ZXSS10 SS1B and MSG-9000
Communication System
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

LEGAL INFORMATION

Revision History

Version	Date	Comment
0.1	Feb 16, 2011	First version
0.2	August 9, 2011	Update after inclusion of Media Gateway
0.3	September 22, 2011	Complete first draft of SFR
0.4	September 29, 2011	First draft
0.5	October 5, 2011	Update according to EOR
0.6	October 6, 2011	Update according to EOR
0.7	October 18, 2011	Update according to EOR
0.8	November 01, 2011	Update according to EOR

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 is intentionally blank.

Contents

1 ST Introduction

1.1 ST and TOE References

This is version 0.8 of the Security Target for the ZTE softswitch and media gateway communication system, which consists of:

- ZTE ZXSS10 SS1b Soft Switching System
- MSG-9000 Media Gateway
- U31 v12.11.40 Element Management System
- Network Management Service Interface (NMSI) v2.3

1.2 TOE Overview and usage

The TOE is ZTE softswitch and media gateway communication system V1.0. The TOE consists of a softswitch (SS1b), a media gateway (MSG-9000) between the SS1b and the PSTN network, an element management system (EMS), and a network management service interface (NMSI). The SS1b is used to provide signal transfer, control, and management to the telecommunications network. The media gateway is a translation device that translates the traffic from PSTN to IP network. It also routes the traffic to the destination media gateway using the routing information provided by the SS1b. The EMS is the management console used for operators to manage the SS1b and media gateway. The NMSI is a gateway between the SS1b and the BOSS (Business operation support system) server from the operator. It provides I&A to the BOSS.

The TOE has the following general functionalities:

- Softswitch SS1b:
  - Telecommunications functionalities:
    - Interact with PSTN, Wireless Network, and Telecommunication IP network to perform the management and control functions of the telecommunication network
    - Interact with the Billing Center to charge for these functionalities
  - Management functionalities:
    - Interact with EMS to be managed and configured (except for lawful interception)
    - Interact with the BOSS to allow the BOSS User to manage the user profile.
- Media gateway MSG-9000:
  - Telecommunication functionalities:
    - Connects the PSTN to the IP core network through trunk lines, and performs voice/fax conversion on the PSTN/ISDN side as well as on the IP network side

- Interconnect signaling between SS7 and packet switched network
- Connects the analog Z interface, ISDN users, V5.2 users and DSL users to the IP network.

- Management functionalities:
  - Interact with EMS to be managed and configured (except for lawful interception)

- EMS system:
  - EMS server (EMS): manage SS1b and media gateway
  - EMS client: a GUI for user to use EMS server
- NMSI:
  - Interface between BOSS to the SS1b.

The interconnection of each part of the TOE is depicted in *Figure 1*.

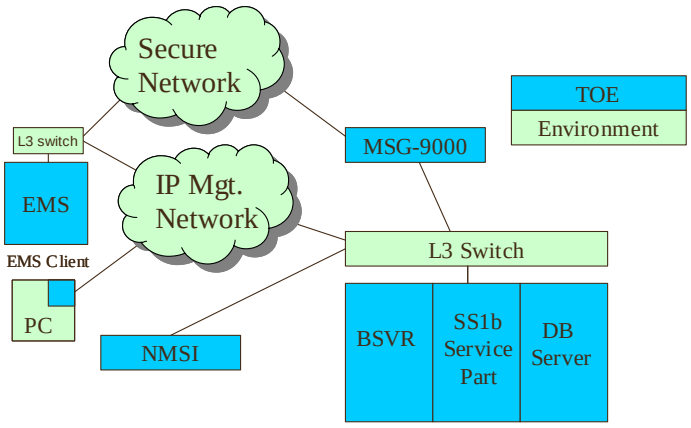


Figure 1 Interconnection between each part of the TOE

These entities are:

- A ZXSS10 SS1b Softswitch, consisting of:
  - A SS1b Service Part, responsible for handling all incoming and outgoing traffic, and performing telecommunications services.
  - A BSVR (Billing Server), responsible for generate billing information and providing this information to the Billing Center for further processing.
  - A DB Server (Database Server), responsible for storing service data such as route data, number analysis data, and the user profile data.
- An ZXMSG 9000 Media Gateway, responsible for translating the traffics from PSTN to IP network.
- An NMSI （Network Management Service Interface), is a gateway between BOSS to the SS1b. It provides I&A to the BOSS and pass MML commands from BOSS to SS1b.
- An EMS (Element Management System), responsible for management and maintenance of the whole SS1b and media gateway.
- An EMS Client, consisting of a Java application, running on a non-TOE workstation.

The BSVR and the DB server connected via the SS1b service part to the external network. They do not directly connect to the external network. The NMSI is connected to the same L3 switch as the SS1b but is located in different VLAN. The EMS Server & EMS client could be further away (e.g. connected over the IP management network). The EMS server does not directly connect to the external network but connect through an L3 switch to the external network.

The ZXSS10 SS1b and MSG-9000 media gateway performs management, control, and routing part of the Telecommunication Network and is therefore connected to a wide variety of other systems, as shown in *Figure 2*.

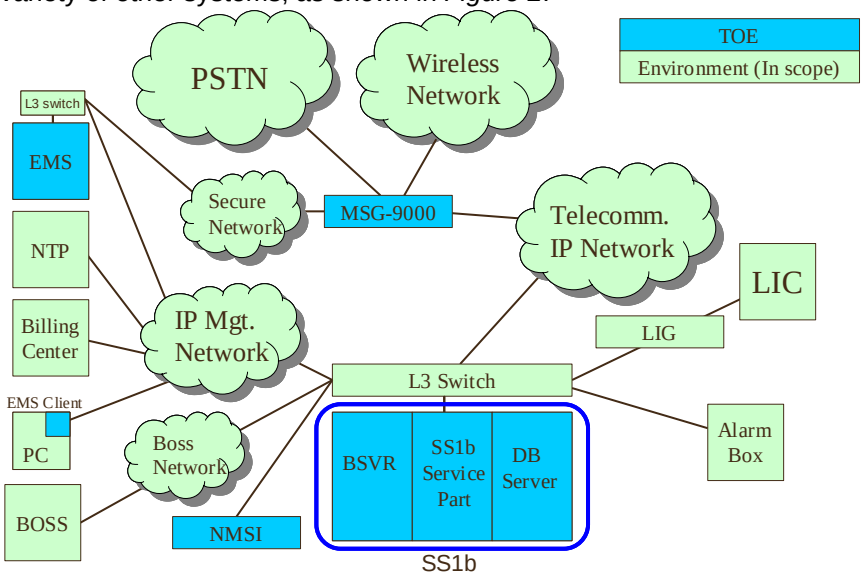


Figure 2: The TOE in its environment

These additional[1] systems and networks are:

