600/9800, OptiX OSN 500/550/580, OptiX OSN 1500(A/B)/3500/7500/7500 II, and OptiX RTN 360/380/905(1A/1C/1E/2A/2E)/950/950A/980/980L) V100R13C00, 14-RPT-360, v1.2, December 22, 2014

[8] Huawei Transmission Equipment Series Certified Configuration v1.4

[9] OSN 1800 I/II Compact Multi-Service Edge Optical Transport Platform V100R005C10 Product Documentation-01

[10] OSN 1800 I/II Compact Multi-Service Edge Optical Transport Platform V100R005C10 Product Documentation-01

[11] OSN 1800 V Packet Enhanced V100R005C10 Deploying Your Network 01

[12] OSN 1800 V Packet Enhanced V100R005C10 Installing, Operating and Maintaining Your Network (For Field Engineer) 01

[13] OSN 1800 V Packet Enhanced V100R005C10 Operating and Maintaining Your Network (For 1st Line Engineer) 01

[14] OSN 1800 V Packet Enhanced V100R005C10 Operating and Maintaining Your Network (For 2nd Line Engineer) 01

[15] OSN 1800 V Packet Enhanced V100R005C10 Planning Your Network 01

[16] OptiX OSN 8800 V100R009C00 Product Documentation 01

[17] OptiX OSN 8800 V100R009C00 Product Documentation 01

[18] OptiX OSN 8800 V100R009C00 Product Documentation 01

[19] OptiX OSN 3800 V100R009C00 Product Documentation 01

[20] OptiX OSN 6800 V100R009C00 Product Documentation 01

[21] OptiX OSN 8800 6800A 3800A V100R008C00 Product Documentation 01(NA)

[22] OptiX OSN 8800 6800A 3800A V100R008C00 Product Documentation 01(NA)

[23] OSN 9800 V100R001C20 Planning Your Network 01

[24] OSN 9800 V100R001C20 Installing, Operating and Maintaining Your Network (For Field Engineer) 01

[25] OSN 9800 V100R001C20 Operating and Maintaining Your Network (For 2nd Line Engineer) 01

[26] OSN 9800 V100R001C20 Operating and Maintaining Your Network (For 1st Line Engineer) 01

[27] OSN 9800 V100R001C20 Deploying Your Network 01

[28] OSN 9800 V100R001C20 Planning Your Network 01

[29] OSN 9800 V100R001C20 Installing, Operating and Maintaining Your Network (For Field Engineer) 01

[30] OSN 9800 V100R001C20 Operating and Maintaining Your Network (For 2nd Line Engineer) 01

[31] OSN 9800 V100R001C20 Operating and Maintaining Your Network (For 1st Line Engineer) 01

[32] OSN 9800 V100R001C20 Deploying Your Network 01

[33] OSN 9600 V100R001C20 运维指导（网络运维工程师用书）01

[34] OSN 9600 V100R001C20 运维指导（网络监控工程师用书）01

[35] OSN 9600 V100R001C20 开局指导 01

[36] OSN 9600 V100R001C20 规划指导 01

[37] OSN 9600 V100R001C20 站点操作指导 01

[38] OSN 9600 V100R001C20 运维指导（网络运维工程师用书）01

[39] OSN 9600 V100R001C20 运维指导（网络监控工程师用书）01

[40] OSN 9600 V100R001C20 开局指导 01

[41] OSN 9600 V100R001C20 规划指导 01

[42] OSN 9600 V100R001C20 站点操作指导 01

[43] OSN 500 V100R007C20 Product Description 01(pdf).zip

[44] OSN 500 V100R007C20 Hardware Description 01(pdf).zip

[45] OptiX OSN 500 Quick Installation Guide 04(pdf).zip

[46] OptiX OSN 500 V100R007C20 Security White Paper.doc

[47] OptiX OSN 500 V100R007C20 Security Configuration, Maintenance, and Hardening Manual.doc

[48] OSN 550 V100R007C20 Product Description 01(pdf).zip

[49] OSN 550 V100R007C20 Hardware Description 01(pdf).zip

[50] OptiX OSN 550 Quick Installation Guide 03(pdf).zip

[51] OptiX OSN 550 Quick Installation Guide for Outdoor Cabinets (APM30H&TMC11H) 04(pdf).zip

