ZXWN MSCS / ZXUN iCX

ZTE Mobile Switching Center Server / intelligent Controller Extensive

Security Target

ZTE CORPORATION
NO. 55, Hi-tech Road South, ShenZhen, P.R.China
Postcode: 518057
Tel: +86-755-26771900
Fax: +86-755-26770801
URL: http://ensupport.zte.com.cn
E-mail: support@zte.com.cn
Publishing Date: 2011-08-18
Version: R1.1

LEGAL INFORMATION

Copyright © 2011 ZTE CORPORATION.

The contents of this document are protected by copyright laws and international treaties.

All company, brand and product names are trade or service marks, or registered trade or service marks, of ZTE CORPORATION or of their respective owners.

This document is provided "as is", and all express, implied, or statutory warranties, representations or conditions are disclaimed, including without limitation any implied warranty of merchantability, fitness for a particular purpose, title or non-infringement. ZTE CORPORATION and its licensors shall not be liable for damages resulting from the use of or reliance on the information contained herein.

ZTE CORPORATION or its licensors may have current or pending intellectual property rights or applications covering the subject matter of this document. Except as expressly provided in any written license between ZTE CORPORATION and its licensee, the user of this document shall not acquire any license to the subject matter herein.

ZTE CORPORATION reserves the right to upgrade or make technical change to this product without further notice.

Users may visit ZTE technical support website http://ensupport.zte.com.cn to inquire related information.

The ultimate right to interpret this product resides in ZTE CORPORATION.

Revision History

Version	Date	Comment
0.1	Feb 16, 2010	First version
0.2	Mar 15, 2011	Updated and expanded. Submitted to SERTIT.
0.3	May 3, 2011	Remove RADIUS server, segregated network in secure and insecure network, changed TOE name and completed all sections.
0.31	May 6, 2011	Some minor corrections based on ZTE comments
0.32	May 18, 2011	Some more minor comments based on PL review
0.4	June 8, 2011	Corrected EORs 1-10
0.41	June 16, 2011	Made consistency improvements for FSP
0.42	June 23, 2011	Added that logs can be deleted after 30 days. ZTE comments added.
0.43	July 14, 2011	Added Certified Configuration Manual, corrected scope.
0.44	July 15, 2011	More minor corrections.
1.0	July 18, 2011	Corrected HW/SW/Guidance list
1.1	Aug 18, 2011	Change reference document's version number and legal information

Serial Number: SJ-20110818121552-001

Publishing Date: 2011-08-18(R1.1)

References

[CCp1] Common Criteria for IT Security Evaluation, Part 1, v3.1r3, July 2009

[CCp2] Common Criteria for IT Security Evaluation, Part 2, v3.1r3, July 2009

[CCp3] Common Criteria for IT Security Evaluation, Part 3, v3.1r3, July 2009

[CEMe] Common Methodology for IT Security Evaluation, v3.1r3, July 2009

This page intentionally left blank.

Contents

Chapter 1

ST Introduction

Table of Contents

1.1 ST and TOE References

This is version 1.1 of the Security Target for the ZTE Mobile Switching Center Server (ZXWN MSCS), version MSCS v4.10.13, ZXUN LIG v3.10.22.

This product is also known as the intelligent Controller extensive (ZXUN iCX), version iCX V4.10.13, ZXUN LIG V3.10.22

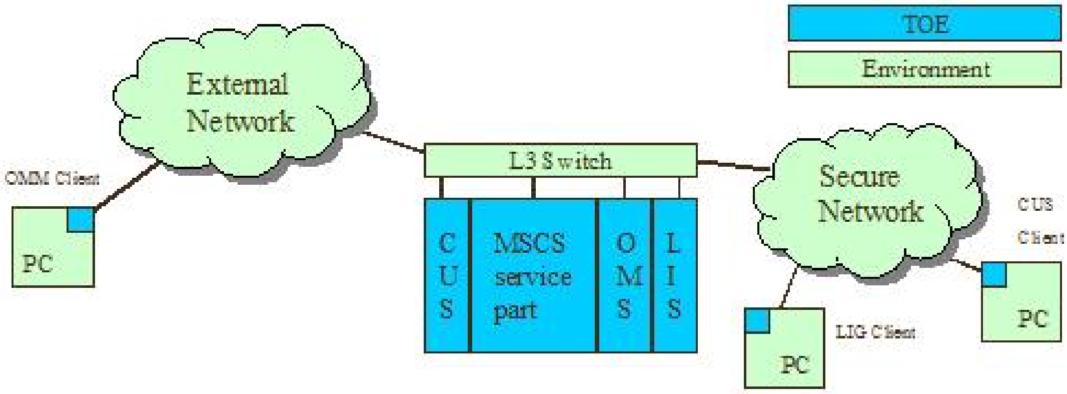
The remainder of this ST will refer to the TOE as MSCS.

1.2 TOE Overview and Usage

The TOE is a softswitch plus clients that together perform the management and control function in an IMS[1] network. The TOE is used to provide signal transfer, control and management and lawful interception services to the IMS telecommunications network.

The TOE (depicted in Figure 1-1) consists of four parts:

Figure 1-1 The TOE



- An MSCS, consisting of:

[1] Intelligent Multimedia Subsystem

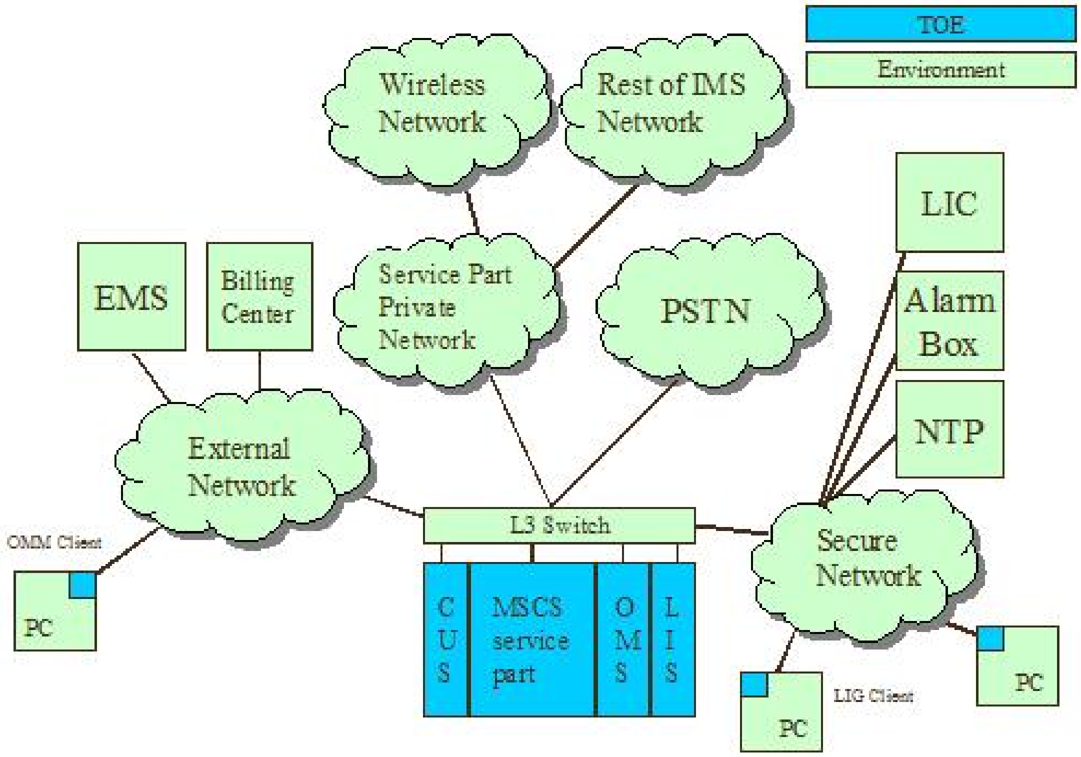
  - An MSCS Service Part, responsible for performing the telecommunication services
  - An OMS (Operations Maintenance Server), responsible for management and maintenance of the MSCS
  - An LIS (Lawful Interception Server), allowing configuration of the Lawful Interception aspects of the MSCS and sending any lawfully intercepted signaling 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.

