SERTIT

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

SERTIT-038 CR Certification Report

Issue 1.0 14.09.2012

ZTE Base Station Controller Series version ZTE ZXG10 iBSC Base Station Controller, V6.20.614, ZXC10 BSCB CDMA2000 Base Station Controller, V8.0.3.400, and ZXWR RNC WCDMA Radio Network Controller, V3.09.30

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 Base Station Controller Series is a base station controller that provides functions such as voice and data services, mobility management including handover and reselection, resource management including access control, channel allocation, circuit management, GPRS and EDGE.

ZTE Base Station Controller Series version ZTE ZXG10 iBSC Base Station Controller, V6.20.614, ZXC10 BSCB CDMA2000 Base Station Controller, V8.0.3.400, and ZXWR RNC WCDMA Radio Network Controller, V3.09.30 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 EAL2 augmented with 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	Lars Borgos Quality Assurance
Approved	Kjell W. Bergan Head of SERTIT Kjell W. Bergan
Date approved	14.09.2012

2 Abbreviations

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
EAL	Evaluation Assurance Level
EMS	Element Management System
EOR	Evaluation Observation Report
EPS	Evolved Packet System
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
FA	Fan Array Module
L3	Layer 3
LTE	Long-Term Evolution
MAC	Media Access Control
MME	Mobility Management Entity
NAS	Non-Access Stratum
NTP	Network Time Protocol
OMM	Operation and Maintenance Module
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 Base Station Controllers Security Target, v 1.0, 5 May 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 Base Station Controller Series, v 1.3, 29 August 2012.

[8] CC Security Evaluation – Certified Configuration v R1.0.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of ZTE Base Station Controller Series version ZTE ZXG10 iBSC Base Station Controller, V6.20.614, ZXC10 BSCB CDMA2000 Base Station Controller, V8.0.3.400, and ZXWR RNC WCDMA Radio Network Controller, V3.09.30 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 versions of the product evaluated was ZTE Base Station Controller Series and version ZTE ZXG10 iBSC Base Station Controller, V6.20.614, ZXC10 BSCB CDMA2000 Base Station Controller, V8.0.3.400, and ZXWR RNC WCDMA Radio Network Controller, V3.09.30.

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

The TOE is a base station controller that provides functions such as voice and data services, mobility management including handover and reselection, resource management including access control, channel allocation, circuit management, GPRS and EDGE

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. 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:

  - performs actions on the BSC, EMS and the EMS Client.
  - gains unauthorized knowledge about traffic between the BSC and EMS, EMS client and EMS.

4.9 Threats Countered by the TOE's environment

- T.PHYSICAL_ATTACK

  TA.PHYSICAL gains physical access to the TOE 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 PSTN, Service Part Private Network, Wireless Network, Core Network and Secure Network are trusted networks, and will not be used to attack the TOE
- The L3 switch will block all traffic from/to the external network except for
  - Selected traffic between BSC and EMS
  - Selected traffic between OMM client and BSC

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:

  - The BSC/OMM and EMS
  - The EMS and the EMS client against masquerading, disclosure and modification

4.13 Non-IT Security Objectives

- OE.CLIENT_SECURITY

  The operator shall ensure that workstations hosting 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 BSC and EMS, and EMS Client and EMS, or similar attacks.
- OE.SERVER_SECURITY

  The operator shall ensure that the BSC and EMS shall be protected from physical attacks.

- OE.PROTECT_COMMUNICATION

  The operator shall configure the Secure Network to protect communication between the TOE and NTP against masquerading and modification

- 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 fulfil those roles.

- OE.TRUSTED_SYSTEMS

  The operator shall ensure that:

  - the NTP, are trusted, and will not be used to attack the TOE.
  - The PSTN, Service Part Private Network, Wireless Network, Core Network and Secure Network are trusted networks, and will not be used to attack the TOE
  - The L3 switch will block all traffic from/to the external network except for:
    - Selected traffic between EMS and BSC/OMM
    - Selected traffic between EMS and EMS Client

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.EMS Basic internal transfer protection
- FDP_ITT.1.BSC Basic internal transfer protection
- 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 iBSC, RNC and BSCB has the following general functionalities:

- Telecommunications functionality
  - Interact with Core Network and Wireless Network to perform as the access control and network optimization equipment
- Management:
  - Manage and configure the TOE
  - Interact with EMS to be managed and configured.

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 29.08.2012. 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 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 document [8] 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 evaluator tested the potential vulnerabilities on the final version of the TOE at the premises of ZTE, Sian, China through remote terminal clients in March/April 2012.

5.6 Developer's Tests

The evaluators considered the results of the EAL2 evaluation of the EMS platform in formulating a testing strategy for the BSC products. The majority of the security functionality for the BSC is implemented in the EMS client and server components. The majority of developer testing for BSC corresponds with the developer testing for the EMS.

