SERTIT

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

SERTIT-030 CR Certification Report

Issue 1.0 15 March 2012

ZTE Softswitch and Media Gateway Communication System V 1.0

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 Softswitch and Media Gateway Communication System consists of a softswitch (SS1b), a media gateway (MSG-9000) between the SS1b and the PSTN network, an element management system (EMS), and a network management service interface (NMSI).

ZTE Softswitch and Media Gateway Communication System version 1.0 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 EAL2 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	Kjartan Jæger Kvassnes Certifier
Quality Assurance	Lars Borgos Quality Assurance Lars Borgos
Approved	Kjell W. Bergan Head of SERTIT Kjell W Bergan
Date approved	15 March 2012

2 Abbreviations

BOSS	Business Operation Support System
BSVR	Billing Server
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
CDMA	Code Division Multiple Access
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
EMS	Network Element Management System
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
GSM	Global System of Mobile Communication
GUI	Graphics User Interface
I&A	Identification and Authentication
IMS	IP Multimedia System
ISDN	Integrated Service Digital Network
L3 switch	|Layer 3 switch
LIG	Lawful interception gateway
LIC	Lawful interception center
MML	Man Manual Language
MSG-9000	ZXMSG 9000 Media Gateway
NE	Network elements in the core network
NMSI	Network management service interface
OMM	Operational Maintenance Module
POC	Point of Contact
PSTN	Public Switching Telecommunication Network
SERTIT	Norwegian Certification Authority for IT Security
SN	Signalling Network

SS7	Signalling System No 7
SSH	Secure Shell
SFTP	Secure FTP
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
UMTS	Universal Mobile Telecommunications System
UDS	Universal Directory Server
VLAN	Virtual Local Area Network
QP	Qualified Participant

3 References

[1] ZXSS10 SS1B and MSG-9000 Communication System Security Target v 1.0, v 08, 01 November2011.

[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 Softswitch and Media Gateway Communication System, v 1.0, 12 January 2012.

[8] ZTE ZXSS10 SS1b&MSG 9000Common Criteria Security Evaluation – Certified Configuration

[9] ZXSS10 SS1b (V2.0.1.07) Documentation Guide

[10] ZXSS10 SS1b (V2.0.1.07) Hardware Installation Guide

[11] ZXSS10 SS1b (V2.0.1.07) Software Installation Guide Foreground Board

[12] ZXSS10 SS1b (V2.0.1.07) Software Installation Guide PC Server

[13] ZXSS10 SS1b (V2.0.1.07) Software Installation Guide SUN Server

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of ZTE Softswitch and Media Gateway Communication System version 1.0 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 Softswitch and Media Gateway Communication System and version 1.0.

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

The TOE is ZTE softswitch and media gateway communication system V1.0. The TOE consists of a softswitch (SS1b), a media gateway (MSG-9000) between the SS1b and the PSTN network, an element management system (EMS), and a network management service interface (NMSI).

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 EAL2, 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. Most of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

The 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.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 network traffic originating from / destined for the TOE or
  - Modify/read network traffic between TOE subsystems
  - Impersonate the TOE

  and thereby perform management actions on other entities on the network or gain unauthorized knowledge about TOE traffic.

- 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 LIG, Billing Center, and BOSS are trusted, and will not be used to attack the TOE. It is assumed that no attacks on the TOE will emanate from the PSTN, the Wireless Network, or IP telecommunication network

4.12 IT Security Objectives

- O. AUTHENTICATE_EMS

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

- O. AUTHORISE_EMS

  The TOE shall support at least two roles on the EMS Client:

  - EMS administrator with all rights
  - EMS operator with limited rights

  Rights include:

  - the ability to perform various management related actions
  - the ability to manage (create, modify rights, delete) other EMS users

- O.AUDITING_EMS

  The TOE shall support logging and auditing of OMM user actions.

- O. AUTHENTICATE_BSVR

  The TOE shall support billing server authentication, allowing the TOE to accept/reject billing server based on username and password.