These are connected by two networks:

- A Secure Network: This is the internal network of the provider, and is considered secure in this evaluation.
- An External network: This is an external network (it might even include Internet) and is considered insecure in this evaluation.

The MSCS is the management and control part of the IMS Network and is therefore connected to a wide variety of other systems and networks, as shown in Figure 1-2 .

Figure 1-2 The TOE in its environment



The additional[2] systems and network are:

- An EMS (Element Management System). This is a centralized management system that can be used to manage multiple TOEs. It connects to the OMS part of the TOE.
- A Billing Center. This is a centralized server that processes the billing information of multiple TOEs (and other equipment). It connects to the CUS part of the TOE.
- LIC (Lawful Interception Center): this is a facility under the control of law enforcement authorities. It can configure the lawful interception functionality of the MSCS through the LIS, receive intercepted signaling data from the LIS and intercepted voice data from the MGW (in the other part of the IMS Network).
- NTP: an NTP-server that provides time services to the TOE.
- Alarm Box: this is a simple box with an audio or visual alarm that can be used to alert the operator.
- The PSTN (Public Switching Telecommunication Network): The traditional fixed switching network that connects many subscribers to each other. It is considered a trusted network in this evaluation.
- The Service Part Private Network: This is a private IP network of the operator. It is considered a trusted network in this evaluation.
- The Wireless Network: This consists of Radio Network Controllers (for UMTS) and Base Station Controllers (for GSM). These are part of the telecommunications network and ultimately (through other equipment) connect to UE (User Equipment), which

[2] Additional to those described earlier.

consists of mobile phones and similar equipment that uses GSM and/or UMTS. It is considered a trusted network in this evaluation.

- The other part of IMS network: This includes elements like:
  - The MGW (Media Gateway), which provides transcoding services and is controlled by the MSCS
  - The HLR (Home Location Register), which provides a mobile subscriber location register.

  These elements interact with the MSCS to perform the management and control functions of the IMS network.

The other part of IMS Network is considered a trusted network in this evaluation, as are the MGW, HLR and other elements.

The MSCS has the following general functionalities:

- Telecommunications functionality
  - Interact with PSTN, Wireless Network, other parts of IMS network to perform the management and control functions of the IMS network
  - Interact with the Billing Center to charge for these functionalities
- Lawful Interception:
  - Interact with LIC to allow configuration of Lawful Interception functionality
  - Interact with LIC to send intercepted signaling data
  - Interact with MGW to ensure that intercepted voice data is sent to the LIC
- Management:
  - Manage and configure the TOE
  - Interact with EMS to be managed and configured (except for lawful interception)

1.2.1 Major Security Features

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

1.2.2 Non-TOE Hardware/Software/Firmware

The TOE requires networking connectivity, a NTP server as time source, and an L3 switch to separate its various networks.

Each CUS Client requires:

Type	Name and version
Workstation	A PC suitable to run the OS (see below)
OS	MS-Windows XP or later

Each OMM or LI Client requires:

Type	Name and version
Workstation	A PC suitable to run the OS (see below)
OS	Any OS that supports Java (see below)
Java	Java(TM) SE Runtime Environment (build 1.6.0_21-b06) Java HotSpot(TM) Client VM (build 17.0-b16, mixed mode)

1.3 TOE Description

1.3.1 Physical Scope

The TOE consists of the following:

Type	Name and version
Hardware[3]	GPBB0[4](for the service part) GPBX1 (for the CUS) GPBX1 (for the LIS) GPBX1 (for the OMS)
Software	MSCS v4.10.13[5][6] LIG v3.10.22
Software	CUS Client SW v4.10.20
Software	LIG Client SW v3.10.22
Software	OMM Client SW v4.10.13

[3] This is the evaluated configuration. The MSCS can be extended with additional GPBX1 boards (for fault tolerance) or additional GPBB0 boards (for increased capacity), but these options were not evaluated.

[4] These are boards built by ZTE. The last digit is the version number.

[5] Note that this includes the Service Part, the CUS (v4.10.20) and the OMS (v4.10.13).

[6] Note that the Service Part of the MSCS is extensible with additional boards to add capacity. This should have no effect on security. In this evaluation only the non-extended configuration was tested.

MSC Server V4.10.13 (all are R1.0 except where indicated)
Certified Configuration • CC Security Evaluation – Certified Configuration R1.2
Standard Guidance • MSC Server Product Description • MSC Server Signaling Description • MSC Server Hardware Description • Hardware Installation Guide • Software Installation Guide • Data Configuration Guide(MSCS I) • Data Configuration Guide(MSCS II) • Alarm Management Operation Guide • Performance Management Operation Guide • Signaling Trace Operation Guide • General Operation Guide R1.2 • Parts Replacement Guide • Alarm Message Reference • Notification Message Reference • Troubleshooting Guide • Routine Maintenance Guide • Performance Counter Reference (Global Traffic) • Performance Counter Reference (Signal Measurement) • Performance Counter Reference (Base Measurement) • Performance Counter Reference (Global Measurement and Charge Statistics) • Performance Counter Reference (Combination Traffic) • Performance Counter Reference (Special Operation) • Performance Counter Reference (Handover Operation) • Performance Index Reference • Documentation Guide • Interception Service User Guide

CUS V4.10.20 (all are R1.0 except where indicated)
• General Operation Guide (Charging System) R1.4 • Product Description (Charging System) • CDR Reference (Charging System) • Command Reference (Charging System) • Data Configuration Guide (Charging System) • Maintenance Guide (Charging System) • Software Installation Guide (Charging System) • System Debugging Guide (Charging System)

LIG V3.10.22
• System Administrator Guide R1.1 • Guide to Documentation • Product Description • Software Installation • Data Configuration Guide • Alarm Management User Guide • Performance Management User Guide • Maintenance Tools User Guide • Maintenance Guide • Performance Measurement Item Reference • Alarm and Notification Reference • Gateway Command Reference

1.3.2 Logical Scope

The logical scope of the TOE is described in Figure 1-2.

The functionalities and threats are related to:

- Secure management of the TOE, to ensure that only properly authorized staff can manage the TOE.
- Secure access to the Lawful Interception functionality of the TOE, ensuring that only the LIC can access this functionality.
- Secure interaction between the TOE and the Billing Center, so that billing data cannot be read or modified in between these two.

Secure management of the TOE, to ensure that only properly authorized staff can manage the TOE.

