



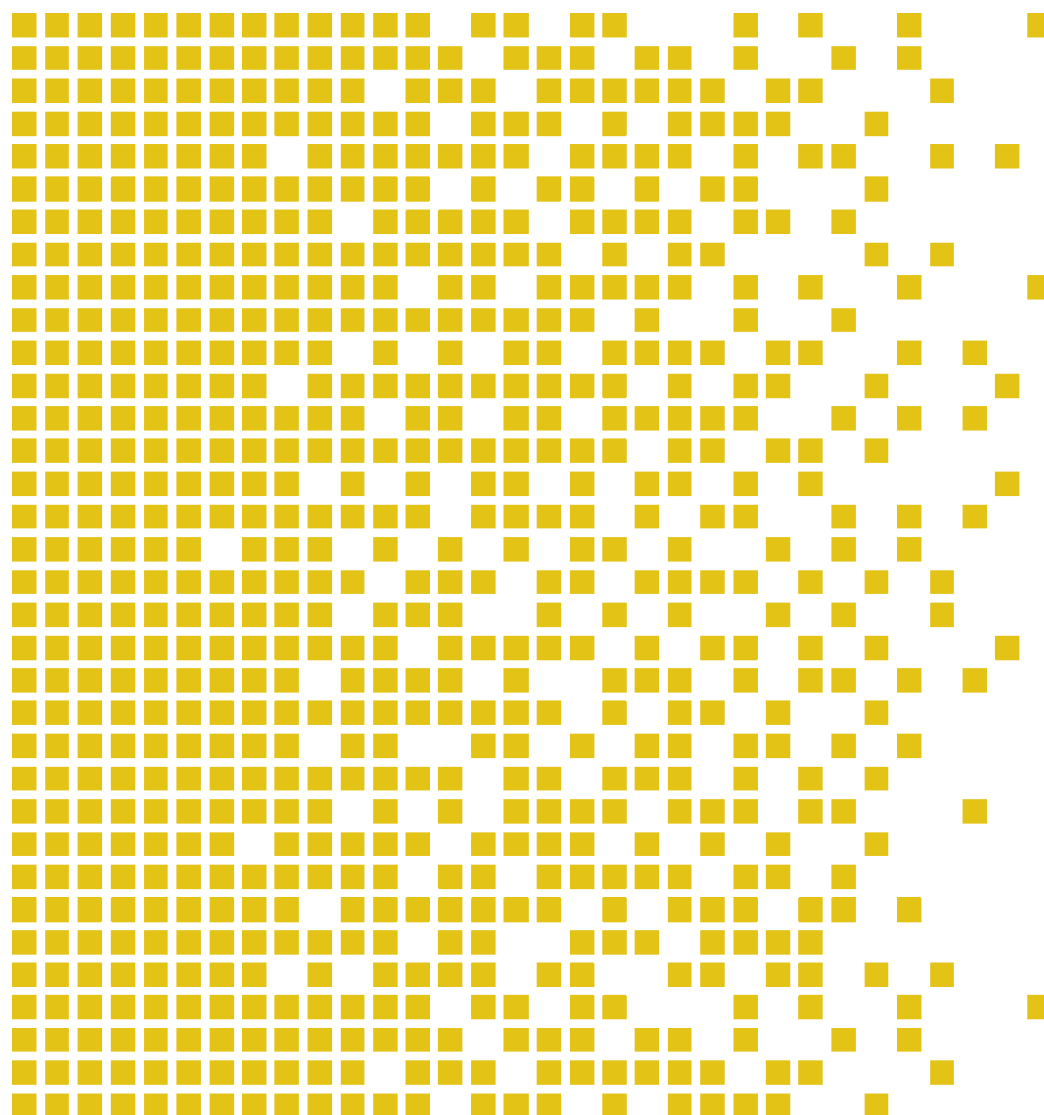
SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet Norwegian Certification Authority for IT Security

SERTIT-031 CR Certification Report

Issue 1.0 26 September 2011

ZTE Mobile Switching Center Server / intelligent Controller
Extensive, ZXWN MSCS / ZXUN iCX v4.10.13, ZXUN LIG v3.10.22



CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009 VERSION 2.0 13.09.2007

**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

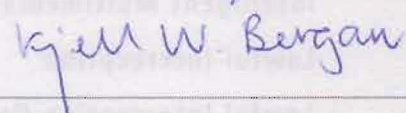
1	Certification Statement	5
2	Abbreviations	6
3	References	8
4	Executive Summary	9
4.1	Introduction	9
4.2	Evaluated Product	9
4.3	TOE scope	9
4.4	Protection Profile Conformance	9
4.5	Assurance Level	9
4.6	Security Policy	9
4.7	Security Claims	10
4.8	Threats Countered	10
4.9	Threats Countered by the TOE's environment	10
4.10	Threats and Attacks not Countered	10
4.11	Environmental Assumptions and Dependencies	10
4.12	IT Security Objectives	11
4.13	Non-IT Security Objectives	12
4.14	Security Functional Requirements	12
4.14.1	CUS-related SFRs	13
4.14.2	LIG-related SFRs	13
4.14.3	OMM-related SFRs	13
4.14.4	Common SFRs	14
4.15	Security Function Policy	14
4.16	Evaluation Conduct	14
4.17	General Points	14
5	Evaluation Findings	15
5.1	Introduction	16
5.2	Delivery	16
5.3	Installation and Guidance Documentation	16
5.4	Misuse	16
5.5	Vulnerability Analysis	16
5.6	Developer's Tests	17
5.7	Evaluators' Tests	17
6	Evaluation Outcome	17
6.1	Certification Result	17
6.2	Recommendations	17
	Annex A: Evaluated Configuration	19
	TOE Identification	19
	TOE Documentation	20
	TOE Configuration	21



1 Certification Statement

ZTE Corporation ZTE Mobile Switching Center Server / intelligent Controller Extensive is a softswitch plus clients that together perform the management and control function in an Intelligent Multimedia Subsystem network.

ZTE Mobile Switching Center Server / intelligent Controller Extensive version ZXWN MSCS / ZXUN iCX v4.10.13, ZXUN LIG v3.10.22 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and have met the Common Criteria Part 3 augmented requirements of Evaluation Assurance Level EAL2 augmented with ALC_FLR.2 for the specified Common Criteria Part 2 extended functionality for the specified environment when running on the platforms specified in Annex A.

Author	Kjartan Jæger Kvassnes Certifier 
Quality Assurance	Lars Borgos Quality Assurance 
Approved	Kjell W. Bergan Head of SERTIT 
Date approved	26 September 2011

2 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
CUS	Charge Uniform Server
EAL	Evaluation Assurance Level
EMS	Element Management System
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
iCX	intelligent Controller Extensive
IMS	Intelligent Multimedia Subsystem
LI	Lawful Interception
LIC	Lawful Interception Center
LIG	Lawful Interception Gateway
LIS	Lawful Interception Server
MSCS	Mobile Switching Center Server
NTP	Network Time Protocol
OMM	Operational Maintenance Module
OMS	Operations Maintenance Server
POC	Point of Contact
PSTN	Public Switching Telecommunication Network
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

- [1] Security Target, ZTE Corporation, ZTE Mobile Switching Center Server / intelligent Controller Extensive (ZXWN MSCS / ZXUN iCX) version 1.1, 18 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 EAL2+ Evaluation of ZXWN MSCS / ZXUN iCX ZTE Mobile Switching Center Server / intelligent Controller Extensive, 19 August 2011, version 1.0.
- [8] ZXWN MSCS MSC Server Common Criteria Security Evaluation – Certified Configuration, Version: R1.2, 18 August 2011.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of ZTE Mobile Switching Center Server / intelligent Controller Extensive version ZXWN MSCS / ZXUN iCX v4.10.13, ZXUN LIG v3.10.22 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 Mobile Switching Center Server / intelligent Controller Extensive and version ZXWN MSCS / ZXUN iCX v4.10.13, ZXUN LIG v3.10.22.

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

The ZTE Mobile Switching Center Server / intelligent Controller Extensive is a softswitch plus clients that together perform the management and control function in an Intelligent Multimedia Subsystem network. The TOE is used to provide signal transfer, control and management and lawful interception services to the IMS telecommunications network.

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

4.3 TOE scope

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

4.4 Protection Profile Conformance

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

4.5 Assurance Level

The assurance incorporated predefined evaluation assurance level EAL2, 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 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[1] 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

- A rouge user performs actions on the TOE that he is not authorized to do
- A rouge 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
- An unknown user gains unauthorized access to the TOE and is able to perform actions on the TOE
- An attacker with IP-access to the External Network that is connected to the TOE gains unauthorized access to the TOE and is able to perform actions on the TOE
- An attacker with IP-access to the External Network that is connected to the TOE is able to modify/read external network traffic originating from / destined for the TOE and thereby:
 - perform actions on the TOE, the EMS or the Billing Center and/or
 - gain unauthorized knowledge about traffic between the TOE and the EMS/Billing Center.

