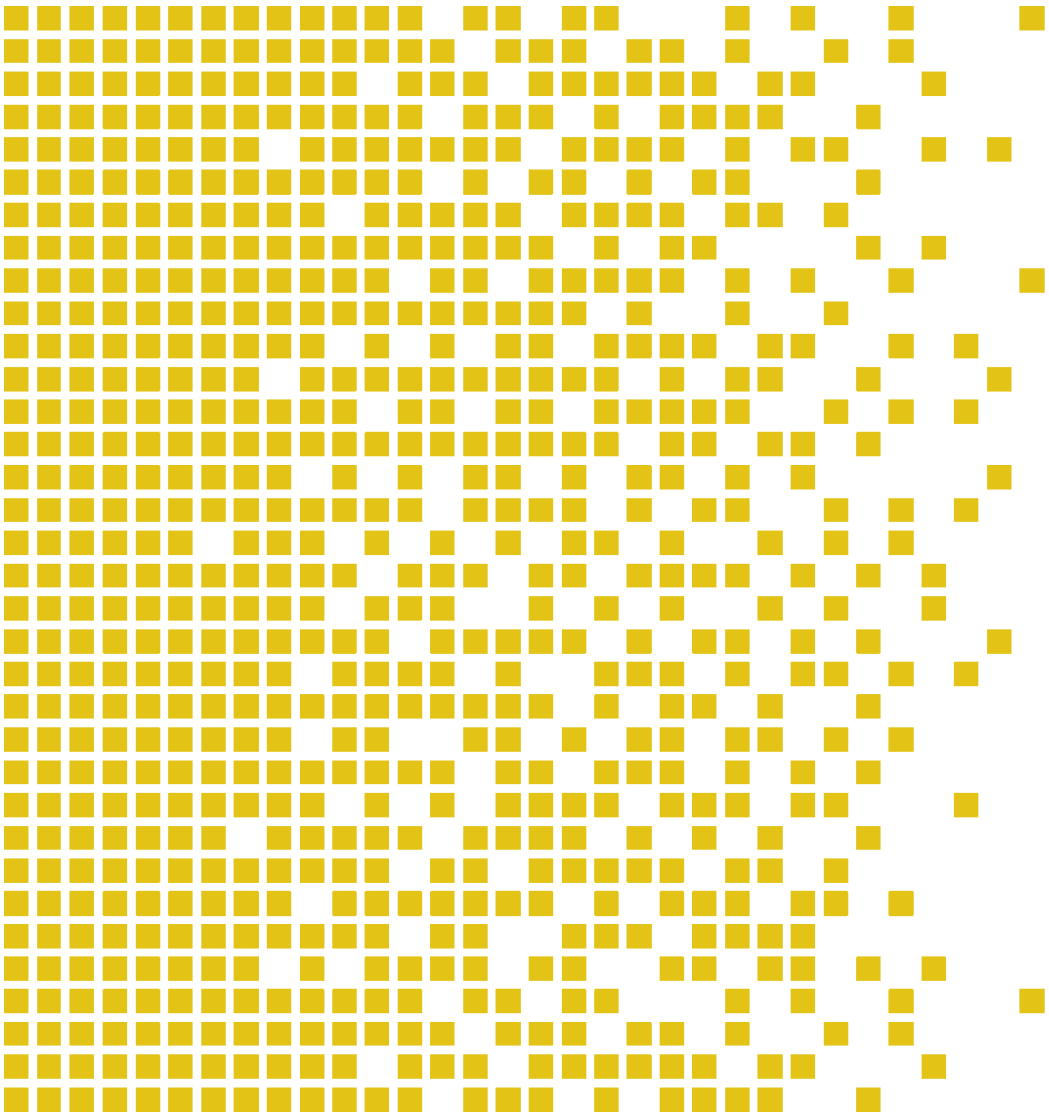
SERTIT-036 CR Certification Report

Issue 1.0 28.06.1012

ZTE eNodeB solution v1.0



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 eNodeB solution is a single node in the Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) for Long-Term Evolution (LTE) network plus an EMS and client.

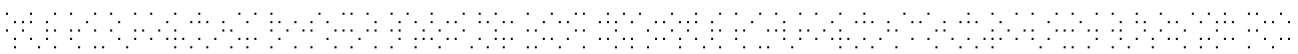
ZTE eNodeB solution version v1.0 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and have met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL 2 augmented by ALC_FLR.2 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality in the specified environment when running on the platforms specified in Annex A.