There are four ways of managing the TOE:

- Through the OMM Client: This allows full access to management functionality except for lawful interception and billing functionality
- Through the EMS: This allows similar access as through the OMM Client[7]
- Through the CUS: This allows management of billing functionality
- Through the LIG: This allows configuration of lawful interception functionality

Secure management means:

- Proper authentication (who is the user), authorization (what is the user allowed to do) and auditing (what has the user done)
- Protection of communication between Client/EMS and MSCS against disclosure, undetected modification and masquerading

[7] The difference is that the EMS is centralised while the OMM Client is local to the specific MSCS instance. EMS has limited management functionalities while OMM has full management functionalities

Note that the first bullet is out-of-scope for the EMS, since it is not part of the TOE. The protection of communication between EMS and OMS is in scope.

Provides secure access to its Lawful Interception functionality, ensuring that only the LIC can access this functionality

The TOE will prevent EMS, OMM and LIG users from accessing its functionality, either directly or by hacking the MSCS.

Provides secure interaction between itself and the Billing Center, itself and the EMS and itself and the OMM Client so that data cannot be read or modified in between

The TOE shall protect the communication between:

- Billing Center and CUS
- OMM Client and OMS
- EMS and OMS

against disclosure, undetected modification and masquerading.

1.3.3 Roles and External Entities

See 5.2 Definitions.

Chapter 2
Conformance Claims

This ST conforms to:

- CC, version 3.1R3, as defined by [CCp1], [CCp2], [CCp3] and [CEMe].
- CC Part 2 as CC Part 2 extended
- CC Part 3 as CC Part 3 conformant

This ST conforms to no Protection Profile.

This ST conforms to EAL 2+ALC_FLR.2, and to no other packages.

This page intentionally left blank.

Chapter 3

General Documentation

Table of Contents

3.1 Organisational Security Policies

OSP.USERS

The TOE must:

- authenticate LIG users, log their activities[8], and allow them to set-up and configure the LIG functionality
- authenticate CUS users, log their activities, and allow them to set-up and configure the billing functionality
- authenticate OMM users, log their activities, and allow OMM users to set-up and configure the TOE functionality (except for billing and LIG functionality)

3.2 Threats

3.2.1 Assets and Threat Agents

The assets are:

- The ability to allow various users to manage various aspects of the TOE securely, especially the lawful interception functionality
- The confidentiality and integrity of the communication between the TOE and:
  - Clients
  - EMS
  - Billing Center
  - Lawful Interception Center

These assets are threatened by the following threat agents:

1. TA.ROGUE_USER A LI, CUS or OMM user seeking to act outside his/her authorization. There are three types:

[8] Note that LIG user activities should be logged, but that LIC activities should not be logged by the LIS due to the law’s restriction in some country.

- TA_ROGUE_USER_LIG: which has legitimate access to the LIG Client, but not to the other Clients
- TA_ROGUE_USER_OMM: which has legitimate access to the OMM Client, but not to the other Clients
- TA_ROGUE_USER_CUS: which has legitimate access to the CUS Client, but not to the other Clients

2. TA.NETWORK An attacker with IP-access to the External Network that is connected to the TOE
3. TA.PHYSICAL An attacker with physical access to the TOE

3.2.2 Threats

The combination of assets and threats gives rise to the following threats:

T.UNAUTHORISED

TA.ROGUE_USER_LIG, TA.ROGUE_USER_CUS or TA.ROGUE_USER_OMM performs actions on the TOE that he is not authorized to do.

T.AUTHORISED

TA.ROGUE_LIG, TA.ROGUE_USER_CUS or TA.ROGUE_USER_OMM performs actions on the TOE that he is authorized to do, but these are undesirable[9] 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, the EMS or the Billing Center and/or
- gain unauthorized knowledge about traffic between the TOE and the EMS/Billing Center.

T.PHYSICAL_ATTACK

TA.PHYSICAL gains physical access to the TOE (either clients or MSC Server) and is able to perform actions on the TOE.

3.3 Assumptions

This Security Target uses one assumption:

A.TRUSTED_SYSTEMS

[9] For example, the user is allowed to modify billing records in case of obvious error, but he misuses this to delete all billing records.

It is assumed that:

- 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

This page intentionally left blank.

Chapter 4
Security Objectives

Table of Contents

4.1 Overfiew

These security objectives describe how the threats described in the previous section will be addressed. It is divided into:

- The Security Objectives for the TOE, describing what the TOE will do to address the threats.
- The Security Objectives for the Operational Environment, describing what other entities must do to address the threats.

A rationale that the combination of all of these security objectives indeed addresses the threats may be found in 7.1 Security Objectives Rationale of this Security Target.

4.2 Security Objectives for the TOE

O. AUTHENTICATE_LIG

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

O. AUTHORISE_LIG

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.

O.AUDITING_LIG

The LIS shall support logging and auditing of LIG user actions.Actions of the LIC shall not be logged.

O. AUTHENTICATE_OMM

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

O. AUTHORISE_OMM

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.

O.AUDITING_OMM

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

O. AUTHENTICATE_CUS

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

O. AUTHORISE_CUS

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.

O.AUDITING_CUS

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

O.SEPARATE_USERS

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

O.PROTECT_COMMUNICATION

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

4.3 Security Objectives for the Operational Environment

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 OMS/CUS/LIS or similar attacks.

OE.PROTECT_COMMUNICATION

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.

OE.SERVER_SECURITY

The operator shall ensure that the MSC Server 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 that LI, CUS and OMM 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 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

This page intentionally left blank.

Chapter 5

Security Requirements

Table of Contents

5.1 Extended Components Definition

This 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.

FAU_GEN.3 Simplified audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.3.1 The TSF shall be able to generate an audit record of the following auditable events**: [assignment:** *defined auditable events*]**.**

FAU_GEN.3.2 The TSF shall record within each audit record: Date and time of the event, **[assignment:** *other information about the event*]**.**

5.2 Definitions

The following terms are used in the security requirements:

Lawful Interception related roles:

- LIG Administrator
- LIG Supervisor
- LIG Maintenance
- LIG PowerUser
- LIG Operator
- Customizable roles

Lawful Interception related external entities:

- LI Center (LIC)

Management related roles

- OMM Administrator
- OMM Supervisor
- OMM Maintainer
- OMM PowerUser
- OMM Operator
- Customizable roles

Management related external entities

- Element Management System (EMS)

Billing related roles

- CUS Admin
- CUS Manager
- CUS Operator

Billing related external entities

- Billing Center

None of the roles above has full “root” access to the TOE. This is reserved for ZTE maintenance staff that regularly service the TOE using the systems console, but this is out of scope and not described further in this ST.

Objects:

- LI Information: Information that directly relates to actual Lawful Interception, such as telephone numbers that are being monitored.

Operations:

- Locking (of a user): a locked user can no longer login to the system until that user has been unlocked.
- Locking (of a role): if a role is locked, users that login and would normally get that role, do not get that role until they login again and the role is unlocked.

The following notational conventions are used in the requirements. Operations are indicated in **bold**, except refinements, which are indicated in ***bold italic***. In general refinements were applied to clarify requirements and/or make them more readable. Iterations were indicated by adding three letters to the component name.

5.3 Security Functional Requirements

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. Note that in some cases the environment supplies the desired functionality.