4.9 Threats Countered by the TOE's environment

- An attacker with physical access to the TOE 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

- The EMS, LIC, NTP Server and Billing Center are trusted, and will not be used to attack the TOE.
- The PSTN, Service Part Private Network, Wireless Network and Rest of IMS Network are trusted networks, and will not be used to attack the TOE

- Traffic on the Secure Network or the connection between LIS and LIC cannot be modified or read by threat agents
- The L3 switch will block all traffic from/to the external network except for:
 - Selected traffic between EMS and OMS
 - Selected traffic between Billing Center and CUS
 - Selected traffic between OMS and OMM Client

4.12 IT Security Objectives

- The LIS shall support LIG Client user authentication, allowing the LIS to accept/reject LIG users based on username and password
- The LIS shall support a flexible role-based authorization framework with predefined and customizable roles. These roles can use the LI Client to manage the LIS. Each role allows a user to perform certain actions, and the LIS shall ensure that users can only perform actions when they have a role that allows this.
- The LIS shall support logging and auditing of LIG user actions. Actions of the LIC shall not be logged
- The OMS shall support OMM Client user authentication, allowing the OMS to accept/reject OMM users based on username and password.
- The OMS shall support a flexible role-based authorization framework with predefined and customizable roles. These roles can use the OMS to manage the OMS and the Service Part. Each role allows a user to perform certain actions, and the OMS shall ensure that users can only perform actions when they have a role that allows this
- The OMS shall support logging and auditing of OMM user actions
- The CUS shall support CUS Client user authentication, allowing the CUS to accept/reject CUS users based on username and password
- The CUS shall support a role-based authorization framework with predefined roles. These roles can use the CUS Client to manage the CUS. Each role allows a user to perform certain actions, and the CUS shall ensure that users can only perform actions when they have a role that allows this
- The TOE shall support logging and auditing of CUS user actions
- The TOE shall:
 - prohibit LIG users from accessing CUS and OMM related data and functionality
 - prohibit CUS users from accessing LIG and OMM related data and functionality
 - prohibit OMM users from accessing LIG and CUS related data and functionality
- The TOE shall:
 - protect communication between the TOE and the EMS against masquerading, disclosure and modification
 - protect communication between the TOE and the Billing Center against masquerading, disclosure and modification
 - protect communication between the OMM Client and the OMS against masquerading, disclosure and modification.

4.13 Non-IT Security Objectives

- 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 OMS/CUS/LIS or similar attacks
- The operator shall configure the Secure Network to:
 - protect communication between the TOE and the NTP Server against masquerading and modification
 - protect communication between LIG Client and LIS against disclosure and modification
 - protect communication between CUS Client and CUS against disclosure and modification
- The operator shall protect the communication between LIC and LIS against disclosure, masquerading and modification according to the laws of the appropriate country.
- The operator shall ensure that the MSC Server shall be protected from physical attacks
- The NTP Server shall supply the TOE with reliable time
- The operator shall ensure that LI, CUS and OMM roles are only assigned to users that are sufficiently trustworthy and sufficiently trained to fulfill those roles.
- The operator shall ensure that the EMS, LIC, Billing Center and NTP are trusted, and will not be used to attack the TOE.
- The operator shall ensure that the PSTN, Service Part Private Network, Wireless Network and Rest of IMS Network are trusted networks, and will not be used to attack the TOE.
- The operator shall configure the L3 switch to block all traffic from/to the external network except for:
 - Selected traffic between EMS and OMS
 - Selected traffic between Billing Center and CUS
 - Selected traffic between OMS and OMM Client

4.14 Security Functional Requirements

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

The TOE uses three client/server combinations (OMM Client/OMS, LIG Client/LIS, CUS Client/CUS), which are similar, but not identical. The following table summarizes these similarities and differences. The full description of the SFRs can be found in the ST[1], chapter 5.3.