- A Billing Center. This is a centralized server that processes the billing information of multiple TOEs (and other equipment). It obtains the billing information from the BSVR part of the TOE.
- A BOSS (Business Operation Support System). BOSS is used as a gateway for operator to manage its subscribers. BOSS connects to the NMSI of the TOE.
- The wireless network and PSTN (Public Switching Telecommunication Network): The traditional fixed switching networks that connect subscribers to each other. These networks connect to the MSG-9000 part of the TOE.
- Telecommunication IP network: IP network such as internet. It connects to the SS1b service part.
- LIG and LIC: Lawful interception gateway and lawful interception center. LIC issues commands to LIG, and LIG connects to SS1b to transfer lawful interception commands from the LIC.

[1] Additional to those described earlier

- NTP: provides time to the TOE.
- IP Management Network: An operator maintained network where all management entities (EMS, Billing center, NTP, EMS server, etc) are all connected to it. IP management network is separated from the telecommunication network.
- BOSS network: a operator maintained VLAN for all BOSSes to connect to NMSI.
- A secure network between the EMS and the MSG-9000 to protect the communication between the EMS and the MSG-9000.
- PSTN: Public Switched Telephone Network, conventional analog telephone network.
- Wireless Network: network such as GSM, UMTS, CDMA. Users from this network can communicate with users in PSTN or telecommunication IP network via SS1b.
- Telecommunication IP network: network contains equipments such as user level VoIP phone, HLR, media gateways, and access gateways. Note that internet is not part of this network.

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 management of SS1b user profile data, to ensure only properly authenticated external entities can manage SS1b user profile data.
- Provides secure access of SS1b billing data, to ensure only properly authenticated external entities can access SS1b billing data.
- Provides a flexible role-based authorization framework with predefined and customizable roles (EMS only)
- Provides logging and auditing of user actions (EMS only)
- Provides secure interaction between SS1b and the billing center, so that billing data cannot be read or modified in between
- Provides secure interaction between SS1b and the BOSS, so that user profile data cannot be read or modified in between

1.2.2 Non-TOE Hardware/Software/Firmware

The TOE requires network connectivity, a NTP server as time source, and L3 switches to separate its various networks. Additionally, the EMS client requires:

Type	Name and version
Workstation	A PC suitable to run the OS (see below) and with at least 2GB memory, or GPDU1 PCBA[2]
OS	ZTE CGSL V3_02_00_P3, or

[2] GPDU1 PCBA is a blade server

	Windows 7 or above

1.3 TOE Description

1.3.1 Physical scope

The TOE consists of the following:

Type		**Name and version**	
Hardware	SS1b service part	ESPC	
	DB server	GPDU1 PCBA	
	BSVR	GPDU1 PCBA	
	MSG-9000	Central Control Unit	2 x MOMP
			2 x MCMP
			2 x MSIPI
			2 x MUIMC
			2 x CLKG
		Service Resource Unit	1 x MRB
			1 x MTDB
			2 x MIPI
			1 x MVTCA
			2 x MUIMT
			1 x MSPB
	EMS server	GPDU1 PCBA	
	NMSI	GPDU1 PCBA	
Software	SS1b service part	ZXSS10 SS1b v2.0.1.07	
	DB server	Oracle 10.2.0.4 Suse linux 10 ZXSS10 SS1b v2.0.1.07	
	BSVR	Oracle 10.2.0.4 Suse linux 10 ZXSS10 SS1b v2.0.1.07	
	MSG-9000	ZXMSG9000 v1.0.05	
	EMS server	NetNumen U31 R30 V12.11.40 CGSL V3.02.00_P3 Oracle 10.2.0.4.0 for Linux JDK1.6.0_18	
	NMSI	CGSL V3_02_00_P3 NMSI 2.2.4	
	EMS client	NetNumen U31 R30 V12.11.40	

The TOE is delivered with the following guidance:

Operational guidance is:

ZXSS10 SS1b guidance
CC Guidance
• ZXSS10 SS1b Common Criteria Security Evaluation – Certified Configuration R1.0
Standard guidance
• ZXSS10 SS1b (V2.0.1.07) Documentation Guide
• ZXSS10 SS1b (V2.0.1.07) System Description
• ZXSS10 SS1b (V2.0.1.07) Product Description
• ZXSS10 SS1b (V2.0.1.07) Hardware Description
Installation and maintenance
• ZXSS10 SS1b (V2.0.1.07) Hardware Installation Guide
• ZXSS10 SS1b (V2.0.1.07) Software Installation Guide Foreground Board
• ZXSS10 SS1b (V2.0.1.07) Software Installation Guide PC Server
• ZXSS10 SS1b (V2.0.1.07) Software Installation Guide SUN Server
Data configuration
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide AG Interconnection
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide Application Server Interconnection
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide Digit Analysis
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide DIGITMAP
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide Disaster Recovery
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide Global Configuration
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide H323 GK Interconnection
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide H323 Terminal Interconnection
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide IAD Interconnection
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide MGCF Feature
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide MSG9000 Interconnection
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide Other SS Interconnection
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide PRA and BRA Subscriber
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide PRA Trunk
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide Route
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide SCP Interconnection
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide SG Interconnection
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide SHLR

