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

SERTIT-042 CR Certification Report

Issue 1.0 25.02.2013

ZTE Optical Transmission Equipment Series, version ZXONE 5800 v1.10, ZXMP S325 v2.10, ZXMP S385 v2.60, ZXMP M720 v1.00, ZXMP M820 v2.51, ZXWM M920 V4.20P01, ZXONE 8300 v1.00, ZXONE 8500 v1.00

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

SERTIT, P.O. Box 14, N-1306 Bærum postterminal, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

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

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

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

* Mutual Recognition under the CC recognition arrangement applies to EAL 2 but not to ALC_FLR.2.

Contents

1 Certification Statement

ZTE Corporation ZTE Optical Transmission Equipment Series is an Optical Transmission Equipment that provides functions such as voice and data services, increasing transmission capacity over optical network.

ZTE Optical Transmission Equipment Series version ZXONE 5800 v1.10, ZXMP S325 v2.10, ZXMP S385 v2.60, ZXMP M720 v1.00, ZXMP M820 v2.51, ZXWM M920 V4.20P01, ZXONE 8300 v1.00, ZXONE 8500 v1.00 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and have met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL 2 augmented with ALC_FLR.2 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended functionality in the specified environment when running on the platforms specified in Annex A.

Author	Kvassnes, Kjartan Jæger Certifier
Quality Assurance	Arne Høye Rage Quality Assurance Arne H. Rage
Approved	Kjell W. Bergan Head of SERTIT Kjell W. Bergan
Date approved	28.02.2013

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
CWDM	Coarse WDM
DWDM	Dense WDM
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
FE	Fast Ethernet
GE	Gigabit Ethernet
JTAG	Joint Test Action Group
NNI	Network-to-Network Interface
NMS	Network Management System
NTP	Network Time Protocol
OC	Optical Carrier
OTE	Optical Transmission Equipment
POC	Point of Contact
QP	Qualified Participant
SDH	Synchronous Digital Hierarchy
SDH/WDM	SDH or WDM
SERTIT	Norwegian Certification Authority for IT Security
SPM	Security Policy Model
ST	Security Target
STM	Synchronous Transport Module
TOE	Target of Evaluation

TSF	TOE Security Functions
TSP	TOE Security Policy
UNI	User Network Interface
WDM	Wave Division Multiplexing

3 References

[1] Security Target of the ZTE Optical Transmission Equipment Series ZXMP M720, ZXMP M820, ZXWM M920, ZXONE 8300, ZXONE 8500, ZXONE 5800, ZXMP S325 and ZXMP S385, version 1.2, 14 august 2012.

[2] Common Criteria Part 1, CCMB-2009-07-001, Version 3.1 R3, July 2009.

[3] Common Criteria Part 2, CCMB-2009-07-002, Version 3.1 R3, July 2009.

[4] Common Criteria Part 3, CCMB-2009-07-003, Version 3.1 R3, July 2009.

[5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2009-07-004, Version 3.1 R3, July 2009.

[7] Common Criteria EAL2+ Evaluation of ZTE Optical Transmission Equipment Series, version 1.2, 15 August 2012.

[8] NetNumen™ U31 R22 Unified Element Management System Security Management Operation Guide (System Management), V12.11.20P01 R1.0, 2011/09/30

[9] NetNumen™ U31 R22 Unified Element Management System Security Management Operation Guide (General Operation), V12.11.20P01 R1.0, 2011/09/30.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of ZTE Optical Transmission Equipment Series version ZXONE 5800 v1.10, ZXMP S325 v2.10, ZXMP S385 v2.60, ZXMP M720 v1.00, ZXMP M820 v2.51, ZXWM M920 V4.20P01, ZXONE 8300 v1.00, ZXONE 8500 v1.00 to the Sponsor, ZTE Corporation, 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 ZTE Optical Transmission Equipment Series and version ZXONE 5800 v1.10, ZXMP S325 v2.10, ZXMP S385 v2.60, ZXMP M720 v1.00, ZXMP M820 v2.51, ZXWM M920 V4.20P01, ZXONE 8300 v1.00, ZXONE 8500 v1.00.