5.7 Evaluators' Tests

Evaluator testing was conducted via a Citrix session into the developer's test network, thus ensuring that the evaluation test environment is equivalent to the developer's testing environment. The evaluator performed these tests based on the final version of the TOE in April 2012. Testing was conducted from the evaluators lab in Singapore and from the ZTE office in Shanghai. Tests were conducted from

Shanghai due to network conditions between ZTE and Singapore affecting the responsiveness of the Citrix remote sessions.

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 Base Station Controller Series version ZTE ZXG10 iBSC Base Station Controller, V6.20.614, ZXC10 BSCB CDMA2000 Base Station Controller, V8.0.3.400, and ZXWR RNC WCDMA Radio Network Controller, V3.09.30 meet the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL2 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 Base Station Controller Series version ZTE ZXG10 iBSC Base Station Controller, V6.20.614, ZXC10 BSCB CDMA2000 Base Station Controller, V8.0.3.400, and ZXWR RNC WCDMA Radio Network Controller, V3.09.30 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 configurations of the hardware are listed below:

ZXG10 iBSC

TYPE	NAME AND VERSION
Hardware	BIPI (for Access Unit) GLI (for Switch Unit) GUP (for Process Unit) OMP(for O&M Unit) PWRD(for Peripheral Monitoring Unit) SBCX (for the OMM)
Software	ZXG10 iBSC (V6.20.614) OMM V6.20.614
Software	OMM Client V6.20.614

ZXWR RNC

TYPE	NAME AND VERSION
Hardware	GIPI, EIPI(for Access Unit) GLI (for Switch Unit) RUB, RCB (for Process Unit) OMP(for O&M Unit) PWRD(for Peripheral Monitoring Unit) SBCX (for the OMM)
Software	ZXWR RNC (V3.09.30) OMM V3.09.30
Software	OMM Client V3.09.30

ZXC10 BSCB

TYPE	NAME AND VERSION
Hardware	ABES/ABPM(for Access Unit) CHUB/THUB (for control plane switching Unit) CLKD/CLKG(for clock driver/generator unit) GCM(for GPS unit) DTB/SDTB(for TDM Interface Unit) GLIQV/GLI(Line Interface Board) IBBE(for BSC-Inter-Connect Unit) ICM (Integrated clock Module) INLP/ SPB (Signaling processing and E1/T1 interface Unit) SIPI/IPI (for IP Signaling/Bearer Interface) IWFB (for IWF Unit) MP (for Processing Unit) OMP (for O&M Unit) PSN (for Packet Switch Network Unit) PWRD (for Power Unit) SDU (for Select/Distribute Unit) UIM/GUIM(for Switch Unit) UPDC /UPCF/ IPCF (for PCF & PTT) VTCD (for Voice Transcode Unit)
Software	ZXC10 BSCB (V8.0.3.400)OMM V3.08.34.00
Software	OMM Client V3.08.34.00

TOE Documentation

The supporting guidance documents evaluated were:

Certified Configuration

[a] CC Security Evaluation – Certified Configuration

Standard Guidance:

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

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

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

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

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

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

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

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

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

[k] iBSC Product Description

[l] Base Station Controller Documentation Guide

[m] Base Station Controller System Description

[n] Harware Description

[o] Hardware Installation Guide

[p] Base Station Controller Routine Maintenance

[q] Base Station Controller Emergency Maintenance

[r] Base Station Controller Software Installation Guide

[s] Feature Configuration Guide

[t] Data Management Operation Guide

[u] Base Station Controller Software Version Management Operation Guide

[v] Diagnosis Test

[w] MML Command Reference

[x] Alarm Handling Reference

[y] Notification Handling Reference

[z] Parts Replacement Guide

[aa] System Management Operation Guide

[bb] Security Management Operation Guide

[cc] Log Management Operation Guide

RNC Standard Guidance

[dd] Product Description

[ee] Alarm and Notification Handling Reference

[ff] Radio Parameter Reference

[gg] Documentation Guide

[hh] System Description

[ii] Hardware Description

[jj] Hardware Installation Guide

[kk] Trouble Shooting

[ll] Routine Maintenance

[mm] Emergency Maintenance

[nn] Log Service

[oo] MML Command Reference

[pp] OMM Software Installation Guide

[qq] Test Management Operation Guide

[rr] Software Management Operation Guide

[ss] Calling Trace Operation Guide

[tt] Radio Configuration Operation Guide

[uu] Dynamic Data Management Operation Guide

[vv] Configuration Tool Operation Guide

[ww] Hardware Replacement Guide

[xx] Ground Configuration Operation Guide

[yy] Manage Object Model Description

[zz] Specifications and Requirements for IRPS

[aaa] System Management Operation Guide

[bbb] Security Management Operation Guide

[ccc] Log Management Operation Guide

BSCB CDMA2000 Standard Guidance

[ddd] System Documentation Guide

[eee] System Basic Principle

[fff] System Product Overview

[ggg] System interface and Protocol Description

[hhh] Controller Technical Manual

[iii] Controller Hardware Manual

[jjj] Controller installation Manual

[kkk] System Cable Preparation Manual

[lll] System DIP Switches and Jumpers Reference Manual

[mmm] Controller Routine Maintenance Manual

[nnn] Station System Trouble shooting Manual

[ooo] System Emergency maintenance Manual

[ppp] System Alarm Handling Manual

[qqq] System Configuration Parameter (Overview)