- O.AUTHENTICATE_BOSS

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

- O.SEPARATE_USERS

  The TOE shall:

  - prohibit EMS users from accessing billing and BOSS related data and functionality
  - prohibit BSVR users from accessing EMS and BOSS related data and functionality
  - prohibit BOSS users from accessing EMS and billing related data and functionality

- O.PROTECT_COMMUNICATION

  The TOE shall:

  - protect communication between the TOE and the BOSS against masquerading, disclosure and modification

- protect communication between the TOE and the Billing Center against masquerading, disclosure and modification
- protect communication between the Clients and Servers of EMS against disclosure and modification
- protect communication between the SS1b and the NMSI against masquerading, disclosure and modification
- protect communication between the SS1b and the EMS against masquerading, disclosure and modification
- protect communication between the EMS and the NTP against masquerading and modification

4.13 Non-IT Security Objectives

- OE.TIME

  The NTP Server connected to the TOE shall supply the TOE with reliable time.

- OE.TRUST&TRAIN_USERS

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

- OE.CLIENT_SECURITY

  The customer 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 EMS or similar attacks.
- OE.PROTECTED_LINE_LIC

  The customer and the law enforcement authority shall ensure that the connection between the TOE and LIG and LIC is protected against masquerading, disclosure and modification.

- OE.PROTECT_COMMUNICATION

  The customer shall provide secure connection to

  - protect communication between MSG-9000 and EMS
  - protect communication between MSG-9000 and SS1b
- OE.VLAN

  The customer shall provide the following networks:

  - IP management network
  - BOSS network
- OE.SERVER_SECURITY

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

- OE.TRUSTED_SYSTEMS

  The customer shall ensure that the Billing Center, LIG, LIC, and BOSS are trusted, and will not be used to attack the TOE. The operator shall also ensure that all end-user level VoIP traffic emanate from the IP telecommunication network are trusted.

4.14 Security Functional Requirements

- FIA_UID.2.EMS User identification before any action
- FIA_UID.2.BOS User identification before any action
- FIA_UID.2.BIL User identification before any action
- FIA_UAU.2.EMS User authentication before any action
- FIA_UAU.2.BOS User authentication before any action
- FIA_UAU.2.BIL User authentication before any action
- FTA_SSL.3 TSF-initiated termination
- FIA_AFL.1 Authentication failure handling
- FIA_SOS.1 Verification of secrets
- 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.EMS Simplified 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.SS Basic internal transfer protection
- FDP_ITT.1.NMSI Basic internal transfer protection
- FTP_ITC.1.BOS Inter-TSF trusted channel
- FTP_ITC.1.BIL Inter-TSF trusted channel
- FTP_ITC.1.NTP Inter-TSF trusted channel
- FMT_SMF.1 Specification of Management Functions

4.15 Security Function Policy

The TOE has the following general functionalities:

Softswitch SS1b:

Telecommunications functionalities:

- Interact with PSTN, Wireless Network, and Telecommunication IP network to perform the management and control functions of the telecommunication network
- Interact with the Billing Center to charge for these functionalities

Management functionalities:

- Interact with EMS to be managed and configured (except for lawful interception)
- Interact with the BOSS to allow the BOSS User to manage the user profile.

Media gateway MSG-9000:

- Telecommunication functionalities:
- Connects the PSTN to the IP core network through trunk lines, and performs voice/fax conversion on the PSTN/ISDN side as well as on the IP network side
- Interconnect signaling between SS7 and packet switched network
- Connects the analog Z interface, ISDN users, V5.2 users and DSL users to the IP network.
- Management functionalities:
- Interact with EMS to be managed and configured (except for lawful interception)

EMS system:

- EMS server (EMS): manage SS1b and media gateway
- EMS client: a GUI for user to use EMS server

NMSI:

- Interface between BOSS to the SS1b.

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 12 January 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] 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 which potential vulnerabilities were already tested by the developer and assessed the results except those tests from [ATE IND AVA].

