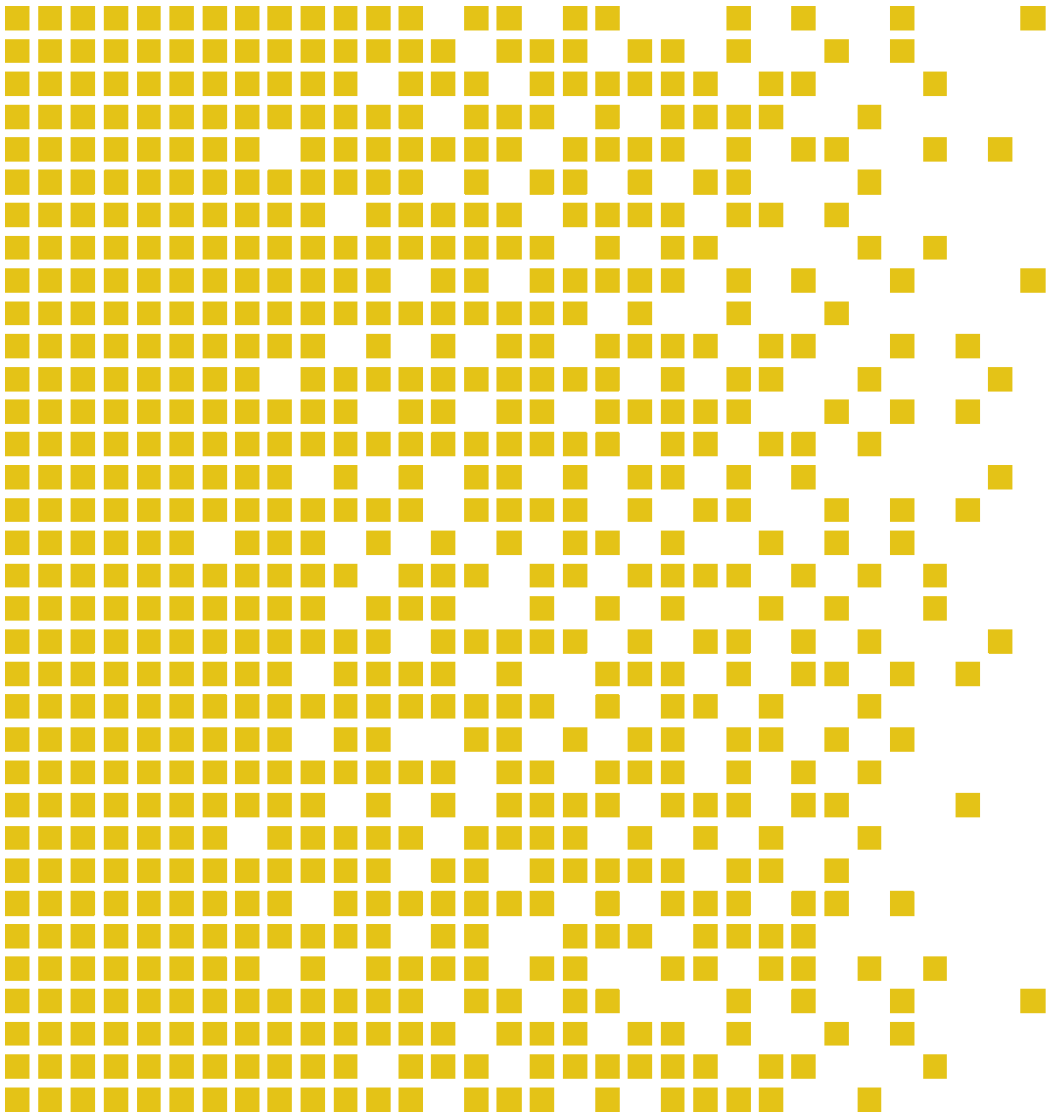
# SERTIT-029 CR Certification Report

Issue 1.0 10.11.2011

## ZXR10 M6000&T8000&8900E Series Routers and Switches Running the ZXROSNG Operating System v1.00.20





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 3 but not to ALC_FLR.2

## Contents

# 1 Certification Statement

ZTE Corporation ZXR10 M6000&T8000&8900E Series Routers and Switches Running the ZXROSNG Operating System version 1.00.20. The TOE enables the delivery of metro Ethernet services and high-density service-aware Ethernet aggregation over IP/MPLS-based networks.