Functionality	**CUS**	**LIG**	**OMS**
Identification	FIA_UID.2.CUS	FIA_UID.2.LIG	FIA_UID.2.OMM
Authentication	FIA_UAU.2.CUS	FIA_UAU.2.LIG	FIA_UAU.2.OMM

Functionality	CUS	LIG	OMS
Logging out	FTA_SSL.3.CUS	FTA_SSL.3.LIG	FTA_SSL.3.OMM
Auth. Failure	FIA_AFL.1.CUS	FIA_AFL.1.LIG	FIA_AFL.1.OMM
Password quality	FIA_SOS.1.CUS	FIA_SOS.1.LIG	FIA_SOS.1.OMM
# of sessions	FTA_MCS.1.CUS	FTA_MCS.1.LIG	FTA_MCS.1.OMM
Roles	FMT_SMR.1.CUS	FMT_SMR.1.LIG	FTA_SMR.1.OMM
Audit	FAU_***.CUS	FAU_***.LIG	FAU_***.OMM
Management	FMT_SMF.1.CUS	FMT_SMF.1.LIG	FMT_SMF.1.OMM
Who can do	FDP_ACC.2,	FDP_ACC.2,	FDP_ACC.2, FDP_ACF.1
what	FDP_ACF.1	FDP_ACF.1	
Client comm. protection	OE.PROTECT_COM-MUNICATION	OE.PROTECT_COM-MUNICATION	FDP_ITT.1.OMM
Ext. Server comm. protection	FTP_ITC.1.BIL	OE.PROTECT_COM-MUNICATION	FTP_ITC.1.EMS

5.3.1 CUS-related SFRs

FIA_UID.2.CUS User identification before any action

FIA_UID.2.1 The ***CUS*** shall require each ***CUS-*** user to be successfully identified

- **by username (in all cases),and**
- **by IP-address (if so configured for that** user[10] **).**

and ensure that the user is allowed to login at this time (if so configured for that user) before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2.CUS User authentication before any action

FIA_UAU.2.1 The ***CUS*** shall require each ***CUS-***user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_AFL.1.CUS Authentication failure handling

FIA_AFL.1.1 The ***CUS*** shall detect when **a *CUS*-administrator configurable positive integer within 2-3** unsuccessful authentication attempts occur related to **the same CUS-user account**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the ***CUS*** shall **lock the CUS-user** account[11]

[10] For administrator, the IP range can directly be configured. For normal users the IP range can be configured via the roles.

[11] Unless this account has been set to unlockable.

- **until unlocked by the CUS-administrator, or**
- **until a CUS administrator configurable positive integer within [24-infinity] of hours have passed, if the account has not been set to permanent locking.**

FIA_SOS.1.CUSVerification of secrets

FIA_SOS.1.1 The ***CUS*** shall provide a mechanism to verify that ***CUS passwords*** meet:

- **At least 6 characters including three of the four types: number, small letter, capital letter, other characters**
- **cannot be the same as the user name, the user name** twice[12] **,the username in** reverse[13] **or a common dictionary word**
- **can be configured to expire after a configurable amount of time < 180 days**
- **can be configured to be different from the previous 5 CUS-passwords when changed**

FTA_SSL.3.CUS TSF-initiated termination

FTA_SSL.3.1 The ***CUS*** shall terminate an interactive ***CUS***-session

- after **a configurable period of inactivity less than 30 minutes**
- when[14] **the allowed work time (if so configured for that CUS-user) expires, or**
- ***when one of the CUS-user roles is being locked while the CUS-user is logged in.***

FTA_MCS.1.CUS Basic limitation on multiple concurrent sessions

FTA_MCS.1.1 The ***CUS*** shall restrict the maximum number of concurrent sessions that belong to the same ***CUS-user***.

FTA_MCS.1.2 The ***CUS*** shall enforce, by default, a limit of **1** sessions per ***CUS-user and a limit of 64 sessions for all CUS-users together.***

FMT_SMR.1.CUS Security roles

FMT_SMR.1.1 The ***CUS*** shall maintain the roles:

- **CUS Admin**
- **CUS Manager**
- **CUS Operator**

FMT_SMR.1.2 The ***CUS*** shall be able to associate ***CUS***-users with ***one or more*** roles.

FAU_GEN.3.CUS Simplified audit data generation

FAU_GEN.3.1 The ***CUS*** shall be able to generate an audit record of the following auditable events**:**

(in the CUS security log):

- **authentication success/failure**
- **user account is locked**

[12] If the username is chang, "changchang" is not allowed.

[13] If the username is chang, "gnahc" is not allowed.

[14] The sentence was refined to make it more readable.

- **user account is unlocked**
- **user account is enabled**
- **user account is disabled**

FAU_GEN.3.2 The ***CUS*** shall record within each audit record:

- Date and time of the event,
- **User name**
- **Type of event**
- **Detailed Information**

FAU_SAR.1.CUS Audit review

FAU_SAR.1.1 The ***CUS*** shall provide **CUS Administrator** with the capability to read **operation log, system log and security log** from the ***CUS*** audit records.

FAU_SAR.1.2 The ***CUS*** shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_STG.1.CUS Protected audit trail storage

FAU_STG.1.1 The ***CUS*** shall protect the stored audit records in the ***CUS*** audit trail from unauthorised deletion.

FAU_STG.1.2 The ***CUS*** shall be able to **prevent** unauthorised modifications to the stored audit records in the ***CUS*** audit trail.

FAU_STG.4.CUS Prevention of audit data loss

FAU_STG.4.1 The ***CUS*** shall **overwrite the oldest stored audit**records[15] if the ***CUS*** audit trail is full.

FTP_ITC.1.BIL Inter-TSF trusted channel

FTP_ITC.1.1 The ***CUS*** shall provide a communication channel between itself and ***the Billing Center*** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The ***CUS*** shall permit the ***CUS and the Billing Center*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The ***CUS*** shall initiate communication via the trusted channel for **sending billing data (Call Detail Records)**.

FMT_SMF.1.CUS Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following ***CUS*** management functions:

[15] The operation was completed to “take no other actions”, and this was subsequently refined away to make the sentence more readable.

CUS Management function	Related to SFR
Set whether a CUS user can only login from certain IP-addresses, and if so, which IP addresses	FIA_UID.2.CUS
Set the time that a CUS user may remain logged in while inactive	FTA_SSL.3.CUS
Set whether a CUS user is only allowed to work at certain times, and if so, at which times	FIA_UID.2.CUS FTA_SSL.3.CUS
Set the number of allowed unsuccessful authentication attempts	FIA_AFL.1.CUS
Set the number of hours that an account remains locked	FIA_AFL.1.CUS
Set whether a user account should be: • unlockable, or • locked (either permanently or temporarily) when it exceeds the number of allowed consecutive unsuccessful authentication attempts	FIA_AFL.1.CUS
Unlock a CUS user account	FIA_AFL.1.CUS
Set whether a CUS user password expires after a certain time, and if so, after how long	FIA_SOS.1.CUS
Set whether the new password of a CUS user must be different from the last 5 passwords when the password is changed by the user	FIA_SOS.1. CUS
Create, edit and delete customized CUS roles	FMT_SMR.1 .CUS
Add or remove roles to/from CUS users	FMT_SMR.1.CUS
Create, edit and delete CU Suser accounts	-
Disable/enable CUS user accounts	-
Lock/unlock roles	-

