ZTE Base Station Controllers

Security Target

Version 1.0

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

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

Revision No.	Revision Date	Revision Reason
0.1	01 Jan 2012	First version
0.2	09 Jan 2012	Fix typo in appendix C
0.3	20 Feb 2012	Addressed EOR
1.0	05 May 2012	Final

Serial Number: SJ-20120505101114-019

Publishing Date: 2012-05-05(R1.0)

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

Contents

Chapter 1
ST Introduction

Table of Contents

1.1 ST and TOE References

This is version 1.0 of the Security Target for the ZTE range of Base Station Controllers. These include ZTE ZXG10 iBSC Base Station Controller, V6.20.614, ZXC10 BSCB CDMA2000 Base Station Controller, V8.0.3.400, and ZXWR RNC WCDMA Radio Network Controller, V3.09.30.

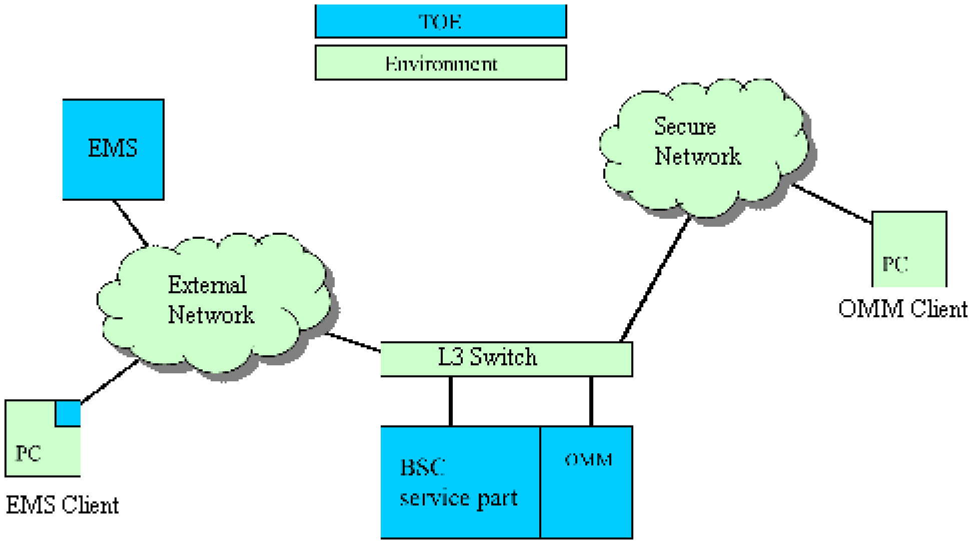
The remainder of this ST will refer to the TOE as BSC.

1.2 TOE Overview and usage

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

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

Figure 1-1 The TOE



- A BSC, consisting of:
  - → A BSC Service Part, responsible for performing the telecommunication services
  - → An OMM (Operation & Maintenance Module) responsible for management and maintenance of the BSC
- An OMM Client that allows operators' access to the OMM
- An EMS Client, consisting of a Java application. This application is intended to run on a workstation. This client is a graphical user interface to the EMS Server.
- An EMS Server, consisting of a server plus software.

The OMM Client, a graphical user interface to the OMM, is not part of the TOE. This interface is only used in emergency cases and during pre-installation by ZTE.

These are connected by two networks:

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

For a more detailed explanation on iBSC, please refer to Appendix **A**. For a more detailed explanation on RNC, please refer to Appendix **B**. For a more detailed explanation on BSCB, please refer to Appendix **C**.

1.2.1 *Major security features*

The TOE:

- Provides secure management of itself, to ensure that only properly authorized staff can manage the TOE.