ZXR10 M6000&T8000&8900E Series Routers and Switches Running the ZXROSNG Operating System version v1.00.20 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 EAL3 augmented with ALC_FLR.2 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality for 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 | 10.11.2011 |

# 2 Abbreviations

| | |
|---|---|
| ACL | Access Control List |
| ATM | Asynchronous Transfer Mode |
| BGP | Border Gateway Protocol |
| 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 Client Interface |
| CR | Cluster Router |
| DoS | Denial of Service |
| CHAP | Challenge Handshake Authentication Protocol |
| EAL | Evaluation Assurance Level |
| EOR | Evaluation Observation Report |
| ESS | Ethernet Service Switches |
| ETR | Evaluation Technical Report |
| EVIT | Evaluation Facility under the Norwegian Certification Scheme for IT Security |
| EXIF | External Interface |
| EWP | Evaluation Work Plan |
| LAN | Local Area Network |
| MAC | Media Access Control |
| MPLS | Multi-Protocol Label Switching |
| NTP | Network Time Protocol |
| OAM | Operational, Administration and Management |
| OSPF | Open Shortest Path First |
| PAP | Password Authentication Protocol |
| PoE | Power over Ethernet |
| POC | Point of Contact |
| QP | Qualified Participant |
| RADIUS | Remote Authentication Dial-In User Service |

| | |
|---|---|
| RFC | Request for Comments |
| RIP | Routing Information Protocol |
| SERTIT | Norwegian Certification Authority for IT Security |
| SNMP | Simple Network Management Protocol |
| SPM | Security Policy Model |
| SR | Service Routers |
| SSH | Secure Shell |
| ST | Security Target |
| TACACS+ | Terminal Access Controller Access Control System Plus |
| TCP | Transmission Control Protocol |
| TOE | Target of Evaluation |
| TSF | TOE Security Functions |
| TSP | TOE Security Policy |
| UDP | User Datagram Protocol |
| URPF | Unicast Reverse Path Forwarding |
| VPN | Virtual Private Network |
| QoS | Quality of Service |

# 3 References

[1] Security Target, ZTE Corporation, ZXR10 M6000&T8000&8900E Series Routers and Switches Running the ZXROSNG Operating System Security Target, Version: R1.6, 19 August 2011.

[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] Evaluation Technical Report Common Criteria EAL3+ Evaluation of ZXR10 M6000&T8000&8900E Series Routers and Switches Running the ZXROSNG Operating System version 1.3, 12 October 2011.

[8] Operational User Guidance ZTE M6000&T8000&8900E Series Routers and Switches Running ZXROSNG Operating System, Version 1.7, 25 July 2011

[9] Preparative Procedures ZTE M6000&T8000&8900E Series Routers and Switches Running ZXROSNG Operating System, Version 1.3, 4 July 2011

# 4 Executive Summary

## 4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of ZXR10 M6000&T8000&8900E Series Routers and Switches Running the ZXROSNG Operating System version v1.00.20 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 ZXR10 M6000&T8000&8900E Series Routers and Switches Running the ZXROSNG Operating System version v1.00.20.

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

The TOE is the M6000&T8000&8900E Series of Router and Switches running the ZXROSNG Operating System v1.00.20.

The TOE enables the delivery of metro Ethernet services and high-density service-aware Ethernet aggregation over IP/ MPLS-based networks. The supported protocols are layer 2 / layer 3 encapsulation and Internet Protocol (IP), and Ethernet. Other protocols may be supported by the product, but are not evaluated..

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_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 detailed in ST[1], chapter 3.3

## 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

- Actions performed by users may not be known to the administrators due to actions not being recorded or the audit records not being reviewed prior to the machine shutting down, or an unauthorized administrator modifies or destroys audit data.
- An unauthorized user may gain access to inappropriately view, tamper, modify, or delete TOE Security Functionality data
- An unauthorized entity may send impermissible information through the TOE which results in the exploitation of resources on the network
- A user may gain unauthorized access to an unattended session and alter the TOE security configuration
- An unauthorized user gains management access to the TOE and alter the TOE security configuration

## 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 authorized administrators are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance; however, they are capable of error. The administrators are trained in the appropriate use of the TOE
- All TOE external interfaces except for the network traffic/data interface are attached to the internal (trusted) network. This includes:
  [1] RADIUS, TACACS+ server interface (optional)
  [2] SNMP/SYSLOG interface (required)
  [3] NTP interface (required)
  [4] SSH interface for remote client (at least one of the local or remote administration client is required)
- The TOE will be located in an environment that provides physical security to prevent unauthorized physical access, commensurate with the value of the IT assets protected by the TOE and uninterruptible power, temperature control required for reliable operation