5.3.2 LIG-related SFRs

FIA_UID.2.LIG User identification before any action

FIA_UID.2.1 The ***LIS*** shall require each ***LIG***-user to be successfully identified

- **by username (in all cases), and**

- **by IP-address (if so configured for that** user[16] **) and ensure that the user is allowed to login at this time (if so configured for that user)**before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2.LIG User authentication before any action

FIA_UAU.2.1 The ***LIS*** shall require each ***LIG***-user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_AFL.1.LIG Authentication failure handling

FIA_AFL.1.1 The ***LIS*** shall detect when **a** ***LIG*****-administrator configurable positive integer within 2-3** unsuccessful authentication attempts occur related to **the same LIG-user account**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the ***LIS*** shall **lock the LIG-user** account[17]

- **until unlocked by the LIG-administrator, or**
- **until a LIG-administrator configurable positive integer within [24-infinity] of hours have passed, if the account has not been set to permanent locking.**

FIA_SOS.1.LIGVerification of secrets

FIA_SOS.1.1 The ***LIS*** shall provide a mechanism to verify that ***LIG passwords*** meet:

- **At least 6 characters including three of the four types: number, small letter, capital letter, other characters**
- **cannot be the same as the user name, the user name twice, the username in reverse or a common dictionary word**
- **can be configured to expire after a configurable amount of time < 180 days**
- **can be configured to be different from the previous 5 LIG-passwords when changed**

FTA_SSL.3.LIG TSF-initiated termination

FTA_SSL.3.1 The ***LIS*** shall terminate an interactive ***LIG***-session

- after a **LIG-administrator configurable period of inactivity less than 30 minutes**
- when[18] **the allowed work time (if so configured for that LIG-user) expires, or**
- ***when one of the LIG-user roles is being locked while the LIG-user is logged in.***

FTA_MCS.1.LIG Basic limitation on multiple concurrent sessions

FTA_MCS.1.1 The ***LIG*** shall restrict the maximum number of concurrent sessions that belong to the same ***LIG-user***.

FTA_MCS.1.2 The ***LIG*** shall enforce, by default, a limit of **1** sessions per ***LIG-user and a limit of 255 sessions for all LIG-users together.***

[16] For administrator, the IP range can directly be configured. For normal users the IP range can be configured via the roles.

[17] Unless this account has been set to unlockable.

[18] The sentence was refined to make it more readable.

FMT_SMR.1.LIG Security roles

FMT_SMR.1.1 The ***LIS*** shall maintain the roles:

- **LIG Administrator**
- **LIG Supervisor**
- **LIG Maintenance**
- **LIG PowerUser**
- **LIG Operator**
- **Customizable roles**

FMT_SMR.1.2 The ***LIS*** shall be able to associate ***LIS***-users with ***one or more*** roles.

FAU_GEN.3.LIG Simplified audit data generation

FAU_GEN.3.1 The ***LIS*** shall be able to generate an audit record of the following auditable events**:**

(in the LIG security log and only of LIG users and not of LIC users):

- **authentication success/failure of existing users**
- **user account is locked**
- **user account is unlocked**
- **user account is enabled**
- **user account is disabled**

FAU_GEN.3.2 The ***LIS*** shall record within each audit record:

- Date and time of the event,
- **User name**
- **Type of event**
- **Host Address**
- **Detailed Information**

FAU_GEN.3.3 ***The LIS shall record nothing on actions of*** LIC[19]

FAU_SAR.1.LIG Audit review

FAU_SAR.1.1 The ***LIS*** shall provide **LIG Administrator** with the capability to read **operation log, system log and security log** from the ***LIS*** audit records.

FAU_SAR.1.2 The ***LIS*** shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_STG.1.LIG Protected audit trail storage

FAU_STG.1.1 The ***LIS*** shall protect the stored audit records in the ***LIS*** audit trail from unauthorised deletion.

FAU_STG.1.2 The ***LIS*** shall be able to **prevent** unauthorised modifications to the stored audit records in the ***LIS*** audit trail.

Application Note:

[19] The addition of the last element is a refinement.

- Deletion of audit records is only authorized when it is done by the LIG administrator (or a suitably customized role) and the records are more than 30 days old
- Modification of audit records is never authorized

FAU_STG.4.LIG Prevention of audit data loss

FAU_STG.4.1 The ***LIS*** shall **overwrite the oldest stored audit** records[20] if the ***LIS*** audit trail is full.

FMT_SMF.1.LIG Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following ***LIG*** management functions:

LIG Management function	**Related to SFR**[21]
Set whether an LIG user can only login from certain IP-addresses, and if so, which IP addresses	**FIA_UID.2.LIG**
Set the time that an LIG user may remain logged in while inactive	**FTA_SSL.3.LIG**
Set whether an LIG user is only allowed to work at certain times, and if so, at which times	**FIA_UID.2.LIG** **FTA_SSL.3.LIG**
Set the number of allowed unsuccessful authentication attempts	**FIA_AFL.1.LIG**
Set the number of hours that an account remains locked	**FIA_AFL.1.LIG**
Set whether an LIG user account should be: • **unlockable, or** • **locked (either permanently or temporarily)** **when it exceeds the number of allowed consecutive unsuccessful authentication attempts**	**FIA_AFL.1.LIG**
Unlock an LIG user account	**FIA_AFL.1.LIG**
Set whether an LIG user password expires after a certain time, and if so, after how long	**FIA_SOS.1.LIG**
Set whether the new password of an LIG user must be different from the last 5 passwords when the password is changed by the user	**FIA_SOS.1.LIG**
Create, edit and delete customized LIG roles	**FMT_SMR.1.LIG**

[20] The operation was completed to “take no other actions”, and this was subsequently refined away to make the sentence more readable.

[21] This column of the table is for reference only, and is not part of the SFR. The same holds for the iterations.

LIG Management function	**Related to SFR**[21]
Add or remove roles to/from LIG users	**FMT_SMR.1.LIG**
Create, edit and delete LIG user accounts	-
Disable/enable LI Guser accounts	-
Lock/unlock roles	-

5.3.3 OMM-related SFRs

FIA_UID.2.OMM User identification before any action

FIA_UID.2.1 The ***OMS*** shall require each ***OMM***-user to be successfully identified

- **by username (in all cases), and**
- **by IP-address (if so configured for that** user[22]**)and ensure that the user is allowed to login at this time (if so configured for that user)** before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2.OMM User authentication before any action

FIA_UAU.2.1 The ***OMS*** shall require each ***OMM***-user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_AFL.1.OMM Authentication failure handling

FIA_AFL.1.1 The ***OMS*** shall detect when **3** unsuccessful authentication attempts occur related to **the same OMM-user account**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the ***OMS*** shall **lock the OMM-user** account[23]

- **until unlocked by the OMM-administrator, or**
- **until a OMM-administrator configurable positive integer within [24-72 or infinity] of hours have passed, if the account has not been set to permanent locking.**

FIA_SOS.1.OMM Verification of secrets

FIA_SOS.1.1 The ***OMS*** shall provide a mechanism to verify that ***OMM passwords*** meet:

- **At least 6 characters including three of the four types: number, small letter, capital letter, other characters**
- **cannot be the same as the user name, the user name twice, the username in reverse or a common dictionary word**
- **can be configured to expire after a configurable amount of time < 90 days**

[22] For administrator, the IP range can directly be configured. For normal users the IP range can be configured via the roles.