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

The TOE is an Optical Transmission Equipment that provides functions such as voice and data services, increasing transmission capacity over optical network

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

4.3 TOE scope

The TOE scope is described in the ST[1], chapter 1.3.

4.4 Protection Profile Conformance

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

4.5 Assurance Level

The assurance incorporated predefined evaluation assurance level EAL 2, augmented with 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

The TOE security policies are described in the ST[1], chapter 3.1

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. Most of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

This Security Target introduces one extended component: FAU_GEN.3 Simplified audit data generation. This component is a simplified version of FAU_GEN.1 and is therefore a suitable member of the FAU_GEN family. It was added to remove the need to log start and stop of auditing and to simplify the requirement.

4.8 Threats Countered

- T.CONFIDENTIALITY
  TA.CLIENT-SIDE is able to read traffic that he is not allowed to read
- T.INTEGRITY
  TA.CLIENT-SIDE is able to modify traffic that he is not allowed to modify
- T.UNAUTHORISED
  TA.ROGUE_USER performs actions on the TOE that he is not authorized to do
- T.AUTHORISED
  TA.ROGUE_USER performs actions on the TOE that he is authorized to do, but these are undesirable and it cannot be shown that this user was responsible.

4.9 Threats Countered by the TOE's environment

- T.PHYSICAL_ATTACK
  TA.PHYSICAL gains physical access to the TOE (OTE, EMS or machine running the EMS Client) 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 Management Network and the SDH/WDM network are trusted. It is also assumed that the NMS and NTP Server are trusted and will not be used to attack the TOE.

4.12 IT Security Objectives

- O. ACCESS

  The TOE shall ensure that client-side equipment can:

  - Only send data across the network to certain other client-side equipment
  - Only receive data across the network from that client-side equipment
  - Is not able to modify data that is not created by it or sent to it.

- O.AUTHORISE

  The TOE shall support a flexible role-based authorization framework with predefined and customizable roles. These roles can use the TOE to manage the SDH/WDM network , and manage the TOE itself. Each role allows a user to perform certain actions, and the TOE shall ensure that users can only perform actions when they have a role that allows this.

- O.AUTHENTICATE

  The TOE shall support a flexible authentication framework, allowing the TOE to accept/reject users based on: username/password and a configurable subset of IP/MAC-addressand time of login.

- O.AUDITING

  The TOE shall support flexible logging and auditing of events.

4.13 Non-IT Security Objectives

- OE.SERVER_SECURITY

  The customer shall ensure that the EMS Server and the Optical Transmission Equipment shall be protected from physical attacks.

- OE.CLIENT_SECURITY

  The customer shall ensure that management workstations that host the EMS Client, are protected from physical and logical attacks that would allow attackers to subsequently:

  - Disclose passwords or other sensitive information
  - Hijack the client
  - Execute man-in-the-middle attacks between client and EMS Server or similar attacks.

- OE.TRUST&TRAIN_USERS

  The customer shall ensure that roles are only assigned to users that are sufficiently trustworthy and sufficiently trained to fulfill those roles.

- OE.TIME

  There shall be a correctly configured NTP-server available on the Management Network to supply the TOE with time.

- OE.TRUSTED_NETWORKS

  The customer shall ensure that:

  - The Management Network and SDH/WDM Network are trusted, and will not be used to attack the TOE
  - The NMS and NTP are trusted, so that they will not be used to attack the TOE

4.14 Security Functional Requirements

- FDP_IFC.1 Subset information flow control
- FDP_IFF.1 Simple security attributes
- FIA_UID.2 User identification before any action
- FIA_UAU.2 User authentication before any action
- FIA_AFL.1 Authentication failure handling
- FIA_SOS.1 Verification of secrets
- FTA_SSL.3 TSF-initiated termination
- FTA_MCS.1 Basic limitation on multiple concurrent sessions
- FMT_SMR.1 Security roles
- FDP_ACC.2 Complete access control
- FDP_ACF.1 Security attribute based access control
- FAU_GEN.3 Audit data generation
- FAU_SAR.1 Audit review
- FAU_STG.1 Protected audit trail storage
- FAU_STG.4 Prevention of audit data loss
- FMT_SMF.1 Specification of Management Functions