[52] OptiX OSN 550 V100R007C20 Security White Paper.doc

[53] OptiX OSN 550 V100R007C20 Security Configuration, Maintenance, and Hardening Manual.doc

[54] OSN 580 V100R007C20 Product Description 01(pdf).zip

[55] OSN 580 V100R007C20 Hardware Description 01(pdf).zip

[56] OptiX OSN 580 Quick Installation Guide 02(pdf).zip

[57] OptiX OSN 580 Quick Installation Guide for Outdoor Cabinets (Mini-shelter) 01(pdf).zip

[58] OptiX OSN 580 V100R007C20 Security White Paper.doc

[59] OptiX OSN 580 V100R007C20 Security Configuration, Maintenance, and Hardening Manual.doc

[60] OSN 1500 V200R013C20 Product Description 01

[61] OSN 1500 V200R013C20 Hardware Description 01

[62] OSN 1500 Quick Installation Guide 13

[63] OptiX OSN 1500 V200R013C20 Security White Paper.doc

[64] OptiX OSN 1500 V200R013C20 Security Configuration, Maintenance, and Hardening Manual.doc

[65] OSN 1500 V200R013C20 Product Description 01

[66] OSN 1500 V200R013C20 Hardware Description 01

[67] OSN 1500 Quick Installation Guide 13

[68] OptiX OSN 1500 V200R013C20 Security White Paper.doc

[69] OptiX OSN 1500 V200R013C20 Security Configuration, Maintenance, and Hardening Manual.doc

[70] OSN 3500 V200R013C20 Product Description 01

[71] OSN 3500 V200R013C20 Hardware Description 01

[72] OSN 3500 Quick Installation Guide 16

[73] OptiX OSN 3500 V200R013C20 Security White Paper.doc

[74] OptiX OSN 3500 V200R013C20 Security Configuration, Maintenance, and Hardening Manual.doc

[75] OSN 7500 V200R013C20 Product Description 01

[76] OSN 7500 V200R013C20 Hardware Description 01

[77] OSN 7500 Quick Installation Guide 16

[78] OptiX OSN 7500 V200R013C20 Security White Paper.doc

[79] OptiX OSN 7500 V200R013C20 Security Configuration, Maintenance, and Hardening Manual.doc

[80] OSN 7500 II V200R013C20 Product Description 01

[81] OSN 7500 II V200R013C20 Hardware Description 01

[82] OSN 7500 II Quick Installation Guide 07

[83] OptiX OSN 7500II V200R013C20 Security White Paper.doc

[84] OptiX OSN 7500II V200R013C20 Security Configuration, Maintenance, and Hardening Manual.doc

[85] RTN 360 V100R001C00 Product Documentation

[86] RTN 380 V100R002C00 Product Documentation

[87] RTN 905 1A&2A&1C V100R007C00 Product Documentation

[88] RTN 905 1A&2A&1C V100R007C00 Product Documentation

[89] RTN 905 1E&2E V100R007C00 Product Documentation

[90] RTN 950 V100R007C00 Product Documentation

[91] RTN 950A V100R007C00 Product Documentation

[92] RTN 980 V100R007C00 Product Documentation

[93] RTN 980L V100R007C00 Product Documentation

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of USP running on Huawei Transmission Equipment Series (WDM/OTN, SDH/MSTP, RTN) version v100R13C00 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 versions of the product evaluated were USP running on Huawei Transmission Equipment Series (WDM/OTN, SDH/MSTP, RTN) and version:

WDM/OTN product series:

Chassis	Product Version	USP Software Version
OptiX OSN 1800 I	V100R005C10SPC210	USPV100R013C00
OptiX OSN 1800 II	V100R005C10SPC210	USPV100R013C00
OptiX OSN 1800 V	V100R005C10SPC210	USPV100R013C00
OptiX OSN 8800 T64	V100R009C00SPC300	USPV100R013C00
OptiX OSN 8800 T32	V100R009C00SPC300	USPV100R013C00
OptiX OSN 8800 T16	V100R009C00SPC300	USPV100R013C00
OptiX OSN 6800	V100R009C00SPC300	USPV100R013C00
OptiX OSN 6800A	V100R009C00SPC300	USPV100R013C00
OptiX OSN 3800	V100R009C00SPC300	USPV100R013C00
OptiX OSN 3800A	V100R009C00SPC300	USPV100R013C00
OptiX OSN 9800 U64	V100R001C20SPC300	USPV100R013C00
OptiX OSN 9800 U32	V100R001C20SPC300	USPV100R013C00
OptiX OSN 9600 U64	V100R001C20SPC300	USPV100R013C00
OptiX OSN 9600 U32	V100R001C20SPC300	USPV100R013C00