Author	Kvassnes, Kjartan Jæger Certifier
Quality Assurance	Arne Høye Rage Quality Assurance
Approved	Kjell W. Bergan Head of SERTIT
Date approved	28.06.1012

2 Abbreviations

AC	Alternating Current
BBU	baseband unit
BPL	Baseband Processing module
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
DC	Direct Current
EAL	Evaluation Assurance Level
EMS	Element Management System
eNode B	Evolved Node B
EOR	Evaluation Observation Report
EPS	Evolved Packet System
ETR	Evaluation Technical Report
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
FA	Fan Array Module
IP	Internet Protocol
IPSEC	Internet Protocol Secure
L3	Layer 3
LED	Light Emitting Diode
LTE	Long-Term Evolution
MAC	Media Access Control
MME	Mobility Management Entity
NAS	Non-Access Stratum
NTP	Network Time Protocol
PDCP	Packet Data Convergence Protocol
PHY	Physical Layer

PM	Power Module
POC	Point of Contact
QP	Qualified Participant
RF	Radio Frequency
RLC	Radio Link Control
RRU	Remote Radio Unit
SA	Site alarm Board
SE	Site alarm Extension Board
SEG	Security gateway
SERTIT	Norwegian Certification Authority for IT Security
S-GW	Serving Gateway
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
UE	User Equipment
UMTS	Universal Mobile Telecommunications System



3 References

[1] ZTE eNodeB Solution Security Target, v.0.8, 09 feb 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] Evaluation Technical Report Common Criteria EAL2+ Evaluation of ZTE eNodeB Solution, v 1.1, 27 Febuary 2012.

[8] Certified Configuration - ZTE eNodeB solution Common Criteria Security Evaluation – Certified Configuration R1.0

[9] NetNumen U31 R18 (V12.11.40) Security Management Operation Guide

[10] NetNumen U31 R18 (V12.11.40) Management Operation Guide

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of ZTE eNodeB solution version v1.0 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 eNodeB solution version v1.0.

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

The TOE is a single node in the Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) for Long-Term Evolution (LTE) network plus an EMS and client.

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 by 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. 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.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.

- T.UNKNOWN_ USER

TA.NETWORK gains unauthorized access to the TOE and is able to perform actions on the TOE.

- T. NETWORK

TA.NETWORK is able to modify/read external network traffic originating from / destined for the TOE and thereby:

  - perform actions on the TOE
  - gain unauthorized knowledge about traffic between parts of the TOE and/or between the TOE and the SEG, another BBU and/or UE.

- T.PHYSICAL_ATTACK

TA.PHYSICAL gains physical access to the TOE and is able to perform actions on the TOE.

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

It is assumed that:

- The SEG and other BBU are trusted, and will not be used to attack the TOE.
- The L3 switch will block all traffic between EMS and Core Network/IP Management network except for:
  - Selected traffic between EMS and EMS Client
  - Selected traffic between EMS and BBU

It is also assumed that the backhaul network, the Core Network and IP Management Network are separated and the Core Network is trusted.

4.12 IT Security Objectives

- O. AUTHENTICATE

The TOE shall support client user authentication, allowing the TOE to accept/reject users based on username and password.

- O. AUTHORISE

The TOE shall support a flexible role-based authorization framework with predefined and customizable roles. These roles can use the Client to manage the TOE. 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.AUDITING

The TOE shall support logging and auditing of user actions.

- O.PROTECT_COMMUNICATION

The TOE shall protect communication between:

- BBU and SGE
- BBU and other BBU
- BBU and UE
- EMS Client and EMS Server

against disclosure, undetected modification and masquerading.

4.13 Non-IT Security Objectives

- OE.CLIENT_SECURITY

The operator shall ensure that workstations that host one of the Clients 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 Server or similar attacks.

- OE.SERVER_SECURITY

The operator shall ensure that the TOE shall be protected from physical attacks.

- OE.TIME

The NTP Server shall supply the TOE with reliable time.

- OE.TRUST&TRAIN_USERS

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

- OE.TRUSTED_SYSTEMS

The operator shall ensure that:

- the SEG and other BBU are trusted, and will not be used to attack the TOE.