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 Client requires:

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

ZXG10 iBSC

Type	Name and version
Hardware	BIPI (for Access Unit) GLI (for Switch Unit) GUP (for Process Unit) OMP(for O&M Unit) PWRD(for Peripheral Monitoring Unit) SBCX (for the OMM)
Software	ZXG10 iBSC (V6.20.614) OMM V6.20.614
Software	OMM Client V6.20.614

ZXWR RNC

Type	Name and version
Hardware	GIPI, EIPI(for Access Unit) GLI (for Switch Unit) RUB, RCB (for Process Unit) OMP(for O&M Unit) PWRD(for Peripheral Monitoring Unit) SBCX (for the OMM)
Software	ZXWR RNC (V3.09.30) OMM V3.09.30
Software	OMM Client V3.09.30

ZXC10 BSCB

Type	Name and version
Hardware	ABES/ABPM(for Access Unit) CHUB/THUB (for control plane switching Unit) CLKD/CLKG(for clock driver/generator unit) GCM(for GPS unit) DTB/SDTB(for TDM Interface Unit) GLIQV/GLI(Line Interface Board) IBBE(for BSC-Inter-Connect Unit) ICM (Integrated clock Module) INLP/ SPB (Signaling processing and E1/T1 interface Unit)

Type	Name and version
	SIPI/IPI (for IP Signaling/Bearer Interface) IWFB (for IWF Unit) MP (for Processing Unit) OMP (for O&M Unit) PSN (for Packet Switch Network Unit) PWRD (for Power Unit) SDU (for Select/Distribute Unit) UIM/GUIM(for Switch Unit) UPDC /UPCF/ IPCF (for PCF & PTT) VTCD (for Voice Transcode Unit)
Software	ZXC10 BSCB (V8.0.3.400)OMM V3.08.34.00
Software	OMM Client V3.08.34.00

There are 4 basic hardware configurations[1] for the EMS Server

- 2 AIX/IBM configurations called Mode IBM-1 and Mode IBM-2
- 2 Solaris/Sun configurations called Mode Sun-1 and Sun-2

All modes are functionally identical, but differ in computing power.

	Mode IBM-1	Mode IBM-2	Mode Sun-1	Mode Sun-2
Platform	IBM P740 CPU 2*2Core 32GB Memory 2*146GB SAS Disks Dual-port HBA cards	IBM P740 CPU 4*2Core 64GB Memory 2*146GB SAS Disks Dual-port HBA cards	Sun M4000 2*4 Core CPUs 32GB Memory 2 146G SAS Disks Dual-port HBA cards	Sun M4000 4*4 Core CPUs 64GB Memory 2 146G SAS Disks Dual-port HBA cards
Disk Array	N6210 8*300G FC15k	N6210 14*300G FC15k	ST6180 8*300G FC15K or EMC CX4-120C 15*300G FC15K	ST6180 16*300G FC15K or EMC CX4-120C 30*300G FC15K

The TOE (EMS Server) contains the following software:

EMS Client	Name and version
Application Software	EMS Client version NetNumen U31 R18 V12.11.40

[1] There are also configurations available that provide the exact same functionality for Dell/Windows and Sun/Solaris, but these have not been evaluated. Similarly, there are also fault-tolerant dual server configurations available, but these also have not been evaluated.

EMS Server (Solaris)	**Name and version**
Application Software	EMS Server version NetNumen U31 R18 V12.11.40
Java	Java(TM) SE Runtime Environment (build 1.6.0_21-b06) Java HotSpot(TM) 64-bit Server VM (build 17.0-b16, mixed mode)
OS	Solaris 10 U9 SPARC
DB	Oracle 11.2.0.2 EE 64 bit for Solaris SPARC
Redundancy[2]	VCS 5.1 and VVR 5.1
Backup&Restore	Veritas NetBackup V7.0

EMS Server (AIX)	**Name and version**
Application Software	EMS Server version NetNumen U31 R18 V12.11.40
Java	Java(TM) SE Runtime Environment (build pap6460sr8fp1-20100624_01(SR8 FP1)) IBM J9 VM (build 2.4, JRE 1.6.0 IBM J9 2.4 AIX ppc64-64 jvmap6460sr8ifx-20100609_59383 (JIT enabled, AOT enabled) J9VM - 20100609_059383 JIT - r9_20100401_15339ifx2 GC - 20100308_AA) JCL - 20100624_01
OS	AIX 6100-03-06-1034
DB	Oracle 11.2.0.2 EE 64bit for AIX
Redundancy[3]	HACMP v6105+SnapMirror
Backup&Restore	IBM TSM V6.2

The TOE is delivered with the following guidance:

EMS R18 (all prefixed with **NetNumenTM U31 (R18 V12.11.40)**)
Standard Guidance: ● NetNumen U31 R18 (V12.11.40) Product Description ● NetNumen U31 R18 (V12.11.40) Maintenance Guide ● NetNumen U31 R18 (V12.11.40) MML Command Reference ● NetNumen U31 R18 (V12.11.40) Security Management Operation Guide ● NetNumen U31 R18 (V12.11.40) Log Management Operation Guide ● NetNumen U31 R18 (V12.11.40) Fault Management Operation Guide ● NetNumen U31 R18 (V12.11.40) Management Operation Guide ● NetNumen U31 R18 (V12.11.40) MML Terminal Operation Guide

[2] Only in Dual-Server or Two-Server

[3] Only in Dual-Server

Maintenance ● NetNumen U31 R18 (V12.11.40) Maintenance Guide

ZXG10 iBSC Base Station Controller, V6.20.614 **(all are R1.0 except where indicated)**
Certified Configuration ● CC Security Evaluation – Certified Configuration
Standard Guidance ● iBSC Product Description ● Base Station Controller Documentation Guide ● Base Station Controller System Description ● Harware Description ● Hardware Installation Guide ● Base Station Controller Routine Maintenance ● Base Station Controller Emergency Maintenance ● Base Station Controller Software Installation Guide ● Feature Configuration Guide ● Data Management Operation Guide ● Base Station Controller Software Version Management Operation Guide ● Diagnosis Test ● MML Command Reference ● Alarm Handling Reference ● Notification Handling Reference ● Parts Replacement Guide ● System Management Operation Guide ● Security Management Operation Guide ● Log Management Operation Guide

ZXWR RNC WCDMA Radio Network Controller, V3.09.30 **(all are R1.0 except where indicated)**
Certified Configuration · CC Security Evaluation – Certified Configuration
Standard Guidance ● Product Description ● Alarm and Notification Handling Reference ● Radio Parameter Reference ● Documentation Guide ● System Description ● Hardware Description ● Hardware Installation Guide ● Trouble Shooting ● Routine Maintenance ● Emergency Maintenance ● Log Service

- MML Command Reference
- OMM Software Installation Guide
- Test Management Operation Guide
- Software Management Operation Guide
- Calling Trace Operation Guide
- Radio Configuration Operation Guide
- Dynamic Data Management Operation Guide
- Configuration Tool Operation Guide
- Hardware Replacement Guide
- Ground Configuration Operation Guide
- Manage Object Model Description
- Specifications and Requirements for IRPS
- System Management Operation Guide
- Security Management Operation Guide
- Log Management Operation Guide

ZXC10 BSCB CDMA2000 Base Station Controller, V8.0.3.400 **(all are R1.0 except where indicated)**

Certified Configuration

- CC Security Evaluation – Certified Configuration

Standard Guidance

- System Documentation Guide
- System Basic Principle
- System Product Overview
- System interface and Protocol Description
- Controller Technical Manual
- Controller Hardware Manual
- Controller installation Manual
- System Cable Preparation Manual
- System DIP Switches and Jumpers Reference Manual
- Controller Routine Maintenance Manual
- Station System Trouble shooting Manual
- System Emergency maintenance Manual
- System Alarm Handling Manual
- System Configuration Parameter (Overview)
- Configuration Parameter Manual(1x Release A)
- Configuration Parameter Manual (DO)
- System Configuration Parameter Manual (A Ap Interface)
- Configuration Parameter Manual_V5 Interface
- Configuration Parameter Manual(Physical Inventory Data)
- Configuration Parameter Manual(Physical Configuration Data)
- System Common Timer Description
- System Command Manual_System Tools
- System Command Manual_Configuration Management