SDH/MSTP product series:

Chassis	Product Version	USP Software Version

Chassis	Product Version	USP Software Version
OptiX OSN 500	V100R007C20SPH203	USPV100R013C00
OptiX OSN 550	V100R007C20SPH203	USPV100R013C00
OptiX OSN 580	V100R007C20SPH203	USPV100R013C00
OptiX OSN 1500A	V200R013C20SPH303	USPV100R013C00
OptiX OSN 1500B	V200R013C20SPH303	USPV100R013C00
OptiX OSN 3500	V200R013C20SPH303	USPV100R013C00
OptiX OSN 7500	V200R013C20SPH303	USPV100R013C00
OptiX OSN 7500 II	V200R013C20SPH303	USPV100R013C00

RTN product series

Chassis	Product Version	USP Software Version
OptiX RTN 380	V100R002C00SPH201	USPV100R013C00
OptiX RTN 360	V100R001C00SPH101	USPV100R013C00
OptiX RTN 9051C	V100R007C00SPH102	USPV100R013C00
OptiX RTN 9051A	V100R007C00SPH102	USPV100R013C00
OptiX RTN 9052A	V100R007C00SPH102	USPV100R013C00
OptiX RTN 9051E	V100R007C00SPH102	USPV100R013C00
OptiX RTN 9052E	V100R007C00SPH102	USPV100R013C00
OptiX RTN 950	V100R007C00SPH102	USPV100R013C00
OptiX RTN 950A	V100R007C00SPH102	USPV100R013C00
OptiX RTN 980	V100R007C00SPH102	USPV100R013C00
OptiX RTN 980L	V100R007C00SPH102	USPV100R013C00

These products are also described in this report as the Target of Evaluation (TOE). The developer was Huawei Technologies.

The TOE is the Huawei USP running on Transmission Equipment Series (OptiX OSN 1800/3800/3800A/6800/6800A/8800/9600/9800, OptiX OSN 500/550/580, OptiX OSN 1500(A/B)/3500/7500/7500 II, and OptiX RTN 360/380/905(1A/1C/1E/2A/2E)/950/950A/980/980L),which consists of the hardware and the software.

The Transmission network equipment provides management interfaces and service interfaces, the interfaces are different in type and quantity for different divices.

The USP is the software core of the transmission equipment. It is the software platform for managing and running communication networking functionalities.

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 by ALC_CMC.4 and ALC_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.UnwantedNetworkTraffic** The traffic here only refers to the traffic on management interfaces, that means, the Unwanted Network Traffic threat only exist on management plane. The Unwanted network traffic may come from an attacker and should be filtered. The overloaded traffic may cause a failure of the TOE to respond to system control and normal management operations.
- **T.UnauthenticatedAccess** An unauthenticated person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE, exhausting system resources.
- **T.UnauthorizedAccess** A user with restricted action and information access authorization gains access to unauthorized commands or information. This threat also includes data leakage to non-intended person or device.
- **T.Eavesdrop** An eavesdropper (remote attacker) is able to intercept, and potentially modify, or re-use information assets that are exchanged between the TOE and EMS.

4.9 Threats Countered by the TOE's environment

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

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

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

- A syslog server to store logs;
- An EMS to manage the TOE;
- A RADIUS server to provide external authentication/authorization decisions.

4.12 IT Security Objectives

The following objectives must be met by the TOE:

- **O.DeviceAvail** The TOE shall ensure its own availability.
- **O.DataFilter** The TOE shall ensure that only allowed management traffic goes through the TOE.
- **O.Authorization** The TOE shall implement different authorization role that can be assigned to users in order to restrict the functionality that is available to individual administrators.
- **O.Authentication** The TOE must authenticate users for access.
- **O.Audit** The TOE shall provide functionality to generate audit records for security-relevant administrator actions.
- **O.Communication** The TOE must implement logical protection measures for network communication between the TOE and LMT/RMT from the operational environment.