The remaining potential vulnerabilities were tested by Brightsight on the final version of the TOE at the premises of ZTE, Nanjing, China through remote terminal clients.

5.6 Developer's Tests

The developer test effort is considered already fairly complete. Any major missing tests haves been added to the developer test set. And the developer integrated tests for similar functionality into bigger test case. Nevertheless the evaluator has modified 9 additional tests for the EMS, NMSI, BSVR and SS1b service part subsystems as the evaluator's independent tests.

5.7 Evaluators' Tests

For independent testing, the evaluator has repeated 5 and modified 10 out of the 33 developer's tests (15 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, Nanjing, China through remote terminal clients in October and November 2011.

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 Softswitch and Media Gateway Communication System version 1.0 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 extended functionality, in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of ZTE Softswitch and Media Gateway Communication System version 1.0 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 are listed below:

TYPE	NAME AND VERSION
Hardware	ESPC (for SS1b service part) GPDU1 PCBA (DB server) GPDU1 PCBA (for BSVR) Central Control Unit[1] & Service Resource Unit[2] (for MSG-9000) GPDU1 PCBA (for EMS Server) GPDU1 PCBA (for NMSI)
SOFTWARE	SS1b service part (ZXSS10 SS1b v2.0.1.07) DB server (ZXSS10 SS1b v2.0.1.07) BSVR (ZXSS10 SS1b v2.0.1.07) MSG-9000 (ZXMSG9000 v1.0.05) EMS server/client (NetNumen U31 R30 V12.11.40) (Note: The EMS client has to be installed on Windows 7 or abovOS.) NMSI (NMSI 2.2.4)

TOE Documentation

The supporting guidance documents evaluated were:

Certified Configuration
- ZTE ZXSS10 SS1b&MSG 9000Common Criteria Security Evaluation – Certified Configuration

Standard guidance
- ZXSS10 SS1b (V2.0.1.07) Documentation Guide
- ZXSS10 SS1b (V2.0.1.07) System Description
- ZXSS10 SS1b (V2.0.1.07) Product Description
- ZXSS10 SS1b (V2.0.1.07) Hardware Description

Installation and maintenance
- ZXSS10 SS1b (V2.0.1.07) Hardware Installation Guide
- ZXSS10 SS1b (V2.0.1.07) Software Installation Guide Foreground Board
- ZXSS10 SS1b (V2.0.1.07) Software Installation Guide PC Server
- ZXSS10 SS1b (V2.0.1.07) Software Installation Guide SUN Server

Data configuration
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide AG Interconnection
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide Application Server Interconnection
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide Digit Analysis
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide DIGITMAP
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide Disaster Recovery
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide Global Configuration
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide H323 GK Interconnection
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide H323 Terminal Interconnection