Interconnection
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide SIP Terminal Interconnection
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide SSF Feature
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide Subscriber Allocation
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide TG Interconnection
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide Trunk
• ZXSS10 SS1b (V2.0.1.07) Data Configuration Guide V5 Interconnection
• ZXSS10 SS1b (V2.0.1.07) Global Variable Reference
• ZXSS10 SS1b (V2.0.1.07) Northbound Interface Reference (Toll_Office_Format)
• ZXSS10 SS1b (V2.0.1.07) Operation Guide Data Backup and Restoration
• ZXSS10 SS1b (V2.0.1.07) Operation Guide File Management and Data Query
• ZXSS10 SS1b (V2.0.1.07) Operation Guide Signaling Tracing
• ZXSS10 SS1b (V2.0.1.07) Operation Guide System Maintenance
• ZXSS10 SS1b (V2.0.1.07) Operation Guide Traffic Control
• ZXSS10 SS1b (V2.0.1.07) Operation Guide Traffic Statistics
• ZXSS10 SS1b (V2.0.1.07) Service Provisioning Guide Authenticationand Call Restriction
• ZXSS10 SS1b (V2.0.1.07) Service Provisioning Guide CENTREX
• ZXSS10 SS1b (V2.0.1.07) Service Provisioning Guide Multi-Line Selected Group
• ZXSS10 SS1b (V2.0.1.07) Service Provisioning Guide Supplementary Service I
• ZXSS10 SS1b (V2.0.1.07) Service Provisioning Guide Supplementary Service II
• ZXSS10 SS1b (V2.0.1.07) Timer Reference
• ZXSS10 SS1b (V2.0.1.07) Traffic Statistics Entity Reference Volume I
• ZXSS10 SS1b (V2.0.1.07) Traffic Statistics Entity Reference Volume II
Alarm
• ZXSS10 SS1b (V2.0.1.07) Alarm and Notification Message Reference Alarm Volume
• ZXSS10 SS1b (V2.0.1.07) Alarm and Notification Message Reference Notification Volume
• ZXSS10 SS1b (V2.0.1.07) Failure Code Reference I
• ZXSS10 SS1b (V2.0.1.07) Failure Code Reference II
• ZXSS10 SS1b (V2.0.1.07) Failure Code Reference III
• ZXSS10 SS1b (V2.0.1.07) Routine Maintenance
• ZXSS10 SS1b (V2.0.1.07) Troubleshooting Guide
BSVR
• ZXSS10 SS1b (V2.0.1.07) Charging Server User Manual
BOSS

• ZXSS10 SS1b (V2.0.1.07) Softswitch Control Equipment BOSS Command Reference
• ZXSS10 SS1b (V2.0.1.07) Softswitch Control Equipment BOSS Command Reference (Supplementary)
MSG-9000 Guidance
• ZXMSG 9000(V1.0.05.R03)_Guide to Documentation_EN
• ZXMSG 9000(V1.0.05.R03)_Hardware Description---9000 Volume_EN
• ZXMSG 9000(V1.0.05.R03)_Hardware Installation---9000 Volume_EN
• ZXMSG 9000(V1.0.05.R03)_Software Installation---9000 Volume_EN
• ZXMSG_9000(V1.0.05.R03)_Operation_Guide---9000_Volume_I_EN
• ZXMSG_9000(V1.0.05.R03)_Operation_Guide---9000_Volume_II_EN
• ZXMSG_9000(V1.0.05.R03)_Operation_Guide---9000_Volume_II_EN_1
• ZXMSG_9000(V1.0.05.R03)_Operation_Guide---9000_Volume_III_EN
NetNumen U31 R30 Guidance
• NetNumen U31 R30 (V12.11.40) SS1b General Operation Guide(Security Management Volume)
• NetNumen U31 R30 (V12.11.40) SS1b General Operation Guide
• NetNumen U31 R30 (V12.11.40) SS1b Network Element Management Command Manual
• NetNumen U31 R30 (V12.11.40) SS1b Product Description
• NetNumen U31 R30 (V12.11.40) SS1b Routine Maintenance Guide
NMSI Guidance
• NetNumen U31 R30 Accouting IMP Commissioning Guide

1.3.2 Logical scope

The logical scope of the TOE is described in *Figure 3*.

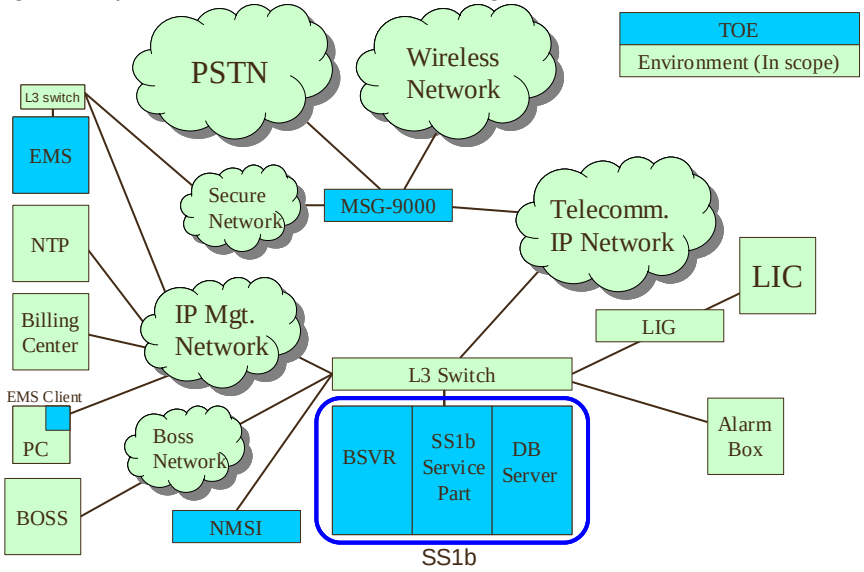


Figure 3: The TOE Scope

The functionalities and threats that are assessed are therefore related to:

Secure management of the TOE, to ensure that only properly authorized staff can manage the TOE (except for lawful interception, BOSS, and billing functionality).

There is one way to manage the TOE:

- Through the EMS Client: This allows full access to management functionality except for lawful interception[3], BOSS, and billing 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 EMS and SS1B, NMSI and SS1B, and EMS and EMS client against disclosure, undetected modification and masquerading

Provides secure management of SS1b user profile data, to ensure only properly authenticated external entities can access SS1b user profile data.

The BOSS interface NMSI provides username/password authentication, to prevent unauthenticated users to access and modify SS1b user profile data.

Provides secure access of billing data, to ensure only properly authenticated external entities can access billing data.

The BSVR provides external entities authentication based on username and password, to prevent unauthenticated external entities to access billing data.