4.13 Non-IT Security Objectives

The following objectives must be met by the operational environment:

- OE.**Physical** The TOE (i.e., the complete system including attached peripherals, such as a board, and CF card inserted in the transmission equipment) shall be protected against unauthorized physical access.
- OE.**NetworkElements** The operational environment shall provide securely and correctly working network devices as resources that the TOE needs to cooperate with. Behaviors of such network devices provided by operational environment shall be also secure and correct. For example, EMS used for TOE management, Syslog servers, and Radius servers for obtaining authentication and authorization decisions.
- OE.**NetworkSegregation** The operational environment shall provide segregation by deploying the management interface in TOE into an independent local network.

- OE.**Person** Personnel working as authorized administrators shall be carefully selected for trustworthyness and trained for proper operation of the TOE.

4.14 Security Functional Requirements

The following functional requirements are met by the TOE:

FAU_GEN.1	Audit Data Generation
FAU_GNE.2	User Identity Association
FAU_SAR.1	Audit Review
FAU_SAR.2	Restricted Audit Review
FAU_STG.1	Protected Audit Trail Storage
FAU_STG.3	Action in Case of Possible Audit Data Loss
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Security Attribute based Access Control
FDP_DAU.1	Basic Data Authentication
FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1	Simple Security Attributes
FIA_AFL.1	Authentication Failure Handling
FIA_ATD.1	User Attribute Definition
FIA_SOS.1	Verification of Secrets
FIA_UAU.1	Timing of Authentication
FIA_UAU.5	Multiple Authentication Mechanisms
FIA_UID.1	Timing of identification
FMT_MOF.1	Management of Security Functions Behavior
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 Timestamps
FTA_SSL.3	TSF-initiated Termination
FTA_TSE.1	TOE Session Establishment
FTP_ITC.1	Trusted Channel(SFTP)
FTP_ITC.1	Trusted Channel (SSL)
FTP_ITC.1	Trusted Channel (WebLCT)
FTP_ITC.1	Trusted Channel (Mobile LCT) (for RTN products only)

4.15 Security Function Policy

The USP is the software core of the transmission equipment. It is the software platform for managing and running communication networking functionalities.

USP provides service configuration and product software management features.

USP provides extensive security features. These features include different interfaces for various access modes, enforced authentication prior to establishment of administrative sessions with the TOE, and auditing of security-related management activities, as well as flexible logging and auditing of events.

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 final Evaluation Technical Report (ETR)[7] to SERTIT in 22-12-2014. 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 versions of its components have 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 provided by the developer. Huawei Transmission Equipment Series Certified Configuration [8] 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 7 different categories, each containing between 1 and 11 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 at least 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 certain that there is no overlap between these tests and the evaluator independent tests, thereby maximizing coverage.

All the repeated tests are performed by the developer under the witness of the evaluator. The evaluator also analyzed the Developer Test Plan to see where additional ATE tests could be performed, and selected 6 additional tests

All of these tests were performed at the Huawei premises in Wuhan in 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 USP running on Huawei Transmission Equipment Series (WDM/OTN, SDH/MSTP, RTN) version v100R13C00 meet the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL3 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 USP running on Huawei Transmission Equipment Series (WDM/OTN, SDH/MSTP, RTN) version v100R13C00 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.

The RTN360/380 series are full outdoor equipment. The user shall be aware about this and take proper precaution/action to detect/prevent physical tampering as per guidance instructs.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of: USP Running on Huawei Transmission Equipment Series (OptiX OSN 1800/3800/3800A/6800/6800A/8800/9600/9800, OptiX OSN 500/550/580, OptiX OSN 1500(A/B)/3500/7500/7500 II, and OptiX RTN 360/380/905(1A/1C/1E/2A/2E)/950/950A/980/980L)

- Chassis of WDM/OTN product series

Chassis	Product Version	USP Software Version
OptiX OSN 1800 I	V100R005C10SPC210	USPV100R013C00
OptiX OSN 1800 II	V100R005C10SPC210	USPV100R013C00
OptiX OSN 1800 V	V100R005C10SPC210	USPV100R013C00
OptiX OSN 8800 T64	V100R009C00SPC300	USPV100R013C00
OptiX OSN 8800 T32	V100R009C00SPC300	USPV100R013C00
OptiX OSN 8800 T16	V100R009C00SPC300	USPV100R013C00
OptiX OSN 6800	V100R009C00SPC300	USPV100R013C00
OptiX OSN 6800A	V100R009C00SPC300	USPV100R013C00
OptiX OSN 3800	V100R009C00SPC300	USPV100R013C00
OptiX OSN 3800A	V100R009C00SPC300	USPV100R013C00
OptiX OSN 9800 U64	V100R001C20SPC300	USPV100R013C00
OptiX OSN 9800 U32	V100R001C20SPC300	USPV100R013C00
OptiX OSN 9600 U64	V100R001C20SPC300	USPV100R013C00
OptiX OSN 9600 U32	V100R001C20SPC300	USPV100R013C00