4.15 Security Function Policy

The major security features of the TOE are:

- Transport data to/from client-side equipment across the SDH/WDM network in such a way that:
  - Only the intended recipients are able to read the signal
  - Nobody can modify the signals
- Supports a flexible role-based authorization framework with predefined and customizable roles for management. These roles can use the TOE to manage the SDH/WDM network, and manage the TOE itself.
- Supports a flexible authentication framework, allowing the TOE to accept/reject users based on: username/password and a configurable subset of IP/MAC-address and time of login.
- Supports 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 at the 15th of August 2012. 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. These classes comprise the EAL 2 assurance package augmented with ALC_FLR.2

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	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_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.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the guidance in the Operational User Guidance documents [8][9] provided by the developer.

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. Brightsight tested the potential vulnerabilities on the final version of the TOE at the premises of ZTE, Shenzhen and Beijing, China in July 2012. Testing was performed by Brightsight personnel at ZTE's premises in Shenzhen and Beijing.

5.6 Developer's Tests

No developer tests were replicated as these tests were performed previously during testing of the EMS component in a related EAL2+ evaluation.

5.7 Evaluators' Tests

The evaluators considered the results of the EAL2 evaluation of the EMS platform in formulating a testing strategy for the OTE series products. The majority of the security functionality for the OTE is implemented in the EMS client and server components. The majority of developer testing for OTE corresponds with the developer testing for the EMS. Therefore the evaluators chose to focus on a subset of tests that were specific to the OTE components.

Evaluator testing was conducted at the developer's test network. Brightsight performed these tests based on the final version of the TOE in July 2012. Testing was conducted from ZTE office in Shenzhen (SDH) and Beijing (WDM).

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 ZTE Optical Transmission Equipment Series version ZXONE 5800 v1.10, ZXMP S325 v2.10, ZXMP S385 v2.60, ZXMP M720 v1.00, ZXMP M820 v2.51, ZXWM M920 V4.20P01, ZXONE 8300 v1.00, ZXONE 8500 v1.00 meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 2 augmented with ALC_FLR.2 for the specified Common Criteria Part 2 extended functionality, in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of ZTE Optical Transmission Equipment Series version ZXONE 5800 v1.10, ZXMP S325 v2.10, ZXMP S385 v2.60, ZXMP M720 v1.00, ZXMP M820 v2.51, ZXWM M920 V4.20P01, ZXONE 8300 v1.00, ZXONE 8500 v1.00 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 OTE, EMS server and an EMS Client:

OTE

ZXONE 5800 v1.10	
Hardware	ZXONE 5800
Software	ZXONE 5800 v1.10
Guidance	Installation Manual R1.2 Maintenance Manual (Volume I) Routine Maintenance R1.1 Maintenance Manual (Volume II) Alarm and Performance R1.2 Maintenance Manual (Volume III) Troubleshooting R1.1 Security Issue R1.1
ZXMP S325 v2.10	
Hardware	ZXMP S325
Software	ZXMP S325 v2.10
Guidance	Installation Manual R1.0 Maintenance Manual R1.0 Security Issue R1.1
ZXMP S385 v2.60	
Hardware	ZXMP S385
Software	ZXMP S385 v2.60
Guidance	Installation Manual R1.0 Maintenance Manual (Volume I) Routine Maintenance R1.0 Maintenance Manual (Volume II) Alarm and Performance R1.0 Maintenance Manual (Volume III) Troubleshooting R1.0 Security Issue R1.1
ZXMP M720 v1.00	
Hardware	ZXMP M720
Software	ZXMP M720 v1.00
Guidance	Hardware Descriptions R1.1 Installation Manual R1.1 Maintenance Manual R1.0 Security Issue R1.1
ZXMP M820 v2.51	
Hardware	ZXMP M820
Software	ZXMP M820 v2.51
Guidance	Hardware Descriptions (Volume I) R1.1 Hardware Descriptions (Volume II) R1.0 Installation Manual R1.1 Maintenance Manual (Volume I) Routine Maintenance R1.1 Maintenance Manual (Volume II) Alarm and Performance R1.1