Provides secure interaction between itself and the Billing Center and itself and the BOSS so that data cannot be read or modified in between

The TOE shall protect communication between

- Billing center and the BSVR
- BOSS and the NMSI

against disclosure, undetected modification and masquerading

Provides secure interaction between itself and NTP, so that the time provided by NTP can be trusted

[3] Users can use EMS client to manage lawful interception configuration of SS, such as enable/disable LI functionality, LI protocol, and connection to the LIG. But they cannot setup lawful interception

The TOE shall protect the communication between NTP and the TOE against undetected modification and masquerading.

1.3.3 Roles and external entities

See section 5.2.

1.4 Excluded from evaluation

The SS1b is always supplied with McAfee VirusScan 8.5, Norton Anti-virus or Trend anti-virus[4]. The anti-virus is manually updated periodically[5] by maintenance personnel and is excluded in the evaluation. The SS1b provides its own CLI and GUI interface, but they are all not part of standard TOE configuration and therefore excluded from evaluation at all during the evaluation and are not allowed to use.

[4] Most of the time the McAffee VirusScan 8.5 is supplied. Only in some special cases, such as request from customers, will the Norton Anti-virus or Trend anti-virus be supplied.
[5] It is required to update the virus definition every month

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 conformant
- 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.

3 Security Problem Definition

3.1 Organisational Security Policies

OSP.USERS

The TOE must:

- authenticate Billing Centers, allowing them access the SS1b billing data
- authenticate BOSSes, allowing them to set-up and configure the SS1b provisioning functionality.
- authenticate EMS users, log their activities, and allow them to set-up and configure the TOE functionality (except for provisioning functionality)

OSP.COMMUNICATION

- The customer must provide secure network to protect the communication between the EMS and the MSG-9000 and between MSG-9000 and SS1b
- The communication between the TOE and LIG and LIC must be protected against masquerading, disclosure, and modification

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 configuration functionality[6]
- The confidentiality and integrity of the communication between the TOE parts:
  - EMS and EMS client
  - EMS and SS1b
  - NMSI and SS1b
- The confidentiality and integrity of the communication between the TOE and:
  - Billing Center
  - BOSS
- The integrity of the communication between the TOE and NTP

These assets are threatened by the following threat agents:

1. TA.ROGUE_USER An EMS, BSVR, or BOSS user seeking to act outside his/her authorization. There are three types:

[6] Such as configure the IP address of LIG and LI protocol, but not setup which number is intercepted

- TA_ROGUE_USER_EMS: which has legitimate access to the EMS Client, but not to the BSVR or NMSI
- TA_ROGUE_USER_BSVR: which has legitimate access to the BSVR, but not to the EMS or NMSI
- TA_ROUGE_USER_BOSS: which has legitimate access to NMSI, but not to EMS or BSVR

2. TA.NETWORK An attacker with IP-access to the IP-management networks that the TOE is part of.
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 performs actions on the TOE that he is not authorized to do.

T.AUTHORISED

TA.ROGUE_USER performs actions on the TOE that he is authorized to do, but these are undesirable[7] and it cannot be shown that this user was responsible.

T.UNKNOWN_ USER

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

T. NETWORK

TA.NETWORK is able to:

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

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

T.PHYSICAL_ATTACK

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

3.3 Assumptions

This Security Target uses one assumption:

A.TRUSTED_SYSTEMS

It is assumed that the LIG, Billing Center, and BOSS are trusted, and will not be used to attack the TOE. It is assumed that no attacks on the TOE will emanate from the PSTN, the Wireless Network, or IP telecommunication network[8].

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

[8] We assumed that attacks such as malicious VoIP will be filtered by other telecommunication equipments like access gateways or session boarder controller (SBC).

4 Security Objectives

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 section 7.1 of this Security Target.

4.1 Security objectives for the TOE

O. AUTHENTICATE_EMS

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

O. AUTHORISE_EMS

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

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

Rights include:

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

O.AUDITING_EMS

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

O. AUTHENTICATE_BSVR

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

O.AUTHENTICATE_BOSS

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

O.SEPARATE_USERS

The TOE shall:

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

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

O.PROTECT_COMMUNICATION

The TOE shall:

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

4.2 Security objectives for the Operational Environment

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

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

OE.CLIENT_SECURITY
The customer shall ensure that workstations that host one of the Clients are protected from physical and logical attacks that would allow attackers to subsequently:

- Disclose passwords or other sensitive information
- Hijack the client
- Execute man-in-the-middle attacks between client and EMS or similar attacks.

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

OE.PROTECT_COMMUNICATION
The customer shall provide secure connection to

- protect communication between MSG-9000 and EMS
- protect communication between MSG-9000 and SS1b

OE.VLAN
The customer shall provide the following networks:

- IP management network
- BOSS network

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

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

5 Security Requirements

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:

Subjects and external entities
EMS related roles

- EMS Administrator: a role with unrestricted access rights over all resources, including right to modify critical information of accounts.
- EMS Maintenance: a role with high access rights, but only to resources assigned to him.
- EMS Operator: a role with limited access rights, but only to resources assigned to him.
- EMS Supervisor: a role with only viewing rights, but only to resources assigned to him
- EMS Customized roles: these roles can be defined in the TOE by the Administrator (or by a configurable role who has the right to create roles) and have customizable rights.

Billing related roles and external entity

Billing user	Users at Billing center who can login BSVR to get CDRs
Billing Center	See *Figure 3*

BOSS related roles and external entity

BOSS	See *Figure 3*

Note that BOSS itself does not have user interface. The operator shall provide its own user interface for its user to perform management actions. The username/password used for BOSS to connect to NMSI is different from the username/password used for users to login the operator-provided user interface.

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:

Resource: The softswitch ZXSS10 SS1b and the media gateway MSG-9000

Operations

Operations in the TOE are divided into

- Topology Management
- Fault Management
- Performance Management
- Configuration Management
- Maintenance Management
- Security Management

A more detailed overview of operations may be found in Appendix A. A full list of operations is outside the scope of this ST, and can be found in the TOE Guidance.

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 indicating by adding three letters to the component name.