- System Command Manual_Radio Configuration 1X
- System Command Manual_Radio Configuration DO
- System Performance Management Counter Description_1x
- System Performance Management Counter Description_EV-DO
- System Performance Management Counter Description_PTT
- System Call Failure Reason and Call Drop Explanation_1X
- Call Failure Reason and Call Drop Explanation(EV-DO)
- Call Failure Reason and Call Drop Explanation(PTT)
- System Operation Manual(Configuration Management)
- System Operation Manual(System Tools)
- System Operation Manual(Alarm Management)
- System Operation Manual(Common Operations)
- System Commissioning Manual
- Controller Data Configuration Manual_DO
- Controller Data Configuration Manual_PTT
- Controller Data Configuration Manual_V5
- Alarm Box(V5.00)User Manual

1.3.2 Logical scope

The security functionality of the TOE consists of:

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

There are two ways of managing the TOE:

- Through the OMM Client: This allows full access to management functionality. This is not in the scope of the evaluation.
- Through the EMS: This allows similar access as through the OMM Client

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 Client and EMS, EMS and BSC against disclosure, undetected modification and masquerading

1.3.3 Roles And External Entities

See section 5.2.

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 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.

This page intentionally left blank.

Chapter 3
Security Problem Definition

Table of Contents

3.1 Organisational Security Policies

OSP.USERS

The TOE shall authenticate users, ensure they are authorized before allowing them to do activities, log their activities, and allow them to configure the TOE functionality.

3.2 Threats

3.2.1 Assets and threat agents

The assets are:

- The ability to allow various users to use the TOE and/or manage various aspects of the TOE securely
- The confidentiality and integrity of the communication between the BSC and EMS, and EMS client and EMS

These assets are threatened by the following threat agents:

- TA.ROGUE_USER — A user seeking to act outside his/her authorization.
- TA.NETWORK — An attacker with IP-access to the External Network that is connected to the TOE
- 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[4] 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 BSC, EMS and the EMS Client.
- gain unauthorized knowledge about traffic between the BSC and EMS, EMS client and EMS.

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

[4] For example, the user is allowed to add users, but he misuses this to add thousands of users.

Chapter 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.

Table of Contents

4.1 Security objectives for the TOE

O.AUTHENTICATE

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

O.AUTHORISE

The TOE shall support a flexible role-based authorization framework with predefined and customizable roles. These roles can use the Client to manage the TOE. Each role allows a user to perform certain actions, and the TOE shall ensure that users can only perform actions when they have a role that allows this.

O.AUDITING

The TOE shall support logging and auditing of user actions.

O.PROTECT_COMMUNICATION

The TOE shall protect communication between:

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

4.2 Security objectives for the Operational Environment

OE.CLIENT_SECURITY

The operator shall ensure that workstations hosting one of the Clients are protected from physical and logical attacks that would allow attackers to subsequently:

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

OE.SERVER_SECURITY

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

OE.PROTECT_COMMUNICATION

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

OE.TIME

The NTP Server shall supply the TOE with reliable time.

OE.TRUST&TRAIN_USERS

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

OE.TRUSTED_SYSTEMS

The operator shall ensure that:

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

Chapter 5
Security Requirements

Table of Contents

5.1 Extended components definition

There are no extended components.

5.2 Definitions

The following terms are used in the security requirements:

Roles

- Administrator: a role with unrestricted access rights over all resources, including right to modify critical information of accounts.
- Maintenance: a role with high access rights, but only to resources assigned to him
- Operator: a role with limited access rights, but only to resources assigned to him.
- Supervisor: a role with only viewing rights, but only to resources assigned to him
- 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.

External entities:

- OMM Client

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.

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

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF 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 EMS user) before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2 User authentication before any action

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

FIA_AFL.1 Authentication failure handling

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

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **lock the EMS user account**[5]

- ***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 ***password*** 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***[6], ***the username in reverse***[7] ***or a common dictionary word***
- ***can be configured to expire after a configurable amount of time < 90 days***
- ***can be configured to be different from the previous 5 or more passwords when changed***

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

[6] If the username is chang, “changchang” is not allowed.

[7] If the username is chang, “gnahc” is not allowed

FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session

- after **a configurable period of inactivity less than 30 minutes**
- ***when*[8]*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***

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 ***user***.