- External NTP services will be available

## 4.12 IT Security Objectives

- The TOE will provide the privileged administrators and authentication administrators the capability to review Audit data and will restrict audit review to administrators who have been granted explicit read-access. The TOE will generate audit records which will include the time that the event occurred and the identity of the administrator performing the event.
- The TOE must provide services that allow effective management of its functions and data and restrict access to the TOE Management functions to the privileged administrators and authentication administrators.
- The TOE must uniquely identify and authenticate the claimed identity of all administrative users before granting management access.
- The TOE shall control the flow of information among its network connections according to routing rules and BGPv4/OSPFv2/IS-IS/RIPv2 routing protocols which prevent the communication with trusted routers from modification, insertion and replay errors.
- The TOE will provide mechanisms that control an administrator's logical access to the TOE and to deny access to unattached session to configure the TOE.
- The TOE shall be able to accept routing data from trusted routers according to BGPv4/OSPFv2/IS-IS/RIPv2.

## 4.13 Non-IT Security Objectives

- NTP server must be available to provide accurate/synchronized time services to the TOE.
- All TOE external interfaces except for the network traffic/data interface are attached to the internal (trusted) network. This includes:
  [1] RADIUS, TACACS+ server interface (optional)
  [2] SNMP, SYSLOG interface (required)
  [3] NTP interface (required)
  [4] SSH interface for remote client (at least one of the local or remote administration client is required)
- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance; however, they are capable of error. The administrators are trained in the appropriate use of the TOE.
- The operational environment provides the TOE with appropriate physical security to prevent unauthorized physical access, commensurate with the value of the IT assets protected by the TOE and uninterruptible power, temperature control required for reliable operation.
- All administrators are assessed for their trustworthiness, and administrator connectivity to the TOE is restricted. Non-administrative entities may have their packets routed by the TOE, but that is the extent of their authorization

to the TOE's resources.

- The SYSLOG/SNMP server will provide the privileged administrators and authentication administrators the capability to review Audit data stored in the log servers and will restrict audit review to administrators who have been granted explicit read-access.

## 4.14 Security Functional Requirements

The TOE provides security functions to satisfy the following Security Functional Requirements (SFRs):

- FAU_GEN.1 Audit data generation
- FAU_GEN.2 User identity association
- FAU_SAR.1 Audit review
- FAU_STG.1 Protected audit trail storage
- FAU_STG.4 Prevention of audit data loss
- FDP_IFC.1(1) Subset information flow control (unauthenticated policy)
- FDP_IFF.1(1) Simple security attributes (unauthenticated policy)
- FDP_IFC.1(2) Subset information flow control (export policy)
- FDP_IFF.1(2) Simple security attributes (export policy)
- FDP_UIT.1 Data exchange integrity
- FIA_AFL.1 Authentication failure handling
- FIA_SOS.1 Verification of secrets
- FIA_UAU.2 User authentication before any action
- FIA_UAU.5 Multiple authentication mechanisms
- FIA_UID.2 User identification before any action
- FMT_MOF.1 Management of security functions behaviour
- FMT_MSA.1 Management of security attributes
- FMT_MSA.3 Static attribute initialization
- FMT_MTD.1(1) Management of TSF data
- FMT_MTD.1(2) Management of TSF data
- FMT_MTD.1(3) Management of TSF data
- FMT_MTD.1(4) Management of TSF data
- FMT_SMF.1 Specification of management functions
- FMT_SMR.1 Security roles
- FPT_STM.1 Reliable Time stamps
- FTA_SSL.3 TSF-initiated termination
- FTA_TSE.1 TOE session establishment
- FTP_ITC.1(1) Trusted channel for SSH client
- FTP_ITC.1(2) Trusted channel for RADIUS/TACACS+ server
- FTP_ITC.1(3) Trusted channel for NTP

## 4.15 Security Function Policy

The TOE provides:

- Handling of packet flows using the BGPv4/OSPFv2/IS-IS/RIPv2 protocols

- Local and remote administration
- Authentication, either in the TOE or through TACACS+ or RADIUS.
- Administrator Profiles to permit or deny access to a hierarchical branch or specific commands.
- Audit functions
- Management and configuration of the TOE
- Mitigation of DoS attacks
- URPF (Unicast Reverse Path Forwarding) to limit the malicious traffic

## 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 final Evaluation Technical Report (ETR)[7] to SERTIT in 12 October 2011. 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_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.3 | Authorisation controls |
| | ALC_CMS.3 | Implementation representation CM coverage |
| | ALC_DEL.1 | Delivery procedures |
| | ALC_DVS.1 | Identification of security measures |
| | ALC_FLR.2 | Flaw reporting procedures |
| | 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/evaluated versions of its consistent 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 in the Operational User Guidance [8] and Preparative Procedures[9] documents 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 TOE is substantially similar to other router/switches on the market. This technology is well-established. The technology and possible vulnerabilities are described in a series of public documents.