5.3 Security Functional Requirements

The SFRs have been divided into five major groups:

- Identification & Authentication
- Roles & Authorisation
- Logging & Auditing
- Communication
- Management

5.3.1 Identification & Authentication

FIA_UID.2.EMS User identification before any action

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

- ***by username (in all cases), and***
- ***by IP-address (if so configured for that user)***
- ***by MAC-address (if so configured for that user)***

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_UID.2.BOS User identification before any action

FIA_UID.2.1 The ***NMSI*** shall require each ***BOSS*** to be successfully identified

- ***by username***

before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.2.BIL User identification before any action

FIA_UID.2.1 The ***BSVR*** shall require each ***Billing Center*** to be successfully identified

- ***by username***

before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2.EMS User authentication before any action

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

FIA_UAU.2.BOS User authentication before any action

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

FIA_UAU.2.BIL User authentication before any action

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

FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The ***EMS*** shall terminate an ***EMS*** interactive session

- ***when[9] the allowed work time (if so configured for that user) expires, or***
- ***when one of the user roles is being locked while he is logged in.***

FIA_AFL.1 Authentication failure handling

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

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the ***EMS*** shall **lock the EMS-user account[10]**

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

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that ***EMS 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[11], the username in reverse[12] 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 or more passwords when changed**

[9] The sentence was refined to make it more readable.
[10] Unless this account has been set to unlockable.
[11] If the username is chang, “changchang” is not allowed.
[12] If the username is chang, “gnahc” is not allowed

FTA_MCS.1 Basic limitation on multiple concurrent sessions

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

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of **1** sessions per ***user and no more than 200 sessions for all users together.***

5.3.2 Roles & Authorisation

FMT_SMR.1 Security roles

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

- **Administrator**
- **Maintenance**
- **Operator**
- **Supervisor**
- **customized roles.**

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

FDP_ACC.2 Complete access control

FDP_ACC.2.1 The ***EMS*** shall enforce the **Role Policy** on **all roles and resources** and all operations among ***roles*** and ***resources and the TOE*****.**

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

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The ***EMS*** shall enforce the **Role Policy** to objects based on the following: **all roles, all resources**[13].

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

- **for the roles Administrator, Maintenance, Operator and Supervisor, as defined in Appendix A**[14]
- **for the customized roles, as defined by their customization**[15]
- **the Administrator and appropriately customized roles can perform the functions in FMT_SMF.1**[16]
- **if a user has multiple roles, it is sufficient if only one role is allowed to do the operation**
- **while a role is locked no user has this role**

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:

- **BOSS cannot perform Billing and EMS actions**
- **Billing users cannot perform BOSS and EMS actions**

[13] The attributes have been refined away as there are no relevant attributes.
[14] These pre-defined roles are local to the EMS only
[15] Roles that can perform operations on SS1b or MSG-9000 are all customized roles
[16] Note that these are also among the functions defined in Appendix A, but the list at FMT_SMF.1 is in more detail as it is more relevant to the security of the TOE.

- **EMS users cannot perform Billing and BOSS actions**

5.3.3 Logging & Auditing

The TOE maintains 3 separate logs:

- A security log for authentication events
- An operation log for operations performed by users
- A system log for EMS server tasks that are not directly related to users performing operations

FAU_GEN.3.EMS Simplified audit data generation

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

In the security log:

- **authentication success/failure**
- **EMS user account is locked**
- **EMS user account is unlocked**
- **EMS user account is enabled**
- **EMS user account is disabled**

FAU_GEN.3.2 The ***EMS*** shall record within each ***security*** audit record at least the following information:

- Date and time of the event
- **EMS user name**
- **Type of event**
- **Host address**
- **Operation time**
- **login details**

FAU_SAR.1 Audit review

FAU_SAR.1.1 The ***EMS*** shall provide **Administrator and suitably customized roles** with the capability to read **security log** from the audit records.

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

FAU_STG.1 Protected audit trail storage

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

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

FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The ***EMS*** shall **overwrite the oldest stored audit records**[17] if the audit trail is full.

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

5.3.4 Communication

FDP_ITT.1.EMS Basic internal transfer protection
FDP_ITT.1.1 The TSF shall[18] prevent the **disclosure or modification** of **all** data when it is transmitted between the **EMS Client and the EMS Server**.

FDP_ITT.1.SS Basic internal transfer protection
FDP_ITT.1.1 The TSF shall[19] prevent the **disclosure or modification** of **all** data when it is transmitted between the **EMS and the SS1b**.

FDP_ITT.1.NMSI Basic internal transfer protection
FDP_ITT.1.1 The TSF shall[20] prevent the **disclosure or modification** of **all** data when it is transmitted between the **NMSI and the SS1b**.

FTP_ITC.1.BOS Inter-TSF trusted channel
FTP_ITC.1.1 The ***NMSI*** shall provide a communication channel between itself and ***BOSS*** 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 ***NMSI*** shall permit the ***NMSI and the BOSS*** to initiate communication via the trusted channel.
FTP_ITC.1.3 ***(refined away)***[21]

FTP_ITC.1.BIL Inter-TSF trusted channel
FTP_ITC.1.1 The ***BSVR*** shall provide a communication channel between itself and ***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 ***BSVR*** shall permit the ***BSVR and the Billing Center*** to initiate communication via the trusted channel.
FTP_ITC.1.3 ***(refined away)***[22]

FTP_ITC.1.NTP Inter-TSF trusted channel
FTP_ITC.1.1 The TSF shall provide a communication channel between itself and ***NTP server with MD5 authentication*** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the communicated

[18] Reference to policy refined away since the policy would simply restate the requirement
[19] Reference to policy refined away since the policy would simply restate the requirement
[20] Reference to policy refined away since the policy would simply restate the requirement
[21] NMSI does not initiate communication
[22] BSVR does not initiate communication

data from modification or disclosure.
FTP_ITC.1.2 The TSF shall permit **the TSF** to initiate communication via the trusted channel.
FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **time synchronization**.