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

FMT_SMR.1.Security roles

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

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

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

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

1. Start-up and shutdown of the audit functions ***(in the system log)***
2. ***(refined away)***

In the security log:

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

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

1. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
2. ***(refined away)***
3. ***(in the system log): task start and end time***

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

4. ***(in the security log): access method, client IP address***
   - **Type of event**
   - **Detailed Information**

FAU_SAR.1 Audit review

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

FAU_SAR.1.2 The TSF 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 TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF 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 TSF shall **overwrite the oldest stored audit records** [9] if the audit trail is full.

FDP_ITT.1.EMS Basic internal transfer protection

FDP_ITT.1.1 The TSF shall[10] prevent the **disclosure or modification** of ***all*** data when it is transmitted between the ***EMS and EMS Client***.

FDP_ITT.1.BSC Basic internal transfer protection

FDP_ITT.1.1 The TSF shall[11] prevent the **disclosure or modification** of ***all*** data when it is transmitted between the ***EMS and BSC***.

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**
Set whether a user can only login from certain IP-addresses, and if so, which IP addresses	**FIA_UID.2**

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

[10] 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.

[11] 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.

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

FDP_ACC.2 Complete access control

FDP_ACC.2.1The TSF shall enforce the **Role Policy** on **all roles and the TOE** and alloperations among ***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, all resources and the TOE**[12].

[12] The attributes have been refined away as there are no relevant attributes.

FDP_ACF.1.2 The TSF 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 the guidance**
- **for the customized roles, as defined by their customization**
- **the Administrator and appropriately customized roles can perform the functions in FMT_SMF.1**[13]
- **if a user has multiple roles, it is sufficient if only one role is allowed to do the operation**
- **if a role is locked no user has this role**

FDP_ACF.1.3, FDP_ACF.1.4 ***(refined away)***.

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

[13] Note that these are also among the functions defined in the guidance, but the list at FMT_SMF.1 is in more detail as it is more relevant to the security of the TOE.

Assurance Class	**Assurance Components**	
	Identifier	**Name**
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 customers' requirements

This page intentionally left blank.

Chapter 6
TOE Summary Specification

Secure management and usage of the TOE, to ensure that only properly authorized staff can manage and/or use 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.

The TOE allows the 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
  - → whether the account is unlocked by the Administrator or unlocks after 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 TOE, 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.1, 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.

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

FDP_ITT.1.EMS

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

FDP_ITT.1.BSC

The connection between the BSC/OMM and the EMS Server is protected by sftp and ssh.

Chapter 7
Rationales

Table of Contents

7.1 Security Objectives Rationale

Assumptions/OSPs/Threats	Objectives
OSP.USERS	This OSP is implemented by: ● O.AUTHENTICATE, which ensures users are authenticated ● O.AUTHORISE, which ensures only authorized users can do actions (including management actions) ● O.AUDITING, which ensures user actions are logged and OE.TIME, which ensures that the audit records have the correct date and time.
T.UNAUTHORISED	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 that only users with certain roles have rights to do certain actions for a certain group of functionality. 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.

Assumptions/OSPs/Threats	Objectives
T.AUTHORISED	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	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 server Together these two security objectives counter the threat
T.NETWORK	This threat is countered by O.PROTECT_COMMUNICATION that protects traffic between: ● The BSC and EMS ● The EMS and the EMS client against masquerading, disclosure and modification and by OE.PROTECT_COMMUNICATION that protects traffic between the TOE and NTP
T.PHYSICAL_ATTACK	This threat is countered by two security objectives: ● OE.SERVER_SECURITY stating that the server 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 objectives counter the entire threat
A.TRUSTED_SYSTEMS	This assumption is upheld by OE.TRUSTED_SYSTEMS, which directly restates the assumption.