4.14.1 CUS-related SFRs

- FIA_UID.2.CUS User identification before any action
- FIA_UAU.2.CUS User authentication before any action
- FIA_AFL.1.CUS Authentication failure handling
- FIA_SOS.1.CUS Verification of secrets
- FTA_SSL.3.CUS TSF-initiated termination
- FTA_MCS.1.CUS Basic limitation on multiple concurrent sessions
- FMT_SMR.1.CUS Security roles
- FAU_GEN.3.CUS Simplified audit data generation
- FAU_SAR.1.CUS Audit review
- FAU_STG.1.CUS Protected audit trail storage
- FAU_STG.4.CUS Prevention of audit data loss
- FTP_ITC.1.BIL Inter-TSF trusted channel
- FMT_SMF.1.CUS Specification of Management Functions

4.14.2 LIG-related SFRs

- FIA_UID.2.LIG User identification before any action
- FIA_UAU.2.LIG User authentication before any action
- FIA_AFL.1.LIG Authentication failure handling
- FIA_SOS.1.LIG Verification of secrets
- FTA_SSL.3.LIG TSF-initiated termination
- FTA_MCS.1.LIG Basic limitation on multiple concurrent sessions
- FMT_SMR.1.LIG Security roles
- FAU_GEN.3.LIG Simplified audit data generation
- FAU_SAR.1.LIG Audit review
- FAU_STG.1.LIG Protected audit trail storage
- FAU_STG.4.LIG Prevention of audit data loss
- FMT_SMF.1.LIG Specification of Management Functions

4.14.3 OMM-related SFRs

- FIA_UID.2.OMM User identification before any action
- FIA_UAU.2.OMM User authentication before any action
- FIA_AFL.1.OMM Authentication failure handling
- FIA_SOS.1.OMM Verification of secrets
- FTA_SSL.3.OMM TSF-initiated termination
- FTA_MCS.1.OMM Basic limitation on multiple concurrent sessions
- FMT_SMR.1.OMM Security roles
- FAU_GEN.3.OMM Simplified audit data generation
- FAU_SAR.1.OMM Audit review
- FAU_STG.1.OMM Protected audit trail storage
- FAU_STG.4.OMM Prevention of audit data loss
- FDP_ITT.1.OMM Basic internal transfer protection
- FTP_ITC.1.EMS Inter-TSF trusted channel
- FMT_SMF.1.OMM Specification of Management Functions

4.14.4 Common SFRs

- FDP_ACC.2 Complete access control
- FDP_ACF.1 Security attribute based access control

4.15 Security Function Policy

The TOE:

- Provides secure management of itself, to ensure that only properly authorized staff can manage the TOE
- Provides secure access to its Lawful Interception functionality, ensuring that only the LIC can access this functionality
- Provides secure interaction between itself and the Billing Center, so that billing data 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 the 19 August 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 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

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 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 Common Criteria Security Evaluation – Certified Configuration document[8].

This document is 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[8] 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 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.

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 in July 2011.

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

The evaluator has shown that TSF is resistant against known attacks at the given time of evaluation.

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 depth and coverage analysis shows that the developers' tests cover all TSF, and that the TOE has been extensively tested against its functional specification. The developer's testing results lead either to a test is passed, or the test is failed and an error report is created for that error.

The results show that the developer testing requirements are extensive and that the TSF satisfies the TOE security functional requirements.

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.

The evaluator's independent testing was spread over some of the interfaces involved for implementation of the SFRs to provide good rigour of testing. Summarized, this testing in combination with the developers testing covers the interfaces involved in the implementation of the SFRs.

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 Mobile Switching Center Server / intelligent Controller Extensive version ZXWN MSCS / ZXUN iCX v4.10.13, ZXUN LIG v3.10.22 meet the Common Criteria Part 3 augmented requirements of Evaluation Assurance Level EAL2+ (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 Mobile Switching Center Server / intelligent Controller Extensive version ZXWN MSCS / ZXUN iCX v4.10.13, ZXUN LIG v3.10.22 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".

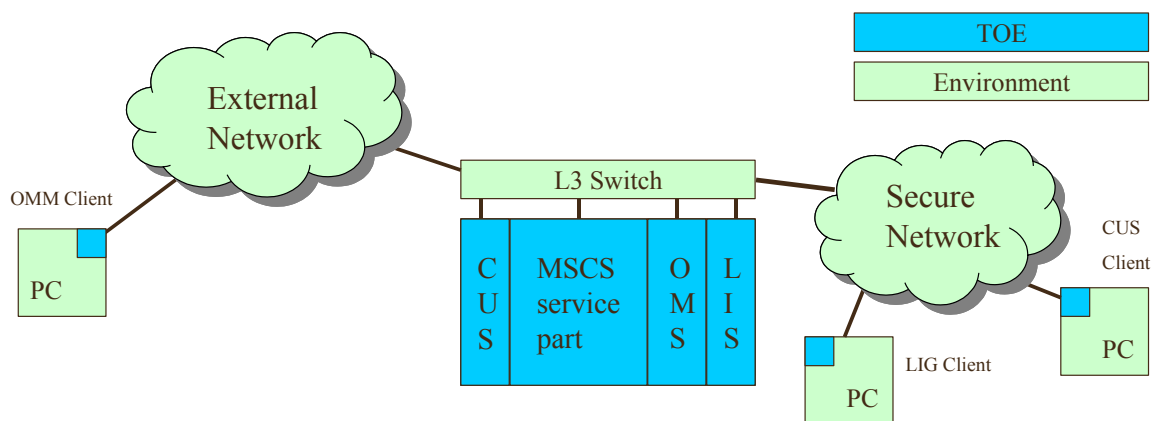
The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