[1] 2 x MOMP,2 x MCMP,2 x MSIPI,2 x MUIMC,2 x CLKG

[2] 1 x MRB,1 x MTDB,2 x MIPI,1 x MVTCA,2 x MUIMT,1 x MSPB

- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide IAD Interconnection
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide MGCF Feature
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide MSG9000 Interconnection
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide Other SS Interconnection
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide PRA and BRA Subscriber
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide PRA Trunk
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide Route
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide SCP Interconnection
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide SG Interconnection
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide SHLR Interconnection
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide SIP Terminal Interconnection
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide SSF Feature
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide Subscriber Allocation
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide TG Interconnection
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide Trunk
- ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide V5 Interconnection
- ZXSS10 SS1b (V2.0.1.07) Global Variable Reference
- ZXSS10 SS1b (V2.0.1.07) Northbound Interface Reference (Toll_Office_Format)
- ZXSS10 SS1b (V2.0.1.07) Operation Guide Data Backup and Restoration
- ZXSS10 SS1b (V2.0.1.07) Operation Guide File Management and Data Query
- ZXSS10 SS1b (V2.0.1.07) Operation Guide Signaling Tracing
- ZXSS10 SS1b (V2.0.1.07) Operation Guide System Maintenance
- ZXSS10 SS1b (V2.0.1.07) Operation Guide Traffic Control
- ZXSS10 SS1b (V2.0.1.07) Operation Guide Traffic Statistics
- ZXSS10 SS1b (V2.0.1.07) Service Provisioning Guide Authenticationand Call Restriction
- ZXSS10 SS1b (V2.0.1.07) Service Provisioning Guide CENTREX
- ZXSS10 SS1b (V2.0.1.07) Service Provisioning Guide Multi-Line Selected Group
- ZXSS10 SS1b (V2.0.1.07) Service Provisioning Guide Supplementary Service I
- ZXSS10 SS1b (V2.0.1.07) Service Provisioning Guide Supplementary Service II
- ZXSS10 SS1b (V2.0.1.07) Timer Reference
- ZXSS10 SS1b (V2.0.1.07) Traffic Statistics Entity Reference Volume I
- ZXSS10 SS1b (V2.0.1.07) Traffic Statistics Entity Reference Volume II

Alarm
- ZXSS10 SS1b (V2.0.1.07) Alarm and Notification Message Reference Alarm Volume
- ZXSS10 SS1b (V2.0.1.07) Alarm and Notification Message Reference Notification Volume
- ZXSS10 SS1b (V2.0.1.07) Failure Code Reference I
- ZXSS10 SS1b (V2.0.1.07) Failure Code Reference II
- ZXSS10 SS1b (V2.0.1.07) Failure Code Reference III
- ZXSS10 SS1b (V2.0.1.07) Routine Maintenance
- ZXSS10 SS1b (V2.0.1.07) Troubleshooting Guide

BSVR
- ZXSS10 SS1b (V2.0.1.07) Charging Server User Manual

BOSS
- ZXSS10 SS1b (V2.0.1.07) Softswitch Control Equipment BOSS Command Reference
- ZXSS10 SS1b (V2.0.1.07) Softswitch Control Equipment BOSS Command Reference (Supplementary)

MSG-9000 Guidance
- ZXMSG 9000(V1.0.05.R03)_Guide to Documentation_EN
- ZXMSG 9000(V1.0.05.R03)_Hardware Description---9000 Volume_EN
- ZXMSG 9000(V1.0.05.R03)_Hardware Installation---9000 Volume_EN
- ZXMSG 9000(V1.0.05.R03)_Software Installation---9000 Volume_EN
- ZXMSG 9000(V1.0.05.R03)_Operation_Guide---9000_Volume_I_EN
- ZXMSG 9000(V1.0.05.R03)_Operation_Guide---9000_Volume_II_EN

- ZXMSG 9000(V1.0.05.R03)_Operation_Guide---9000_Volume_II_EN_1
- ZXMSG 9000(V1.0.05.R03)_Operation_Guide---9000_Volume_III_EN

NetNumen U31 R30 Guidance
- NetNumen U31 R30 (V12.11.40) SS1b General Operation Guide(Security Management Volume)
- NetNumen U31 R30 (V12.11.40) SS1b General Operation Guide
- NetNumen U31 R30 (V12.11.40) SS1b Network Element Management Command Manual
- NetNumen U31 R30 (V12.11.40) SS1b Product Description
- NetNumen U31 R30 (V12.11.40) SS1b Routine Maintenance Guide

NMSI Guidance
- NetNumen U31 R30 Accouting IMP Commissioning 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:

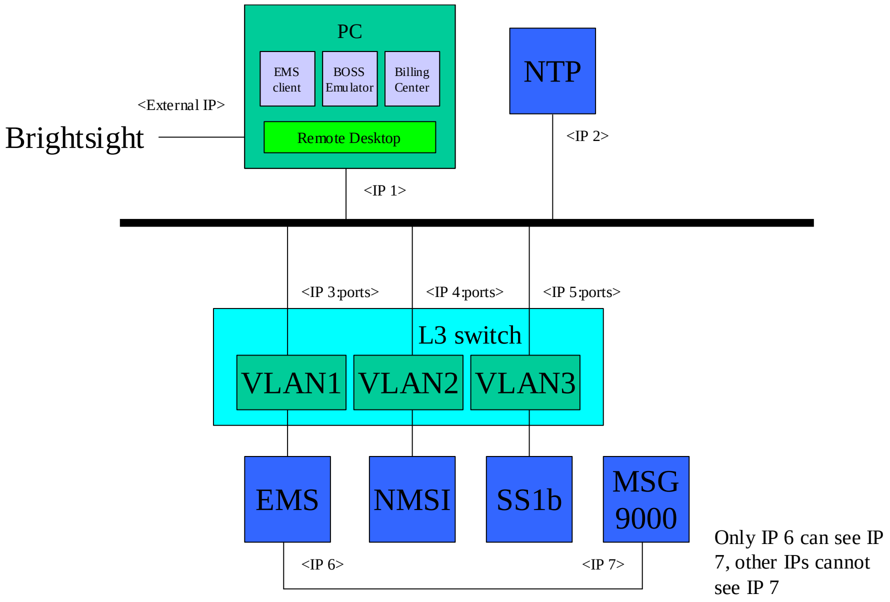
ITEM	IDENTIFIER	VERSION
HARDWARE	ESPC (for SS1b service part) GPDU1 PCBA (DB server) GPDU1 PCBA (for BSVR) Central Control Unit & Service Resource Unit (for MSG-9000) GPDU1 PCBA (for EMS Server) GPDU1 PCBA (for NMSI)	ESPC GPDU1 PCBA GPDU1 PCBA Minor Versions[3] [4] GPDU1 PCBA GPDU1 PCBA
SOFTWARE	SS1b service part (ZXSS10 SS1b v2.0.1.07) DB server (ZXSS10 SS1b v2.0.1.07) BSVR (ZXSS10 SS1b v2.0.1.07) MSG-9000 (ZXMSG9000 v1.0.05) EMS server/client (NetNumen U31 R30 V12.11.40) NMSI (NMSI 2.2.4)	ZXSS10 SS1b v2.0.1.07 ZXSS10 SS1b v2.0.1.07 ZXSS10 SS1b v2.0.1.07 ZXMSG9000 v1.0.05 NetNumen U31 R30 V12.11.40 NMSI 2.2.4
MANUAL	ZTE ZXSS10 SS1b&MSG 9000 Common Criteria Security Evaluation – Certified Configuration	R1.0
DEVELOPMENT EVIDANCE	- Security Target ZTE Softswitch and Media Gateway Communication System V1.0 - ZTE Softswitch and Media Gateway Communication System FSP-TDS - ZTE Softswitch and Media Gateway Communication System Security Architecture / Guidance - ALC_DEL.1, ALC_CMC.2, ALC_CMS.2, ALC_FLR.2 documentation for ZTE Softswitch and Media Gateway Communication System - Testplan for ZTE softswitch and media gateway communication system	V0.8 V0.3 V0.1 V0.1 V4.0

[3] 2 x MOMP,2 x MCMP,2 x MSIPI,2 x MUIMC,2 x CLKG

[4] 1 x MRB,1 x MTDB,2 x MIPI,1 x MVTCA,2 x MUIMT,1 x MSPB

Environmental Configuration

The TOE was tested in the following test set-up



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 Softswitch and Media Gateway Communication System

Type of Product: Telecommunication switch

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-030 CR, issue 1.0, 15 March 2012

Certificate Identifier: SERTIT-030 C

Date Issued: 15 March 2012

Kjartan Jæger Kvassnes
Certifier

Lars Borgos
Lars Borgos
Quality Assurance

Kjell W Bergan
Kjell Werner Bergan
Head of SERTIT

SERTIT
Norwegian Certification Authority for IT Security