[23] Unless this account has been set to unlockable.

- **can be configured to be different from the previous 5 OMM-passwords when changed**

FTA_SSL.3.OMM TSF-initiated termination

FTA_SSL.3.1 The ***OMS*** shall terminate an interactive ***OMM***-session

- after**an OMM-administrator configurable period of inactivity less than 30 minutes**
- when[24]**the allowed work time (if so configured for that OMM-user) expires, or**
- **when one of the OMM-user roles is being locked while the OMM-user is logged in.**

FTA_MCS.1.OMM Basic limitation on multiple concurrent sessions

FTA_MCS.1.1 The ***OMS*** shall restrict the maximum number of concurrent sessions that belong to the same ***OMM-user***.

FTA_MCS.1.2 The ***OMS*** shall enforce, by default, a limit of **1** sessions per ***OMM-user and a limit of 255 sessions for all OMM-users together.***

FMT_SMR.1.OMM Security roles

FMT_SMR.1.1 The ***OMS*** shall maintain the roles:

- **OMM Administrator**
- **OMM Supervisor**
- **OMM Maintainer**
- **OMM PowerUser**
- **OMM Operator**
- **Customizable roles**

FMT_SMR.1.2 The ***OMS*** shall be able to associate ***OMS***-users with ***one or more*** roles.

FAU_GEN.3.OMM Simplified audit data generation

FAU_GEN.3.1 The ***OMS*** shall be able to generate an audit record of the following auditable events**:**

(in the OMM security log):

- **authentication success/failure of existing users**
- **user account is locked**
- **user account is unlocked**
- **user account is enabled**
- **user account is disabled**

FAU_GEN.3.2 The ***OMS*** shall record within each audit record:

- Date and time of the event,
- **User name**
- **Type of event**
- **Host Address**

[24] The sentence was refined to make it more readable.

- **Detailed Information**

FAU_SAR.1.OMM Audit review

FAU_SAR.1.1 The ***OMS*** shall provide **OMM Administrator** with the capability to read **operation log, system log and security log** from the ***OMS*** audit records.

FAU_SAR.1.2 The ***OMS*** shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_STG.1.OMM Protected audit trail storage

FAU_STG.1.1 The ***OMS*** shall protect the stored audit records in the ***OMM*** audit trail from unauthorised deletion.

FAU_STG.1.2 The ***OMS*** shall be able to **prevent** unauthorised modifications to the stored audit records in the ***OMM*** audit trail.

Application Note:

- Deletion of audit records is only authorized when it is done by the OMM administrator (or a suitably customized role) and the records are more than 30 days old
- Modification of audit records is never authorized

FAU_STG.4.OMM Prevention of audit data loss

FAU_STG.4.1 The ***OMS*** shal• **overwrite the oldest stored audit** records[25] if the ***OMM*** audit trail is full.

FDP_ITT.1.OMM Basic internal transfer protection

FDP_ITT.1.1 The TSF shall[26] prevent the **disclosure or modification** of ***all*** data when it is transmitted between the ***OMM Client and the OMS***.

FTP_ITC.1.EMS Inter-TSF trusted channel

FTP_ITC.1.1 The ***OMS*** shall provide a communication channel between itself and ***the EMS*** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The ***OMS*** shall permit the ***OMS and the EMS***to initiate communication via the trusted channel.

FTP_ITC.1.3 The ***OMS*** shall initiate communication via the trusted channel for **performing OMM-related actions**.

FMT_SMF.1.OMM Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following ***OMM***management functions:

[25] The operation was completed to “take no other actions”, and this was subsequently refined away to make the sentence more readable.

[26] The reference to the SFP was refined away: as FDP_ITT.1 already states all relevant parts of the policy, defining it separately is superfluous.

OMM Management function	Related to SFR
Set whether an OMM user can only login from certain IP-addresses, and if so, which IP addresses	**FIA_UID.2.OMM**
Set the time that an OMM user may remain logged in while inactive	**FTA_SSL.3.OMM**
Set whether an OMM user is only allowed to work at certain times, and if so, at which times	**FIA_UID.2.OMM** **FTA_SSL.3.OMM**
Set the number of hours that an account remains locked	**FIA_AFL.1.OMM**
Set whether an OMM user account should be: • **unlockable, or** • **locked (either permanently or temporarily) when it exceeds the number of allowed consecutive unsuccessful authentication attempts**	**FIA_AFL.1.OMM**
Unlock an OMM user account	**FIA_AFL.1.OMM**
Set whether an OMM user password expires after a certain time, and if so, after how long	**FIA_SOS.1.OMM**
Set whether the new password of an OMM user must be different from the last 5 passwords when the password is changed by the user	**FIA_SOS.1.OMM**
Create, edit and delete customized OMM roles	**FMT_SMR.1.OMM**
Add or remove roles to/from OMM users	**FMT_SMR.1.OMM**
Create, edit and delete OMM user accounts	-
Disable/enable OMM user accounts	-
Lock/unlock roles	-

5.3.4 Common SFRs

FDP_ACC.2 Complete access control

FDP_ACC.2.1The TSF shall enforce the **Role Policy** on **all roles and the TOE** and alloperationsamong ***roles and the TOE*** .

FDP_ACC.2.2 The TSF shall ensure that all operations between any ***role and the TOE*** are covered by an access control SFP.

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **Role Policy** to objects based on the following: **all roles, the TOE**.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among ***roles*** and ***the TOE*** is allowed:

- **LIG Administrator can configure the LIG and perform the actions specified in FMT_SMF.1.LIG**
- **Other LIG Roles can perform LIG-related actions according to their role definition/customization**
- **·LI Center can access LI-information**
- **CUS Administrator can perform all CUS-related actions in the TOE, including those specified in FMT_SMF.1.CUS**
- **Other CUS Roles can perform CUS-related actions according to their role definition/customisation**
- **OMM Administrator can perform all OMM-related actions in the TOE, including those specified in FMT_SMF.1.OMM**
- **Other OMM Roles can perform OMM-related actions according to their role definition/customisation**

FDP_ACF.1.3, ***(refined away)***.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- **LIG Users cannot perform OMM and CUS actions**
- **CUS Users cannot perform OMM and LIG actions**
- **OMM Users cannot perform CUS and LIG actions**
- **No users (other than LI Center) can access LI-information**

5.4 Security Assurance Requirements

The assurance requirements are EAL2+ALC_FLR.2 and have been summarized in the following table:

Assurance Class	Assurance Components	
	Identifier	Name
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures

ALC: 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
ASE: 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
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

5.5 Security Assurance Requirements Rationale

The Security Assurance Requirements for this Security Target are EAL2+ALC_FLR.2. The reasons for this choice are that:

- EAL 2 is deemed to provide a good balance between assurance and costs and is in line with ZTE customer requirements.
- ALC_FLR.2 provides assurance that ZTE has a clear and functioning process of accepting security flaws from users and updating the TOE when required. This is also in line with ZTE customer requirements.
- The refinements are derived from ZTE customer requirements as well.

This page intentionally left blank.