  - The L3 switch will block all traffic between EMS and Core Network/IP management network except for:
    - Selected traffic between EMS and EMS Client
    - Selected traffic between EMS and BBU
  - The L3 switch will block all traffic between BBU and backhaul except for IPSec communications.
- OE.NETWORK

The operator shall ensure that the backhaul network, the Core Network and IP Management Network are separated and ensure the security of the Core Network.

4.14 Security Functional Requirements

- 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
- FAU_GEN.1 Audit data generation
- FAU_SAR.1 Audit review
- FAU_STG.1.Protected audit trail storage
- FAU_STG.4 Prevention of audit data loss
- FDP_ITT.1.CLI Basic internal transfer protection
- FTP_ITC.1.SEG Inter-TSF trusted channel
- FTP_ITC.1.BBU Inter-TSF trusted channel
- FTP_ITC.1.UE Inter-TSF trusted channel
- FMT_SMF.1.Specification of Management Functions
- FDP_ACC.2 Complete access control
- FDP_ACF.1 Security attribute based access control

4.15 Security Function Policy

The TOE has the following general functionalities:

- Radio resource management: radio bearer control, radio admission control,
- Access mobility management, uplink/downlink dynamic resource allocation.
- IP header compression and user data stream encapsulation.
- Selecting MME during UE attaching progress
- Routing user plane data to S-GW
- Paging message scheduling and transmission
- Broadcast message scheduling and transmission.
- Measurement used for mobility and scheduling, and configuration of measurement report

Major security features of the TOE:

- Secure management and usage of the TOE, to ensure that only properly authorized staff can manage and/or use the TOE.
- Provides secure interaction between various parts of the TOE and between the TOE and various machines in the environment, so that user data and/or management commands cannot be read or modified in between

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 on 27.02 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[8][9][10] 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 evaluators assessed all possible vulnerabilities found during evaluation of the classes. This resulted in a list of possible vulnerabilities to be tested.

The evaluators assessed which potential vulnerabilities were already tested by the developer and assessed the results.

Brightsight tested the remaining potential vulnerabilities on the final version of the TOE at the premises of ZTE, Sian, China through remote terminal clients in December 2011 and January, February 2012.

5.6 Developer's Tests

The developer test effort is considered already fairly complete. Any major missing tests have been added to the developer test set. And the developer integrated tests for similar functionality into bigger test case. Nevertheless the evaluator has modified 10 additional tests for the EMS and BBU subsystems as the evaluator's independent tests.

5.7 Evaluators' Tests

For independent testing, the evaluator has repeated 6 and modified 10 out of the 29 developer's tests (16 evaluator's ATE_IND.2 tests in total). For each of the TSFI available at least one test is performed.

Brightsight performed these tests based on the final version of the TOE at the premises of ZTE, Sian, China through remote terminal clients in December 2011 and January, February 2012.

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 eNodeB solution version v1.0 meet 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 conformant functionality, in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of ZTE eNodeB solution version v1.0 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

There is no special hardware requirement. Since the TOE already includes the hardware components. The configuration of the hardware is listed below:

TYPE	NAME AND VERSION	
Hardware	BBU	B8200 (V2.00)
	RRU	R8964 (V5.00) or R8962 (v2.00)
	EMS	Sun M4000, 2*4 Core CPUs, 32GB Memory 2 146G SAS Disks, Dual-port HBA cards ST6180 8*300G FC15K Disk Array

TOE Documentation

The supporting guidance documents evaluated were:

Certified Configuration - ZTE eNodeB solution Common Criteria Security Evaluation – Certified Configuration R1.0

Standard guidance:

[a] - NetNumen U31 R18 (V12.11.40) Product Description

[b] - NetNumen U31 R18 (V12.11.40) Maintenance Guide

[c] - NetNumen U31 R18 (V12.11.40) MML Command Reference

[d] - NetNumen U31 R18 (V12.11.40) Security Management Operation Guide

[e] - NetNumen U31 R18 (V12.11.40) Log Management Operation Guide

[f] - NetNumen U31 R18 (V12.11.40) Fault Management Operation Guide

[g] - NetNumen U31 R18 (V12.11.40) Management Operation Guide

[h] - NetNumen U31 R18 (V12.11.40) MML Terminal Operation Guide

[i] - ZXSDR R8962 L26A(V1.00)TDD LTE RRU Hardware Installation

[j] - ZXDSR R8962 L26A(V1.00)TDD LTE RRU User Manual

[k] - ZXSDR R8964(V5.00)TD-LTE Remote Radio Unit Hardware Installation

[l] - ZXSDR R8964(V5.00) TD-LTE Remote Radio Unit User Manual

[m] - ZXSDR B8200 TL200(V2.00) TD-LTE Baseband Resource Unit System Description

[n] - ZXSDR B8200 TL200(V2.00) TD-LTE Baseband Resource Unit Hardware Installation