Annex A: Evaluated Configuration

TOE Identification

The TOE is a soft switch plus clients that together perform the management and control function in an IMS network. The TOE is used to provide signal transfer, control and management and lawful interception services to the IMS telecommunications network.

The TOE consists of four parts:



- An MSCS, consisting of:
 - An MSCS Service Part, responsible for performing the telecommunication services
 - An OMS (Operations Maintenance Server), responsible for management and maintenance of the MSCS
 - An LIS (Lawful Interception Server), allowing configuration of the Lawful Interception aspects of the MSCS and sending any lawfully intercepted signalling data to the Lawful Interception Center.
 - A CUS (Charge Uniform Server), responsible for generate billing information and sending this information to the Billing Center for further processing.
- An OMM Client, consisting of a Java application, running on a non-TOE workstation. This client is a graphical user interface to the OMS. The combination of Client and OMS is called the OMM (Operational Maintenance Module).
- A LIG Client, consisting of a Java application, running on a non-TOE workstation. This client is a graphical user interface to the LIS. The combination of Client and LIS is called the LIG (Lawful Interception Gateway)
- A CUS Client, consisting of a Java application, running on a non-TOE workstation. This client is a graphical user interface to the CUS.

TOE Documentation

The supporting guidance documents evaluated were:

Certified Configuration

- [a] CC Security Evaluation – Certified Configuration R1.2

MSC Server V4.10.13 (all are R1.0 except where indicated)

- [b] MSC Server Product Description
- [c] MSC Server Signaling Description
- [d] MSC Server Hardware Description
- [e] Hardware Installation Guide
- [f] Software Installation Guide
- [g] Data Configuration Guide (MSCS I)
- [h] Data Configuration Guide (MSCS II)
- [i] Alarm Management Operation Guide
- [j] Performance Management Operation Guide
- [k] Signaling Trace Operation Guide
- [l] General Operation Guide R1.2
- [m] Parts Replacement Guide
- [n] Alarm Message Reference
- [o] Notification Message Reference
- [p] Troubleshooting Guide
- [q] Routine Maintenance Guide
- [r] Performance Counter Reference (Global Traffic)
- [s] Performance Counter Reference (Signal Measurement)
- [t] Performance Counter Reference (Base Measurement)
- [u] Performance Counter Reference (Global Measurement and Charge Statistics)
- [v] Performance Counter Reference (Combination Traffic)
- [w] Performance Counter Reference (Special Operation)
- [x] Performance Counter Reference (Handover Operation)
- [y] Performance Index Reference
- [z] Documentation Guide
- [aa] Interception Service User Guide

CUS V4.10.20 (all are R1.0 except where indicated)

- [bb] General Operation Guide (Charging System) R1.4
- [cc] Product Description (Charging System)
- [dd] CDR Reference (Charging System)
- [ee] Command Reference (Charging System)
- [ff] Data Configuration Guide (Charging System)
- [gg] Maintenance Guide (Charging System)
- [hh] Software Installation Guide (Charging System)
- [ii] System Debugging Guide (Charging System)

LIG V3.10.22 (all are R1.0 except where indicated)

- [jj] System Administrator Guide R1.1
- [kk] Guide to Documentation
- [ll] Product Description
- [mm] Software Installation
- [nn] Data Configuration Guide
- [oo] Alarm Management User Guide
- [pp] Performance Management User Guide
- [qq] Maintenance Tools User Guide
- [rr] Maintenance Guide
- [ss] Performance Measurement Item Reference
- [tt] Alarm and Notification Reference
- [uu] Gateway Command Reference

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	Name and version
Hardware	GPBB0 (for the service part) GPBX1 (for the CUS) GPBX1 (for the LIS) GPBX1 (for the OMS)
Software	MSCS v4.10.13 LIG v3.10.22 LIG Client SW v3.10.22 CUS Client SW v4.10.20 OMM Client SW v4.10.13