[rrr] Configuration Parameter Manual(1x Release A)

[sss] Configuration Parameter Manual (DO)

[ttt] System Configuration Parameter Manual (A Ap Interface)

[uuu] Configuration Parameter Manual_V5 Interface

[vvv] Configuration Parameter Manual(Physical Inventory Data)

[www] Configuration Parameter Manual(Physical Configuration Data)

[xxx] System Common Timer Description

[yyy] System Command Manual_System Tools

[zzz] System Command Manual_Configuration Management

[aaaa] System Command Manual_Radio Configuration 1X

[bbbb] System Command Manual_Radio Configuration DO

[cccc] System Performance Management Counter Description_1x

[dddd] System Performance Management Counter Description_EV-DO

[eeee] System Performance Management Counter Description_PTT

[ffff] System Call Failure Reason and Call Drop Explanation_1X

[gggg] Call Failure Reason and Call Drop Explanation(EV-DO)

[hhhh] Call Failure Reason and Call Drop Explanation(PTT)

[iiii] System Operation Manual(Configuration Management)

[jjjj] System Operation Manual(System Tools)

[kkkk] System Operation Manual(Alarm Management)

[llll] System Operation Manual(Common Operations)

[mmmm] System Commissioning Manual

[nnnn] Controller Data Configuration Manual_DO

[oooo] Controller Data Configuration Manual_PTT

[pppp] Controller Data Configuration Manual_V5

[qqqq] Alarm Box(V5.00)User Manual

All these documents are version R1.0 except where otherwise.

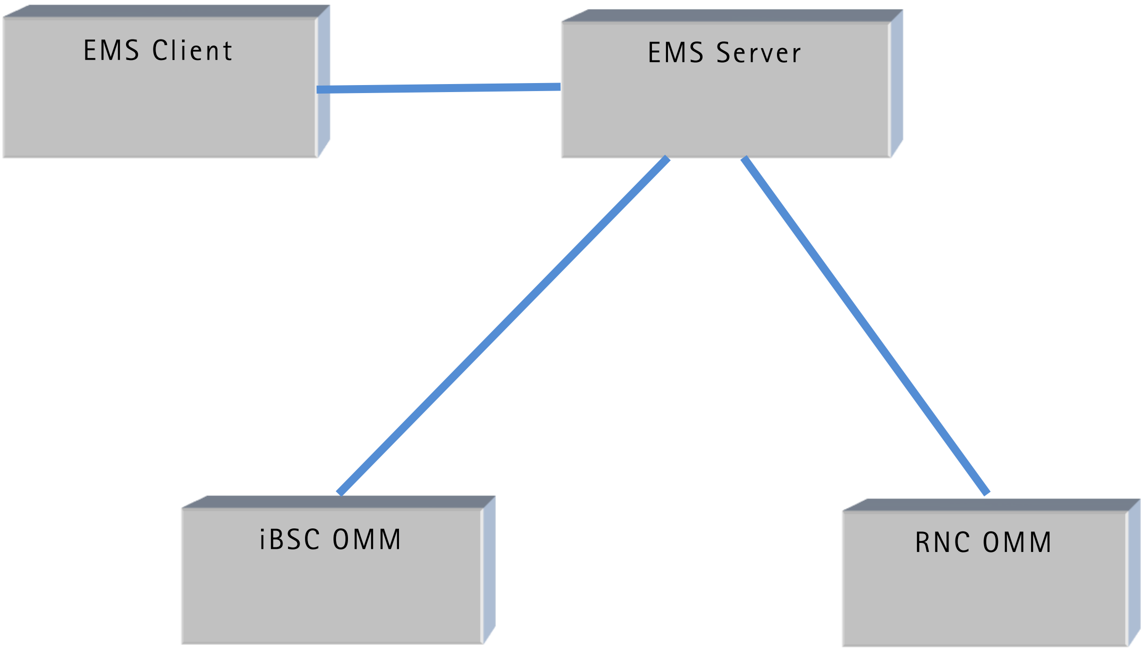
TOE Configuration

The following configuration was used for testing:

HARDWARE	IBM P740, 2*2 core CPUs, 32GB Memory (For EMS Server) ——2 146G SAS Disks, Dual-port HBA cards (EMS) ST6180 8*300G FC15K Disk Array (EMS)
SOFTWARE	ZXG10 iBSC (V6.20.614) ZXC10 BSCB (V8.0.3.400)OMM V3.08.34.00 OMM V6.20.614 OMM V3.09.30 OMM Client V6.20.614 OMM Client V3.09.30 OMM Client V3.08.34.00 ZXWR RNC (V3.09.30) EMS server/client (NetNumen U31 R18 V12.11.40)™

Environmental Configuration

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


EMS Client
EMS Server
iBSC OMM
RNC OMM