	Maintenance Manual (Volume III) Troubleshooting R1.1 Security Issue R1.1
ZXWM M920 V4.20P01	
Hardware	ZXWM M920
Software	ZXWM M920 V4.20P01
Guidance	Hardware Descriptions (Volume I) R1.0 Hardware Descriptions (Volume II) R1.0 Installation Manual R1.0 Maintenance Manual (Volume I) Routine Maintenance R1.0 Maintenance Manual (Volume II) Alarm and Performance R1.0 Maintenance Manual (Volume III) Troubleshooting R1.0 Security Issue R1.1
ZXONE 8300 v1.00	
Hardware	ZXONE 8300
Software	ZXONE 8300 v1.00
Guidance	Hardware Descriptions (Volume I) R1.2 Hardware Descriptions (Volume II) R1.2 Installation Manual R1.1 Maintenance Manual (Volume I) Routine Maintenance R1.2 Maintenance Manual (Volume II) Alarm and Performance R1.2 Maintenance Manual (Volume III) Troubleshooting R1.1 Security Issue R1.1
ZXONE 8500 v1.00	
Hardware	ZXONE 8500
Software	ZXONE 8500 v1.00
Guidance	Hardware Description (Volume I) R1.3 Hardware Description (Volume II) R1.3 Installation Manual R1.2 Maintenance Manual (Volume I) Routine Maintenance R1.3 Maintenance Manual (Volume II) Alarm and Performance R1.3 Maintenance Manual (Volume III) Troubleshooting R1.2 Security Issue R1.1

EMS Server

EMS U31 R22 v12.12.20	

Hardware	SUN M5000，CPU 4x2.53GHz SPARC64 VII four-core Processors;
	Memory 32GB(8*4GB);Disks 2x300GB;
	4*1000 Mbps Ethernet ports

Software	EMS Server version NetNumen U31 R22 v12.12.20 Java version 1.6.0_21 Java(TM) SE Runtime Environment (build 1.6.0_21-b06) Java HotSpot(TM) Server VM (build 17.0-b16, mixed mode) Oracle Solaris 10 update 8 Oracle Database 10g Enterprise Edition Release 10.2.0.4.0 - (64bit)
Guidance	Operation Guide (General Operations) R1.0

(common)	Operation Guide (System Management) R1.0 Routine Maintenance Guide R1.0 User Guide (Northbound CORBA Interface) R1.0 User Guide (Northbound SNMP Interface) R1.0 User Guide (Northbound XML Interface) R1.0
Guidance (SDH-specific)	Operation Guide (SDHCTN End-to-End Management) R1.0 Operation Guide (SDH NE Management) R1.0 SDH Security Issues (in preparation)
Guidance (WDM-specific)	Operation Guide (WDMOTN End-to-End Management) R1.0 Operation Guide (WDMOTN NE Management) R1.0 WDM Security Issues (in preparation)

EMS Client

EMS CLIENT	NAME AND VERSION
Software	EMS Client version NetNumen U31 R22 V12.12.20
Workstation	A Workstation suitable to run the OS (see below)
OS	Windows, Linux or Solaris suitable to run java (see below)
Java	Java(TM) SE Runtime Environment (build 1.6.0_21-b06)
Java HotSpot(TM)	Client VM (build 17.0-b16, mixed mode)

TOE Documentation

The supporting guidance documents evaluated were:

[a] Security Target ZTE Optical Transmission Equipment Series v1.2

[b] ZTE WDM-SDH FSP-TDS-ARC v0.1

[c] ALC_DEL.1, ALC_CMC.2, ALC_CMS.2, ALC_FLR.2 for OTE 0.1

[d] NetNumen U31 (R22 V12.12.20) Test Result (v1.0) Solaris v1.0

[e] [ATE S325] Test plan for Optical Transport Equipment (S325), [ATE S385] Test plan for Optical Transport Equipment (S385) v1.0

[f] [ATE 5800] Test plan for Optical Transport Equipment (5800) v1.0

[g] [ATE M720] CC Test Specification: Multi-transmission Platform Compact WDM Equipment (ZXMP M720) v1.0

[h] [ATE M820] CC Test Specification: Multi-transmission Platform Compact WDM Equipment (ZXMP M820) v1.0

[i] [ATE 8300] CC Test Specification: Multi-transmission Platform Compact WDM Equipment (ZXONE 8300) v1.0

[j] [ATE 8500] CC Test Specification: Multi-transmission Platform Compact WDM Equipment (ZXONE 8500) v1.0

[k] [ATE M920] CC Test Specification: Multi-transmission Platform Compact WDM Equipment (ZXWM M920) v1.0

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

TOE Configuration

The following configuration was used for testing:

ITEM	IDENTIFIER	VERSION
HARDWARE	ZXONE 5800 (SDH) ZXMP S325 (SDH) ZXMP S385 (SDH) ZXMP M720 (WDM) ZXMP M820 (WDM) ZXWM M920 (WDM) ZXONE 8300 (WDM) ZXONE 8500 (WDM) SUN M5000，CPU 4x2.53GHz SPARC64 VII four-core Processors; (EMS) Memory 32GB(8*4GB);Disks 2x300GB (EMS); 4*1000Mbps Ethernet ports (EMS)	V1.1 v2.1 v2.6 v1.00 v2.51 V4.20P01 V1.00 V1.00
SOFTWARE	ZXONE 5800 (SDH) ZXMP S325 (SDH) ZXMP S385 (SDH) ZXMP M720 (WDM) ZXMP M820 (WDM) ZXWM M920 (WDM) ZXONE 8300 (WDM) ZXONE 8500 (WDM) EMS server/client (NetNumen U31 R22 V12.12.20) (Note: The EMS client has to be installed on Windows 7 or abovOS.)™ Java version 1.6.0_21 Java(TM) SE Runtime Environment (build 1.6.0_21-b06) Java HotSpot(TM) Server VM (build 17.0-b16, mixed mode) Oracle Solaris 10 update 8 Oracle Database 10g Enterprise Edition Release 10.2.0.4.0 - (64bit)	V1.1 v2.1 v2.6 v1.00 v2.51 V4.20P01 V1.00 V1.00 R22 V12.12.20 1.6.0_21 build 17.0-b16, mixed mode v10 update 8 v10.2.0.4.0

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: ZTE Corporation

Product Name: ZTE Optical Transmission Equipment Series

Type of Product: Optical Transmission Equipment

Version and Release Numbers: ZXONE 5800 v1.10, ZXMP S325 v2.10, ZXMP S385 v2.60, ZXMP M720 v1.00, ZXMP M820 v2.51, ZXWM M920 V4.20P01, ZXONE 8300 v1.00, ZXONE 8500 v1.00

Assurance Package: EAL 2 augmented with ALC_FLR.2

Evaluation Criteria: Common Criteria version 3.1R3 (ISO/IEC 15408)

Name of IT Security Evaluation Facility: Brightsight B.V.

Name of Certification Body: SERTIT

Certification Report Identifier: SERTIT-042 CR, issue 1.0, 25 February 2013

Certificate Identifier: SERTIT-042 C

Date Issued: 25 February 2013

Kjartan Jæger Kvassnes
Certifier

Arne H. Rage
Arne Høye Rage
Quality Assurance

Kjell W. Bergan
Kjell Werner Bergan
Head of SERTIT

SERTIT
Norwegian Certification Authority for IT Security