- Chassis of MSTP product series

Chassis	Product Version	USP Software Version
OptiX OSN 500	V100R007C20SPH203	USPV100R013C00
OptiX OSN 550	V100R007C20SPH203	USPV100R013C00
OptiX OSN 580	V100R007C20SPH203	USPV100R013C00
OptiX OSN 1500A	V200R013C20SPH303	USPV100R013C00
OptiX OSN 1500B	V200R013C20SPH303	USPV100R013C00
OptiX OSN 3500	V200R013C20SPH303	USPV100R013C00

Chassis	Product Version	USP Software Version
OptiX OSN 7500	V200R013C20SPH303	USPV100R013C00
OptiX OSN 7500 II	V200R013C20SPH303	USPV100R013C00

- Chassis of RTN product series

Chassis	Product Version	USP Software Version
OptiX RTN 380	V100R002C00SPH201	USPV100R013C00
OptiX RTN 360	V100R001C00SPH101	USPV100R013C00
OptiX RTN 9051C	V100R007C00SPH102	USPV100R013C00
OptiX RTN 9051A	V100R007C00SPH102	USPV100R013C00
OptiX RTN 9052A	V100R007C00SPH102	USPV100R013C00
OptiX RTN 9051E	V100R007C00SPH102	USPV100R013C00
OptiX RTN 9052E	V100R007C00SPH102	USPV100R013C00
OptiX RTN 950	V100R007C00SPH102	USPV100R013C00
OptiX RTN 950A	V100R007C00SPH102	USPV100R013C00
OptiX RTN 980	V100R007C00SPH102	USPV100R013C00
OptiX RTN 980L	V100R007C00SPH102	USPV100R013C00

TOE Documentation

The supporting guidance documents evaluated were:

[a] Huawei Transmission Equipment Series Certified Configuration v1.4

[b] OSN 1800 I/II Compact Multi-Service Edge Optical Transport Platform V100R005C10 Product Documentation-01

[c] OSN 1800 I/II Compact Multi-Service Edge Optical Transport Platform V100R005C10 Product Documentation-01

[d] OSN 1800 V Packet Enhanced V100R005C10 Deploying Your Network 01

[e] OSN 1800 V Packet Enhanced V100R005C10 Installing, Operating and Maintaining Your Network (For Field Engineer) 01

[f] OSN 1800 V Packet Enhanced V100R005C10 Operating and Maintaining Your Network (For 1st Line Engineer) 01

[g] OSN 1800 V Packet Enhanced V100R005C10 Operating and Maintaining Your Network (For 2nd Line Engineer) 01

[h] OSN 1800 V Packet Enhanced V100R005C10 Planning Your Network 01

[i] OptiX OSN 8800 V100R009C00 Product Documentation 01

[j] OptiX OSN 8800 V100R009C00 Product Documentation 01

[k] OptiX OSN 8800 V100R009C00 Product Documentation 01

[l] OptiX OSN 3800 V100R009C00 Product Documentation 01

[m] OptiX OSN 6800 V100R009C00 Product Documentation 01

[n] OptiX OSN 8800 6800A 3800A V100R008C00 Product Documentation 01(NA)

[o] OptiX OSN 8800 6800A 3800A V100R008C00 Product Documentation 01(NA)

[p] OSN 9800 V100R001C20 Planning Your Network 01

[q] OSN 9800 V100R001C20 Installing, Operating and Maintaining Your Network (For Field Engineer) 01

[r] OSN 9800 V100R001C20 Operating and Maintaining Your Network (For 2nd Line Engineer) 01

[s] OSN 9800 V100R001C20 Operating and Maintaining Your Network (For 1st Line Engineer) 01

[t] OSN 9800 V100R001C20 Deploying Your Network 01

[u] OSN 9800 V100R001C20 Planning Your Network 01

[v] OSN 9800 V100R001C20 Installing, Operating and Maintaining Your Network (For Field Engineer) 01