Chapter 6

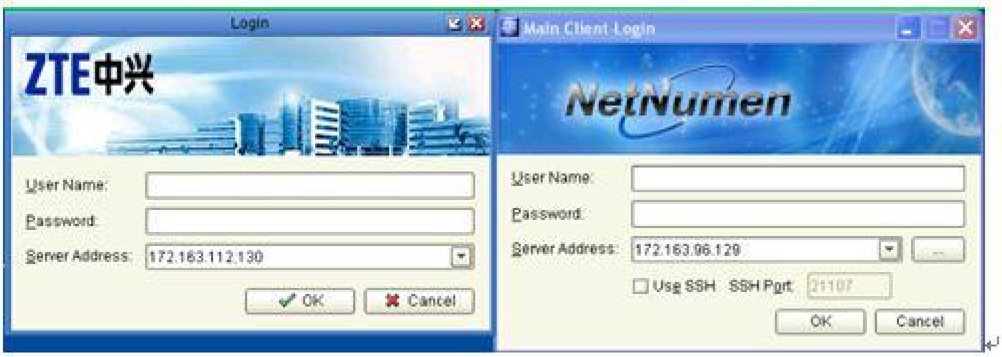
TOE Summary Specification

Secure management of the TOE, to ensure that only properly authorized staff can manage the TOE.

General: functionality is provided through the use of the login screens depicted below and a series of standard windows providing the management functionality.

FIA_UID.2.*, FIA_UAU.2.*, FIA_AFL.1.*

Whenever a user of the TOE wishes to use the TOE, the user needs to use one of the clients of the TOE. The first action required by the user is then to log-in.



Login

User Name:

Password:

Server Address: 172.163.112.130

Main Client Login

User Name:

Password:

Server Address: 172.163.96.129

□ Use SSH SSH Port 21107

The TOE allows the appropriate administrator to configure (for each user), how that user must log-in:

- The user must always provide a username and a password
- Whether the user can only login from a predefined IP-address
- Whether the user is only allowed to be logged in during a certain time interval (e.g. office hours)
- Whether an account is unlockable or not, and when an account is not unlockable:
  - how many times a user can fail consecutive authentication attempts before that account is locked
  - how the account is unlocked by the Administrator or until a predefined time elapses

FTA_MCS.1.*

Even if all of the above is correct, the user can still be denied access when:

- the user is already logged in
- too many other users are already logged in

FTA_SSL.3.*

The TOE will log a user out when:

- The Administrator locks one of the roles that that user currently has. The user can subsequently log in again, but he will not have that role.
- The user is only allowed to be logged in during a certain time interval, and this interval expires.

FIA_SOS.1.*

Whenever the user has to provide a new password to the TSF, these passwords have to meet certain rules to ensure that the passwords cannot be easily guessed or broken by brute force. Passwords that do not meet these rules are rejected by the TOE.

FMT_SMR.1.*, FDP_ACC.2, FDP_ACF.1, FMT_SMF.1.*

The TOE provides a set of roles that can be assigned to users. The users can then use these roles to perform the actions (including various management actions) allowed by the roles.

FAU_GEN.3.*, FAU_SAR.1, FAU_STG.1, FAU_STG.4

Activities of the users are logged, and only certain roles are allowed to view the logs. The logs cannot be edited. They can only be deleted by the respective administrators (or a suitably customized role) and then only when they are 30 days old or older. When they fill up they overwrite themselves.

An exception is made for FAU_GEN.3.LIC: no actions of the LI Center are logged.

Provides secure access to its Lawful Interception functionality, ensuring that only the LIC can access this functionality

FDP_ACF.1

No user (except LIC) has any form of access to the LI functionality. LIG users can only perform some minor configuration to allow the LIC to connect to the LIS, but cannot access the LI functionality of the LIS by themselves. The other clients cannot see the LIS at all. Data exchange between LIS, CUS, OMS and Service Part is carefully controlled to prevent LI data from the LIS or Service Part leaking out.

Provides secure interaction between itself and the Billing Center, itself and the EMS and itself and the OMM Client so that data cannot be read or modified in between

FTP_ITC.1.BIL

The connection between the Billing Center and the TOE is protected by sftp.

FTP_ITC.1.EMS

The connection between the EMS and the TOE is protected by sftp and ssh.

FDP_ITT.1.OMM

The connection between the OMM Client and the TOE is protected by sftp and ssh.

Chapter 7
Rationales

Table of Contents

7.1 Security Objectives Rationale

Assumptions/OSPs/Threats Objectives	
OSP.USERS The TOE must: • authenticate LIG users, log their activities, and allow them to set-up and configure the LIG functionality • authenticate CUS users, log their activities, and allow them to set-up and configure the billing functionality • authenticate OMM users, log their activities, and allow OMM users to set-up and configure the TOE functionality (except for billing and LI functionality)	This OSP is primarily implemented by: • the combination of O.*_LIG that together restate the first bullet. • the combination of O.*_CUS, that together restate the second bullet. • the combination of O.*_OMM, that together restate the third bullet. Additionally, to perform logging, the TOE must have a time source. OE.TIME states that this time source will be an external NTP Server connected to the TOE.
T.UNAUTHORISED TA.ROGUE_USER_LIG, TA.ROGUE_USER_CUS or TA.ROGUE_USER performs actions on the TOE that he is not authorized to do.	This threat is countered by the following security objectives: • OE.TRUST&TRAIN that ensures that only users that are properly trusted and trained will be able to gain access to certain roles • O.AUTHENTICATE_* that ensures users are properly authenticated so the TOE knows which roles they have • O.AUTHORISE_* that ensures users with certain roles have rights to do certain actions for a certain group of functionality (OMM, CUS, LIG). • O.SEPARATE_USERS that ensures that users without rights for certain functionality groups cannot access that functionality.

Assumptions/OSPs/Threats	Objectives
	So the only way that a user can perform an action is when he has a role for that action, and the only way he can get this role is if he is properly trained and trusted. Therefore this threat is countered.
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.	This threat is countered by: • OE.TRUST&TRAIN that ensures that only users that are properly trusted and trained will be able to gain access to certain roles. This should go a long way to prevent the threat from being realized. • Should this prove insufficient, O.AUDITING_* will ensure that the actions of the user can be traced back to him. Together these security objectives counter the threat.
T.UNKNOWN_USER TA.NETWORK gains unauthorized access to the TOE and is able to perform actions on the TOE.	This threat is countered by: • OE.CLIENT_SECURITY, preventing the attacker to gain access to the clients • O.AUTHENTICATE_*, preventing the attacker to gain access to the servers Together these two security objectives counter the threat.
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, the EMS or the Billing Center and/or. • gain unauthorized knowledge about traffic between the TOE and the EMS/Billing Center.	This threat is countered by O.PROTECT_COM-MUNICATION that protects traffic between: • the OMS and the EMS • the CUS and the Billing Center • the OMS and the OMM Client As this is all traffic between the TOE and the EMS/Billing Center, this threat is countered.
T.PHYSICAL_ATTACK TA.PHYSICAL gains physical access to the TOE (either client or server) and is able to use its functionality.	This threat is countered by two security objectives: • OE.SERVER_SECURITY stating that the MSCS part of the TOE must be protected from physical attack • OE.CLIENT_SECURITY stating that the client part of the TOE must be protected from physical attack. Together these two counter the entire threat.

Assumptions/OSPs/Threats Objectives	
A.TRUSTED_SYSTEMS It is assumed that: • 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	The first, second and fourth bullet of this assumption are upheld by OE.TRUSTED_SYSTEMS which restates the assumption. The third bullet of this assumption is upheld by OE.PROTECT_COMMUNICATION which lists the various communications to be protected.