5.3.5 Management

FMT_SMF.1 Specification of Management Functions

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

Management function	Related to SFR[23]
Set whether an EMS user can only login from certain IP-addresses, and if so, which IP addresses	FIA_UID.2.EMS
Set whether an EMS user can only login from certain MAC-addresses, and if so, which MAC-addresses	FIA_UID.2.EMS
Set whether an EMS user can only login at certain times, and if so, at which times	FIA_UID.2.EMS
Set the time that an EMS user may remain logged in while inactive	FTA_SSL.3
Set whether an EMS user is only allowed to work at certain times, and if so, at which times	FTA_SSL.3
Set the number of allowed unsuccessful authentication attempts for EMS	FIA_AFL.1
Set the number of hours that an EMS account remains locked	FIA_AFL.1
Set whether an EMS user account should be: o unlockable, or o locked (either permanently or temporarily) when it exceeds the number of allowed consecutive unsuccessful authentication attempts	FIA_AFL.1
Unlock an EMS user account	FIA_AFL.1
Set whether an EMS user password expires after a certain time, and if so, after how long	FIA_SOS.1
Set whether the new password of an EMS user must be different from the last n passwords when the password is changed by the user and configure n	FIA_SOS.1
Set the maximum number of concurrent sessions for the same user	FTA_MCS.1
Create, edit and delete customized roles	FMT_SMR.1
Add or remove roles to/from users	FMT_SMR.1
Add or delete types of events to be logged in the security log	FAU_GEN.3.1
Create, edit and delete user accounts	-
Disable/enable[24] user accounts	-

[23] This column of the table is for reference only, and is not part of the SFR.

Lock/unlock[25] roles	-

[24] The effect is the same as locking of an EMS user account, but disabling is actively done by the administrator, while locking an EMS user account is done by failing to authenticate too many times.

[25] Locking and unlocking roles is done by the administrator. The effect is that any EMS user with that role loses all access rights provided by that role, unless he has those rights also by a non-locked role.

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:

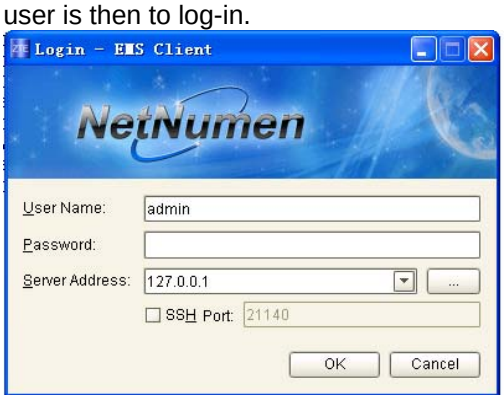
- EAL 2 is deemed to provide a good balance between assurance and costs and is in line with ZTE customer requirements.
- ALC_FLR.2 provides assurance that ZTE has a clear and functioning process of accepting security flaws from users and updating the TOE when required. This is also in line with ZTE customer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

6 TOE Summary Specification

Secure management of the TOE, to ensure that only properly authorized staff can manage the TOE (except for lawful interception, BOSS, and billing functionality).

FIA_UID.2.EMS, FIA_UAU.2.EMS, FIA_AFL.1

Whenever an EMS user of the TOE wishes to use the EMS to manage the TOE, the user needs to use the EMS client of the TOE. The first action required by the user is then to log-in.



The TOE allows the appropriate administrator to configure (for each EMS 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 EMS will log an EMS 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 EMS 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 EMS 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.

FDP_ITT.1.EMS
The communication between the EMS and the EMS client is protected by SSH and SFTP

FDP_ITT.1.SS
The communication between the EMS and SS1b is protected by SSH and SFTP

FDP_ITT.1.NMSI
The communication between the SS1b and the NMSI is protected by SSH and SFTP

Provides secure management of SS1b user profile data, to ensure only properly authenticated external entities can access SS1b user profile data.

FIA_UID.2.BOS and FIA_UAU.2.BOS
Whenever a BOSS wishes to manage the user profile, the BOSS need to identify and authenticate itself to the NMSI.

Provides secure access of billing data, to ensure only properly authenticated external entities can access billing data.

FIA_UID.2.BIL and FIA_UAU.2.BIL
Whenever a billing server wishes to fetch the CDR from the BSVR, the billing server need to identify and authenticate itself to the BSVR.

Provides secure interaction between itself and the Billing Center and itself and the BOSS so that data cannot be read or modified in between

FTP_ITC.1.BIL

The communication between the billing center and the BSVR is protected by sftp.

FTP_ITC.1.BOS
The communication between the BOSS and the NMSI is protected by SSH

Provides secure interaction between itself and NTP, so that the time provided by NTP can be trusted

FTP_ITC.1.NTP
The communication between the TOE and the NTP is protected by MD5 authentication.

7 Rationales

7.1 Security Objectives Rationale

Assumptions/OSPs/Threats	Objectives
OSP.USERS The TOE must: o authenticate Billing centers, allowing them access SS1b billing data o authenticate BOSS users, allowing them to set-up and configure the SS1b provisioning functionality o authenticate EMS users, log their activities, and allow them to set-up and configure the TOE functionality (except for provisioning functionality)	This OSP is primarily implemented by: • O.AUTHENTICATE_BSVR restate the first bullet • O.AUTHENTICATE_BOSS restate the second bullet • the combination of O.*_EMS, 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.
OSP.COMMUNICATION o The customer must provide secure network to protect the communication between the EMS and the MSG-9000 and between MSG-9000 and SS1b. o The communication between the TOE and LIG and LIC must be protected against masquerading, disclosure, and modification.	This OSP is primarily implemented by • OE.COMMUNICATION which states that the communication between the EMS and the SS1b shall be protected by secure network. • OE_PROTECTED_LINE_LIC which restates the second bullet
T.UNAUTHORISED 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 (EMS). • O.SEPARATE_USERS that ensures that users without rights for certain functionality groups cannot access that functionality. So the only way that a user can perform a management action for a functionality is when he has a role for that

	functionality, 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_EMS 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 use its functionality.	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 TOE Together these two security objectives counter the threat.
T. NETWORK TA.NETWORK is able to: • Modify/read network traffic originating from / destined for the TOE or • Modify/read network traffic between TOE subsystems • Impersonate the TOE and thereby perform management actions on other entities on the network or gain unauthorized knowledge about the TOE traffic.	This threat is countered by O.PROTECT_COMMUNICATION that protects traffic between: o EMS and EMS client o EMS and SS1b o NMSI and SS1b o BSVR and the Billing Center o NMSI and the BOSS o NTP and EMS OE.PROTECTED_COMMUNICATION that protects traffic between o EMS and MSG-9000 o SS1b and MSG-9000 and OE_PROTECTED_LIE_LIC that protects traffic between o SS1b and LIG and LIC and OE_VLAN prevents unauthorized management knowledge about the TOE traffic leak from the BOSS network. Therefore 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 TOE 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.
A.TRUSTED_SYSTEMS It is assumed that the LIG, Billing Center, and BOSS	This assumption is upheld by the objective OE.TRUSTED_SYSTEMS which restates the assumption.