[w] OSN 9800 V100R001C20 Operating and Maintaining Your Network (For 2nd Line Engineer) 01

[x] OSN 9800 V100R001C20 Operating and Maintaining Your Network (For 1st Line Engineer) 01

[y] OSN 9800 V100R001C20 Deploying Your Network 01

[z] OSN 9600 V100R001C20 运维指导（网络运维工程师用书）01

[aa] OSN 9600 V100R001C20 运维指导（网络监控工程师用书）01

[bb] OSN 9600 V100R001C20 开局指导 01

[cc] OSN 9600 V100R001C20 规划指导 01

[dd] OSN 9600 V100R001C20 站点操作指导 01

[ee] OSN 9600 V100R001C20 运维指导（网络运维工程师用书）01

[ff] OSN 9600 V100R001C20 运维指导（网络监控工程师用书）01

[gg] OSN 9600 V100R001C20 开局指导 01

[hh] OSN 9600 V100R001C20 规划指导 01

[ii] OSN 9600 V100R001C20 站点操作指导 01

[jj] OSN 500 V100R007C20 Product Description 01(pdf).zip

[kk] OSN 500 V100R007C20 Hardware Description 01(pdf).zip

[ll] OptiX OSN 500 Quick Installation Guide 04(pdf).zip

[mm] OptiX OSN 500 V100R007C20 Security White Paper.doc

[nn] OptiX OSN 500 V100R007C20 Security Configuration, Maintenance, and Hardening Manual.doc

[oo] OSN 550 V100R007C20 Product Description 01(pdf).zip

[pp] OSN 550 V100R007C20 Hardware Description 01(pdf).zip

[qq] OptiX OSN 550 Quick Installation Guide 03(pdf).zip

[rr] OptiX OSN 550 Quick Installation Guide for Outdoor Cabinets (APM30H&TMC11H) 04(pdf).zip

[ss] OptiX OSN 550 V100R007C20 Security White Paper.doc

[tt] OptiX OSN 550 V100R007C20 Security Configuration, Maintenance, and Hardening Manual.doc

[uu] OSN 580 V100R007C20 Product Description 01(pdf).zip

[vv] OSN 580 V100R007C20 Hardware Description 01(pdf).zip

[ww] OptiX OSN 580 Quick Installation Guide 02(pdf).zip

[xx] OptiX OSN 580 Quick Installation Guide for Outdoor Cabinets (Mini-shelter) 01(pdf).zip

[yy] OptiX OSN 580 V100R007C20 Security White Paper.doc

[zz] OptiX OSN 580 V100R007C20 Security Configuration, Maintenance, and Hardening Manual.doc

[aaa] OSN 1500 V200R013C20 Product Description 01

[bbb] OSN 1500 V200R013C20 Hardware Description 01

[ccc] OSN 1500 Quick Installation Guide 13

[ddd] OptiX OSN 1500 V200R013C20 Security White Paper.doc

[eee] OptiX OSN 1500 V200R013C20 Security Configuration, Maintenance, and Hardening Manual.doc