The evaluators assessed all possible vulnerabilities found during evaluation. This resulted in a shortlist with a number of possible vulnerabilities to be tested. The evaluators assessed which potential vulnerabilities were already tested by the developer and assessed the results. The remaining potential vulnerabilities where tested by the evaluator.

## 5.6 Developer's Tests

The testing results from the developer show that the TOE exhibits the expected behaviour at TSFI and SFR enforcing module level. The developers test specification are directly linked to its corresponding functional specification, and passing one test shows that that specific functional specification works according to the documentation.

The developer test effort is considered already fairly complete. Any major missing features reported by the evaluators are added to the developer test set. Nevertheless the evaluator has defined 8 additional tests.

In May 2011 tests on a preliminary version of the TOE are performed at the premises of Brightsight. Subsequently the evaluator has witnessed tests of similar TOEs at the site of ZTE in Nanjing, China from 7 – 10 June 2011. During the tests the evaluator has extended some tests to create more variety in the tests. As a last step the evaluators have tested the final TOE at the premises of Brightsight, in July 2011.

## 5.7 Evaluators' Tests

For independent testing, the evaluator has chosen to perform some additional testing although the developer's testing was extensive but some additional assurance could be gained by additional testing.

For independent testing, the evaluator has repeated 11 of the 40 developer's tests. For each of the TSFI available one test was performed.

# 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 ZXR10 M6000&T8000&8900E Series Routers and Switches Running the ZXROSNG Operating System version v1.00.20 meet the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL3 augmented with 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 ZXR10 M6000&T8000&8900E Series Routers and Switches Running the ZXROSNG Operating System version v1.00.20 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 M6000&T8000&8900E Series of Router and Switches running the ZXROSNG Operating System v1.00.20.The M6000&T8000&8900E series consists of the Cluster Routers (CR), Ethernet Service Switches (ESS)s and Service Routers (SR)s as listed below. The major difference between models is the type, capacity and number of the physical interfaces. No other hardware requirements are applicable.

| SERIES | MODEL | INTERFACE DESCRIPTION | TYPE |
|---|---|---|---|
| M6000-n Series | M6000-8 | 8 x PFU<br>4 x SFU<br>2 x MPU | SR |
| | M6000-16 | 16 x PFU<br>4 x SFU<br>2 x MPU | |
| | 1. MPU supported interfaces:<br>a. 1 x Ethernet Management Interface<br>b. 1 x RS232 Console<br>2. PFU supported interfaces:<br>a. 1-port 10 Gbps Electronical Ethernet<br>b. 4-port 10 Gbps Electronical Ethernet<br>c. 10-port 1 Gbps Optical Ethernet<br>d. 12-port Gigabit Optical Interface<br>e. 16-Port 100M Electrical Interface<br>f. 40-port Gigabit Optical interface<br>g. 48-port Gigabit Electrical interface<br>h. 1-Port IEEE1588 LAN/WAN Interface<br>i. 2-Port IEEE1588 LAN/WAN Interface<br>3. SFU supported interface: none | | |
| M6000-nS Series | M6000-3S | 3 x PFU<br>2 x MPU | SR |
| | M6000-5S | 5 x PFU<br>2 x SRU | |
| | M6000-8S | 8 x PFU<br>2 x SRU<br>2 x SFU | |
| | 1. MPU/SRU supported interfaces:<br>a. 1 x Ethernet Management Interface<br>b. 1 x RS232 Console<br>2. FPU supported interfaces:<br>a. 2-port 10GE LAN/WAN Interface<br>b. 12-port Gigabit combo Interface<br>3. SFU supported interface: none | | |
| T8000 Series | T8000 | 16 x PFU<br>4 x SFU<br>2 x MPU | CR |