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

7.2 Security Functional Requirements Rationale

Security objectives	SFRs addressing the security objectives
O. AUTHENTICATE_EMS The TOE shall support EMS Client user authentication, allowing the TOE to accept/reject EMS users based on username and password.	This objective is met by: • FIA_UID.2.EMS stating that identification will be done by username, but also IP-address, MAC-address, and login time • FIA_UAU.2.EMS stating that the users must be authenticated • FIA_SOS.1 stating that passwords must have a minimum quality • FIA_AFL.1 stating what happens when authentication fails repeatedly • FTA_SSL.3 logging users off when they are no longer allowed to work or when their role is locked • FMT_SMF.1 configuring all of the above. Together, these SFRs meet the objective in a flexible and configurable manner.
O. AUTHENTICATE_BSVR The TOE shall support billing server authentication, allowing the TOE to accept/reject billing server based on username and password.	This objective is met by: • FIA_UID.2.BIL stating that identification will be done by username • FIA_UAU.2.BIL stating that the billing server must be authenticated Together, these SFRs meet the objective.
O.AUTHENTICATE_BOSS The TOE shall support BOSS authentication, allowing the TOE to accept/reject BOSS based on username and password.	This objective is met by: • FIA_UID.2.BOS stating that identification will be done by username • FIA_UAU.2.BOS stating that the BOSS must be authenticated Together, these SFRs meet the objective.
O. AUTHORISE_EMS The TOE shall support at least two roles on the EMS Client: o EMS administrator with all rights o EMS operator with limited rights Rights include:	This objective is met by: ▢ FMT_SMR.1 stating the predefined and customizable roles. ▢ FDP_ACC.2 and FDP_ACF.1 defining a Role Policy, which states how the two

Security objectives	SFRs addressing the security objectives
o the ability to perform various management related actions o the ability to manage (create, modify rights, delete) other OMM users	roles manage the TOE. ▢ FMT_SMF.1 configuring all of the above. Together, these SFRs support a flexible authorization framework.
O.SEPARATE_USERS The TOE shall: o prohibit EMS users from accessing billing and BOSS related data and functionality o prohibit BSVR users from accessing EMS and BOSS related data and functionality o prohibit BOSS users from accessing EMS and billing 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.
O.AUDITING_EMS The TOE shall support logging and auditing of EMS user actions.	This objective is met by: • FAU_GEN.3 showing which events are logged in the security and system logs • FAU_SAR.1 showing that the logged events can be audited and by whom • FAU_STG.1 showing how the audit logs are protected • FAU_STG.4 stating what happens when the audit log becomes full • FMT_SMF.1 configuring all of the above Together, these SFRs support a flexible logging and auditing framework.
O.PROTECT_COMMUNICATION The TOE shall: • protect communication between the TOE and the BOSS against masquerading, disclosure and modification • protect communication between the TOE and the Billing Center against masquerading, disclosure and modification • protect communication between the Clients and the EMS against disclosure and modification • protect communication between the SS1b and the EMS against disclosure and modification • protect communication between the SS1b and the NMSI against disclosure and modification • protect communication between the SS1b and	This objective is met by: • FTP_ITC.1.BOS restating the first bullet • FTP_ITC.1.BIL restating the second bullet • FDP_ITT.1.EMS restating the third bullet • FDP_ITT.1.SS restating the fourth bullet • FDP_ITT.1.NMSI restating the fifth bullet • FTP_ITC.1.NTP restating the sixth bullet

Security objectives	SFRs addressing the security objectives
the NTP against masquerading and modification	