[fff] OSN 1500 V200R013C20 Product Description 01

[ggg] OSN 1500 V200R013C20 Hardware Description 01

[hhh] OSN 1500 Quick Installation Guide 13

[iii] OptiX OSN 1500 V200R013C20 Security White Paper.doc

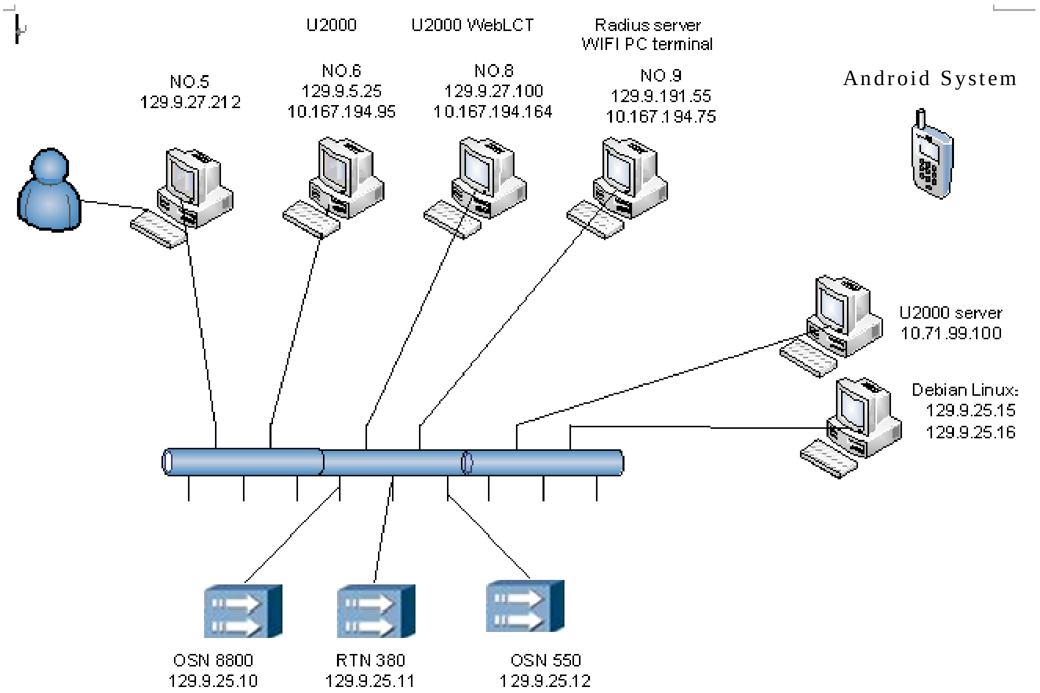
TOE Configuration

The following configuration was used for testing:

Item	Identifier
HARDWARE	One of the hardware models listed in section "TOE Identification" for each series
SOFTWARE	The software listed in TOE Identification for each series configured according to [a] in section "TOE Documentation".
MANUAL	The appropriate guidance document in section "TOE Documentation", for each series

Environmental Configuration

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



[jjj] OptiX OSN 1500 V200R013C20 Security Configuration, Maintenance, and Hardening Manual.doc

[kkk] OSN 3500 V200R013C20 Product Description 01

[lll] OSN 3500 V200R013C20 Hardware Description 01

[mmm] OSN 3500 Quick Installation Guide 16

[nnn] OptiX OSN 3500 V200R013C20 Security White Paper.doc

[ooo] OptiX OSN 3500 V200R013C20 Security Configuration, Maintenance, and Hardening Manual.doc

[ppp] OSN 7500 V200R013C20 Product Description 01

[qqq] OSN 7500 V200R013C20 Hardware Description 01

[rrr] OSN 7500 Quick Installation Guide 16

[sss] OptiX OSN 7500 V200R013C20 Security White Paper.doc

[ttt] OptiX OSN 7500 V200R013C20 Security Configuration, Maintenance, and Hardening Manual.doc

[uuu] OSN 7500 II V200R013C20 Product Description 01

[vvv] OSN 7500 II V200R013C20 Hardware Description 01

[www] OSN 7500 II Quick Installation Guide 07

[xxx] OptiX OSN 7500II V200R013C20 Security White Paper.doc

[yyy] OptiX OSN 7500II V200R013C20 Security Configuration, Maintenance, and Hardening Manual.doc

[zzz] RTN 360 V100R001C00 Product Documentation

[aaaa] RTN 380 V100R002C00 Product Documentation

[bbbb] RTN 905 1A&2A&1C V100R007C00 Product Documentation

[cccc] RTN 905 1A&2A&1C V100R007C00 Product Documentation

[dddd] RTN 905 1E&2E V100R007C00 Product Documentation

[eeee] RTN 950 V100R007C00 Product Documentation

[ffff] RTN 950A V100R007C00 Product Documentation

[gggg] RTN 980 V100R007C00 Product Documentation

[hhhh] RTN 980L V100R007C00 Product Documentation

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

Certificate

Product Manufacturer: Huawei Technologies

Product Name: USP running on Huawei Transmission Equipment Series (WDM/OTN, SDH/MSTP, RTN)

Type of Product: Switch

Version and Release Numbers: Version V100R013C00

Assurance Package: EAL 3 augmented with ALC_ FLR.2

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-065 CR, issue 1.0, 2 June 2015

Certificate Identifier: SERTIT-065 C

Date Issued: 2 June 2015

Kjartan Jæger Kvassnes
Certifier

Arne H. Rage
Arne Høye Rage
Quality Assurance

Øystein Hole
Øystein Hole
Head of SERTIT

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.

SERTIT
Norwegian Certification Authority for IT Security

SOGIS