| SERIES | MODEL | INTERFACE DESCRIPTION | TYPE |
|---|---|---|---|
| | 1. MPU supported interfaces:<br>a. 1 x Ethernet Management Interface<br>b. 1 x RS232 Console<br>2. PFU supported interfaces:<br>a. 1-port 10 Gbps Electronical Ethernet<br>b. 4-port 10 Gbps Electronical Ethernet<br>c. 10-port 1 Gbps Optical Ethernet<br>d. 16-Port 100M Electrical Interface<br>e. 48-port Gigabit Electrical interface<br>3. SFU supported interface: none | | |
| 8900E Series | 8902E | 2 x MCS<br>2 x LIC | ESS |
| | 8905E | 2 x MCS<br>5 x LIC | |
| | 8908E | 2 x MCS<br>8 x LIC | |
| | 8912E | 2 x MCS<br>12 x LIC | |
| | 1. MCS supported interfaces:<br>a. 1 x Ethernet Management Interface<br>b. 1 x RS232 Console<br>2. LIC supported interfaces:<br>a. 8-port 10GE Optical Ethernet<br>b. 12-port 10GE Optical interface<br>c. 48-port Gigabit Electrical interface<br>d. 48 port Gigabit Optical interface | | |

## TOE Documentation

The supporting guidance documents evaluated were:

[a] Operational User Guidance ZTE M6000&T8000&8900E Series Routers and Switches Running ZXROSNG Operating System, Version 1.7, 25 July 2011

[b] Preparative Procedures ZTE M6000&T8000&8900E Series Routers and Switches Running ZXROSNG Operating System, Version 1.3, 4 July 2011

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

## TOE Configuration

The TOE is tested on three representative samples from the M6000&T8000&8900E, the M6000-16, T8000-16 and 8902E.

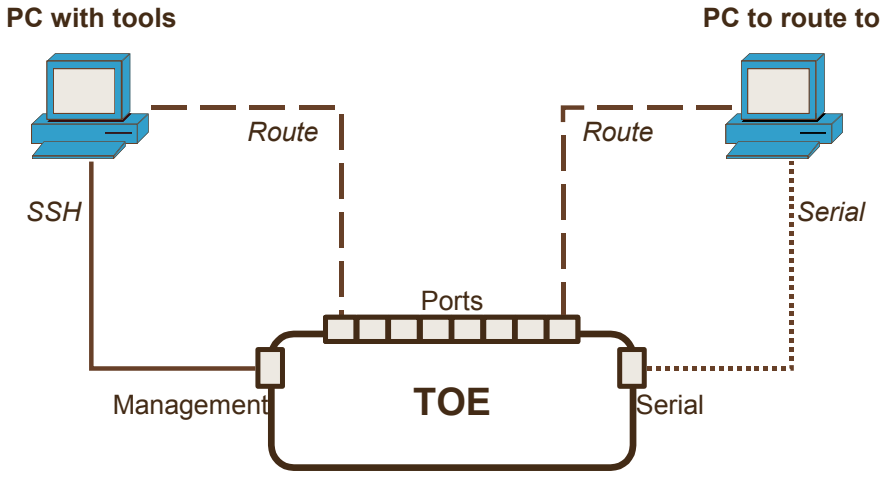
```
ZXR10 M6000-16
ZTE ZXR10 Software, Version: M6000 v1.00.30(1.0.70), ZXROSNG V1.00.20, Release
software
Build on 2011/06/07 09:27:25

ZXR10 T8000-16
ZTE ZXR10 Software, Version: T8000v1.00.12(1.0.70), ZXROSNG V1.00.20, Release
software
Build on 2011/06/07 09:27:25

ZXR10 8902E Software, 8900&8900E Version: V3.00.01.B08P06, ZXROSNG V1.00.20
RELEASE SOFTWARE
Compiled 2011-6-8, 16:51:27
```

## Environmental Configuration

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



# Certificate

*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.*

**Product Manufacturer:** ZTE Corporation

**Product Name:** ZXR10 M6000&T8000&8900E Series Routers and Switches Running the ZXROSNG Operating System

**Type of Product:** Router Operating System

**Version and Release Numbers:** Version 1.00.20

**Assurance Package:** EAL 3 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-029 CR, issue 1.0, 10 November 2011

**Certificate Identifier:** SERTIT-029 C

**Date Issued:** 10 November 2011

Kjartan Jæger Kvassnes
Certifier

Lars Borgos
Quality Assurance

Kjell Werner Bergan
Head of SERTIT

SERTIT
Norwegian Certification Authority for IT Security