[o] - ZXSDR B8200 TL200(V2.00) TD-LTE Baseband Resource Unit Hardware Description

[p] - IPSec configuration guide

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

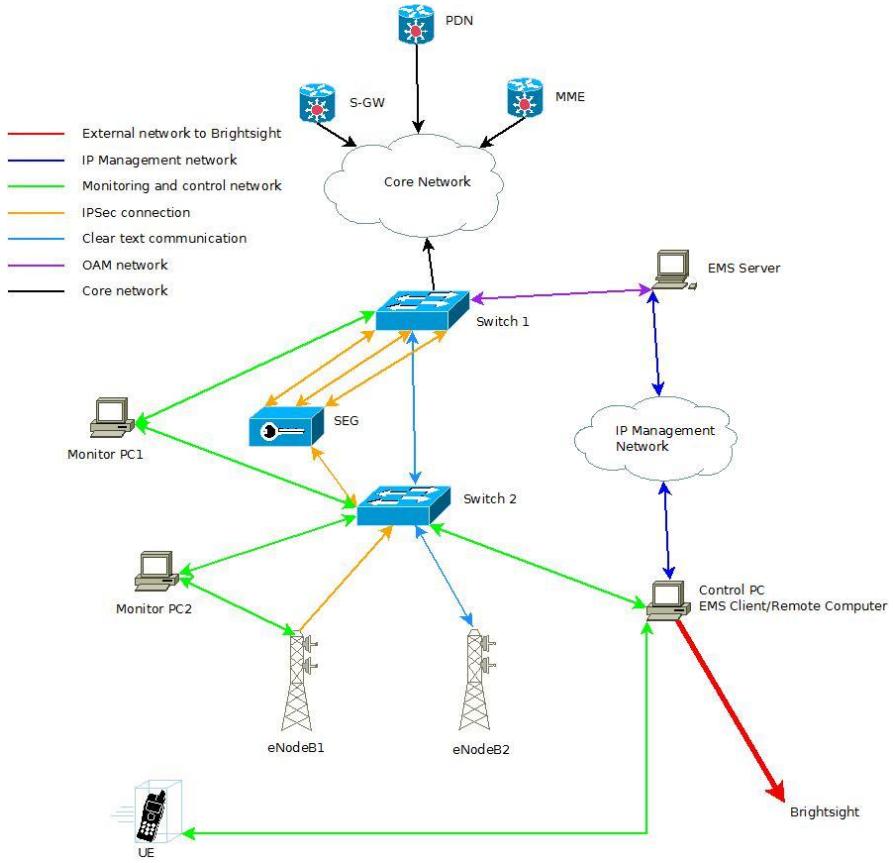
TOE Configuration

The following configuration was used for testing:

HARDWARE	B8200 * 2 - BBU1(eNodeB1), BBU2(eNodeB2) R8964 * 1 - RRU1(eNodeB1) R8962 *1 - RRU2(eNodeB2) Sun M4000, 2*4 Core CPUs, 32GB Memory (EMS) 2 146G SAS Disks, Dual-port HBA cards (EMS) ST6180 8*300G FC15K Disk Array (EMS)
SOFTWARE	TD-LTE (eNodeB) (V2.00.041) EMS Server server NetNumen U31 R18 V12.11.40 Java(TM) SE Runtime Environment (build 1.6.0_21-b06) Java HotSpot(TM) 64-bit Server VM (build 17.0-b16, mixed mode) Solaris 10 U9 SPARC Oracle 11.2.0.2 EE 64 bit for Solaris SPARC

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: ZTE eNodeB solution

Type of Product: Base Station Controller

Version and Release Numbers: Version 1.0

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-036 CR, issue 1.0, 28 June 2012

Certificate Identifier: SERTIT-036 C

Date issued: 28 June 2012

Kjartan Jæger Kvassnes
Certifier

Arne Høye Rage
Quality Assurance

Kjell W. Bergan
Head of SERTIT

SERTIT
Norwegian Certification Authority for IT Security