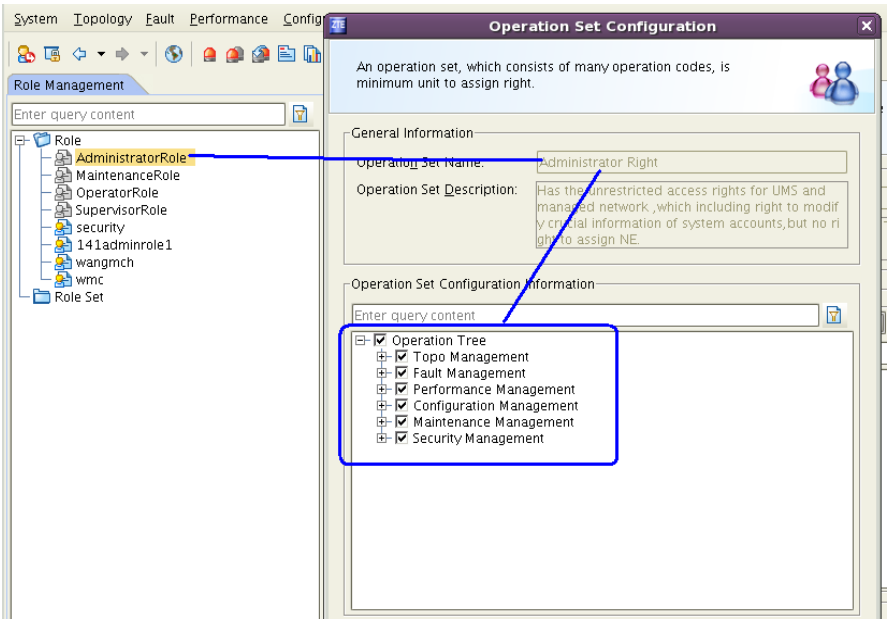
7.3 Dependencies

SFR	Dependencies
FIA_UID.2.EMS	-
FIA_UID.2.BOS	-
FIA_UID.2.BIL	-
FIA_UAU.2.EMS	FIA_UID.1: met by FIA_UID.2.EMS
FIA_UAU.2.BOS	FIA_UID.1: met by FIA_UID.2.BOS
FTA_SSL.3	-
FIA_AFL.1	FIA_UAU.1: met by FIA_UAU.2.EMS
FIA_SOS.1	-
FTA_MCS.1	FIA_UID.1: met by FIA_UID.2.EMS
FMT_SMR.1	FIA_UID.1: met by FIA_UID.2.EMS
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.
FAU_GEN.3	FPT_STM.1: met in environment by OE.TIME
FAU_SAR.1	FAU_GEN.1: met by FAU_GEN.3, which is similar enough to FAU_GEN.1 to meet the dependency
FAU_STG.1	FAU_GEN.1: met by FAU_GEN.3, which is similar enough to FAU_GEN.1 to meet the dependency
FAU_STG.4	FAU_GEN.1: met by FAU_GEN.3, which is similar enough to FAU_GEN.1 to meet the dependency
FDP_ITT.1.EMS	FDP_ACC.1 or FDP_IFC.1: not met, since the policy was refined away the dependency is unnecessary
FDP_ITT.1.SS	FDP_ACC.1 or FDP_IFC.1: not met, since the policy was refined away the dependency is unnecessary
FDP_ITT.1.NMSI	FDP_ACC.1 or FDP_IFC.1: not met, since the policy was refined away the dependency is unnecessary
FTP_ITC.1.BOS	-
FTP_ITC.1.BIL	-
FMT_SMF.1	-
SAR	**Dependencies**
EAL 2	All dependencies within an EAL are satisfied
ALC_FLR.2	-

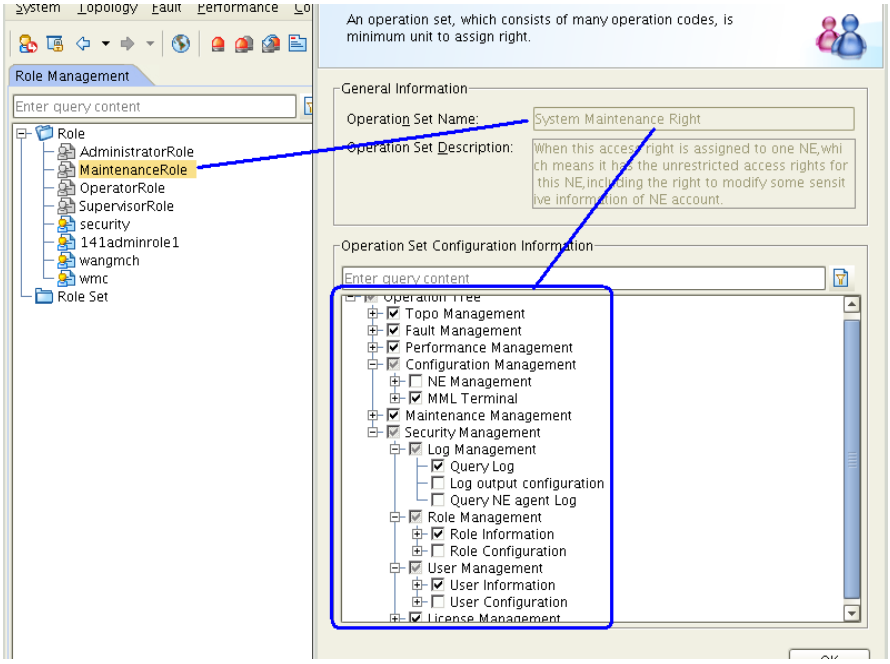
A Roles and Operations

This Appendix provides a graphical overview of which roles can do what operations for the various roles

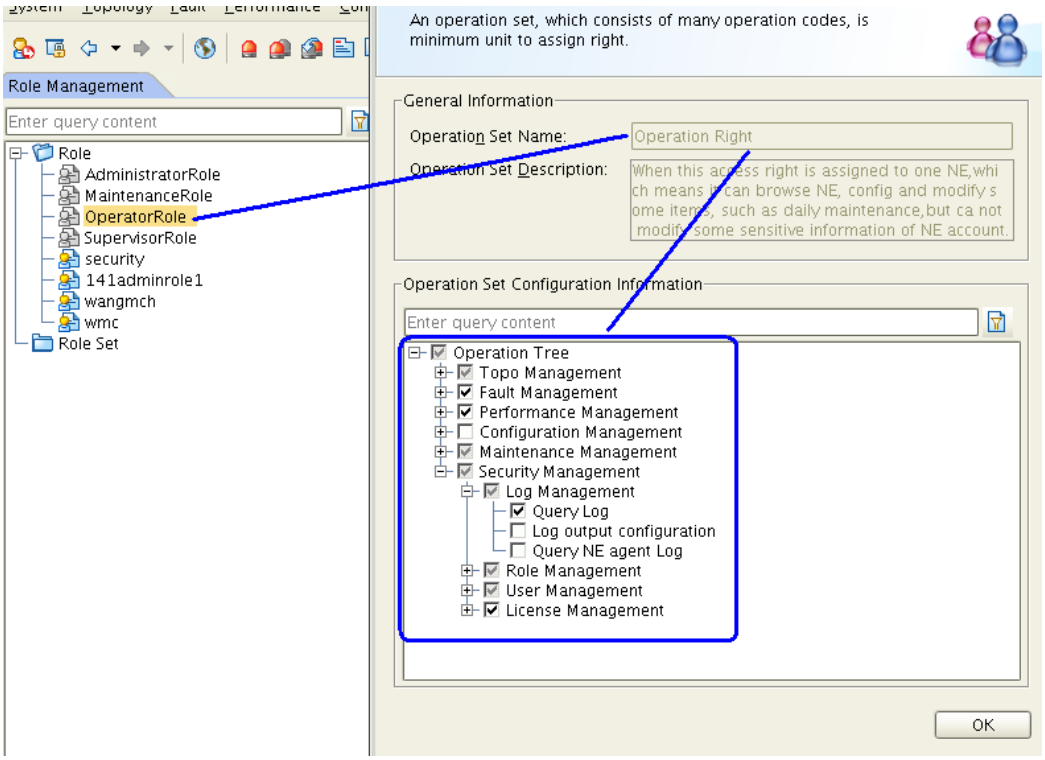
A.1 Administrator



A.2 Maintenance



A.3 Operator



A.4 Supervisor