7.2 Security Functional Requirements Rationale

Security objectives	SFRs addressing the security objectives
O. AUTHENTICATE_LIG The TOE shall support LIG Client user authentication, allowing the LIS to accept/reject LIG users based on username and password.	This objective is met by: • FIA_UID.2.LIG stating that identification will be done by username, but also IP-address and login time • FIA_UAU.2.LIG stating that the users must be authenticated • FIA_SOS.1.LIG stating that passwords must have a minimum quality • FIA_AFL.1.LIG stating what happens when authentication fails repeatedly • FTA_SSL.3.LIG logging users off when they are no longer allowed to work or when their role is locked • FTA_MCS.1.LIG limiting the number of logins per user • FMT_SMF.1.LIG configuring all of the above. Together, these SFRs meet the objective and provide further detail.

Security objectives	SFRs addressing the security objectives
O. AUTHENTICATE_OMM The TOE shall support OMM Client user authentication, allowing the OMS to accept/reject OMM users based on username and password.	This objective is met by: • FIA_UID.2.OMM stating that identification will be done by username, but also IP-address and login time. • FIA_UAU.2.OMM stating that the users must be authenticated. • FIA_SOS.1.OMM stating that passwords must have a minimum quality. • FIA_AFL.1.OMM stating what happens when authentication fails repeatedly. • FTA_SSL.3.OMM logging users off when they are no longer allowed to work or when their role is locked. • FTA_MCS.1.OMM limiting the number of logins per user. • FMT_SMF.1.OMM configuring all of the above. Together, these SFRs meet the objective and provide further detail.
O. AUTHENTICATE_CUS The TOE shall support CUS Client user authentication, allowing the TOE to accept/reject CUS users based on username and password.	This objective is met by: • FIA_UID.2.CUS stating that identification will be done by username, but also IP-address and login time. • FIA_UAU.2.CUS stating that the users must be authenticated. • FIA_SOS.1.CUS stating that passwords must have a minimum quality. • FIA_AFL.1.CUS stating what happens when authentication fails repeatedly. • FTA_SSL.3.CUS logging users off when they are no longer allowed to work or when their role is locked. • FTA_MCS.1.CUS limiting the number of logins per user. • FMT_SMF.1.CUS configuring all of the above. Together, these SFRs meet the objective and provide further detail.

Security objectives	SFRs addressing the security objectives
O. AUTHORISE_LIG 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.	This objective is met by: • FMT_SMR.1.LIG stating the predefined and customizable roles. • FDP_ACC.2 and FDP_ACF.1 defining a Role Policy, which states how the various roles manage the TOE. • FMT_SMF.1.LIG configuring all of the above. Together, these SFRs support a flexible authorization framework.
O. AUTHORISE_OMM 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.	This objective is met by: • FMT_SMR.1.OMM stating the predefined and customizable roles. • FDP_ACC.2 and FDP_ACF.1 defining a Role Policy, which states how the various roles manage the TOE. • FMT_SMF.1.OMM configuring all of the above. Together, these SFRs support a flexible authorization framework.
O. AUTHORISE_CUS 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.	This objective is met by: • FMT_SMR.1.CUS stating the predefined and customizable roles. • FDP_ACC.2 and FDP_ACF.1 defining a Role Policy, which states how the various roles manage the TOE. • FMT_SMF.1.CUS configuring all of the above. Together, these SFRs support a flexible authorization framework.
O.SEPARATE_USERS 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	This objective is met by FDP_ACC.2 and FDP_ACF.1. FDP_ACF.1.4 specifically forbids the actions listed in the security objective.

Security objectives	SFRs addressing the security objectives
O.AUDITING_LIG The TOE shall support logging and auditing of LIG user actions. Actions of the LIC shall not be logged.	This objective is met by: • FAU_GEN.3.LIG showing which events are logged • FAU_SAR.1.LIG showing that the logged events can be audited and by whom • FAU_STG.1.LIG showing how the audit logs are protected • FAU_STG.4.LIG stating what happens when the audit log becomes full • FMT_SMF.1.LIG configuring all of the above Together, these SFRs support a flexible logging and auditing framework. The additional 3rd element of FAU_GEN.3.LIG shows that no LIC actions hall be logged.
O.AUDITING_CUS The TOE shall support logging and auditing of CUS user actions	This objective is met by: • FAU_GEN.3.CUS showing which events are logged • FAU_SAR.1.CUS showing that the logged events can be audited and by whom • FAU_STG.1.CUS showing how the audit logs are protected • FAU_STG.4.CUS stating what happens when the audit log becomes full • FMT_SMF.1.CUS configuring all of the above Together, these SFRs support a flexible logging and auditing framework.
O.AUDITING_OMM The TOE shall support logging and auditing of OMM user actions.	This objective is met by: • FAU_GEN.1.OMM showing which events are logged in the security and system logs • FAU_SAR.1.OMM showing that the logged events can be audited and by whom • FAU_STG.1.OMM showing how the audit logs are protected • FAU_STG.4.OMM stating what happens when the audit log becomes full • FMT_SMF.1.OMM configuring all of the above Together, these SFRs support a flexible logging and auditing framework.

Security objectives	SFRs addressing the security objectives
O.PROTECT_COMMUNICATION 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 disclosure and modification	This objective is met by: • FTP_ITC.1.EMS restating the first bullet • FTP_ITC.1.BIL restating the second bullet • FDP_ITT.1.OMM restating the third bullet

7.3 Dependencies

SFR	Dependencies
FIA_UID.2.XYZ[27]	-
FIA_UAU.2.XYZ	FIA_UID.1: met by FIA_UID.2.XYZ
FIA_AFL.1.XYZ	FIA_UAU.1: met by FIA_UAU.2.XYZ
FIA_SOS.1.XYZ	-
FTA_SSL.3.XYZ	-
FTA_MCS.1.XYZ	FIA_UID.1: met by FIA_UID.2.XYZ
FMT_SMR.1.XYZ	FIA_UID.1: met by FIA_UID.2.XYZ
FAU_GEN.3.XYZ	FPT_STM.1: met in environment by OE.TIME
FAU_SAR.1.XYZ	FAU_GEN.1: met by FAU_GEN.3.XYZ, which is similar enough to FAU_GEN.1 to meet the dependency
FAU_STG.1.XYZ	FAU_GEN.1: met by FAU_GEN.3.XYZ, which is similar enough to FAU_GEN.1 to meet the dependency
FAU_STG.4.XYZ	FAU_GEN.1: met by FAU_GEN.3.XYZ, which is similar enough to FAU_GEN.1 to meet the dependency
FPT_SMF.1.XYZ	-
FPT_ITC.1.BIL	-
FPT_ITC.1.EMS	-
FDP_ITT.1.OMM	FDP_ACC.1 or FDP_IFC.1: not met, since the policy was refined away the dependency is unnecessary

[27] Where XYZ can be CUS, LIG or OMM

SFR	Dependencies
FDP_ACC.2	FDP_ACF.1: met
FDP_ACF.1	FDP_ACC.1: met by FDP_ACC.2 FMT_MSA.3: not met, as the policy does not use security attributes, management of these attributes is unnecessary.

SAR	Dependencies
EAL 2	All dependencies within an EAL are satisfied
ALC_FLR.2	-

Figures