7.2 Security Functional Requirements Rationale

Security objectives	SFRs addressing the security objectives
O. AUTHENTICATE	This objective is met by: ● FIA_UID.2 stating that identification will be done by username, IP-address and login time ● FIA_UAU.2 stating that the users must be authenticated ● FIA_SOS.1 stating that passwords must have a minimum quality

Security objectives	SFRs addressing the security objectives
	● 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 ● FTA_MCS.1 limiting the number of logins per user ● FMT_SMF.1 configuring all of the above. Together, these SFRs meet the objective and provide further detail.
O. AUTHORISE	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 various roles manage the TOE. ● FMT_SMF.1 configuring all of the above. Together, these SFRs support a flexible authorization framework.
O.AUDITING	This objective is met by: ● FAU_GEN.1 showing which events are logged ● 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	This objective is met by FDP_ITT.1.EMS for the protection of communication between EMS Client and EMS, and with FDP_ITT.1.BSC, for the protection of communication between BSC and EMS

7.3 Dependencies

SFR	Dependencies
FIA_UID.2	-
FIA_UAU.2	FIA_UID.1: met by FIA_UID.2
FIA_AFL.1	FIA_UAU.1: met by FIA_UAU.2
FIA_SOS.1	-
FTA_SSL.3	-

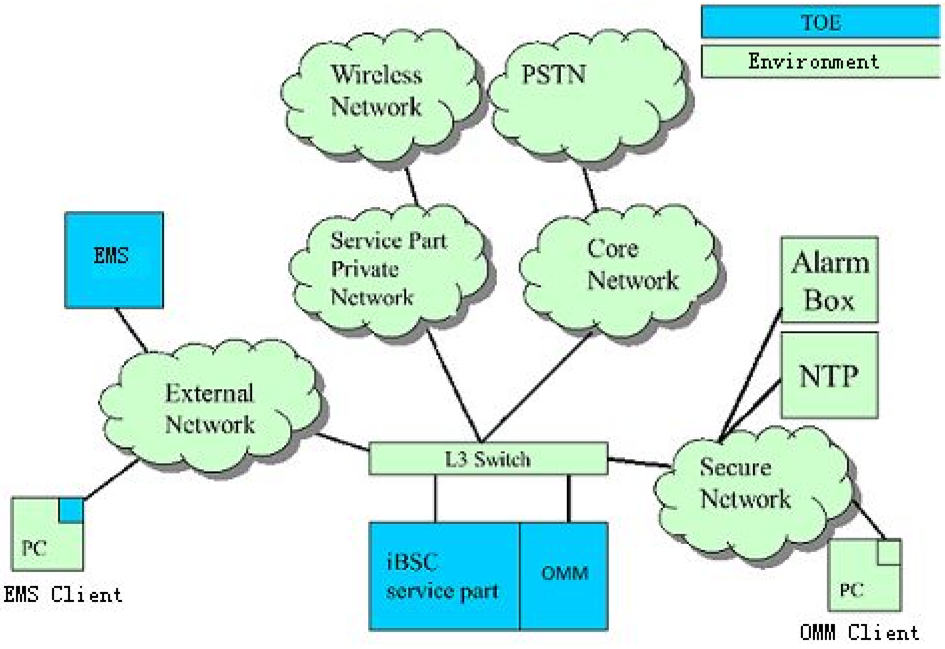
SFR	Dependencies
FTA_MCS.1	FIA_UID.1: met by FIA_UID.2
FMT_SMR.1	FIA_UID.1: met by FIA_UID.2
FAU_GEN.1	FPT_STM.1: met in environment by OE.TIME
FAU_SAR.1	FAU_GEN.1: met by FAU_GEN.3, which is similar enough to FAU_GEN.1 to meet the dependency
FAU_STG.1	FAU_GEN.1: met by FAU_GEN.3, which is similar enough 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
FPT_SMF.1	-
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.BSC	FDP_ACC.1 or FDP_IFC.1: not met, since the policy was refined away the dependency is unnecessary
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	-

Appendix A
iBSC

The iBSC is the base station controller part of the second generation mobile cell communication system and is thereforeconnected to a wide variety of other systems and networks, as shown in Figure A-1.

Figure A-1 The TOE in its envrionment



The additional[14] systems and network are

- The OMM Client, a graphical user interface to the OMM, is not part of the TOE. This interface is only used in emergency cases and during pre-installation by ZTE.
- 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 atrusted 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

[14] Additional to those described earlier.

- 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 consists of mobile phones and similar equipment that uses GSM and/or UMTS. It is considered a trusted network in this evaluation.
- The Core Network: It is divided to CS domain and PS domain. It is the control center of the mobile core network ,and the gateway of the mobile network and internet. It is considered a trusted network in this evaluation.

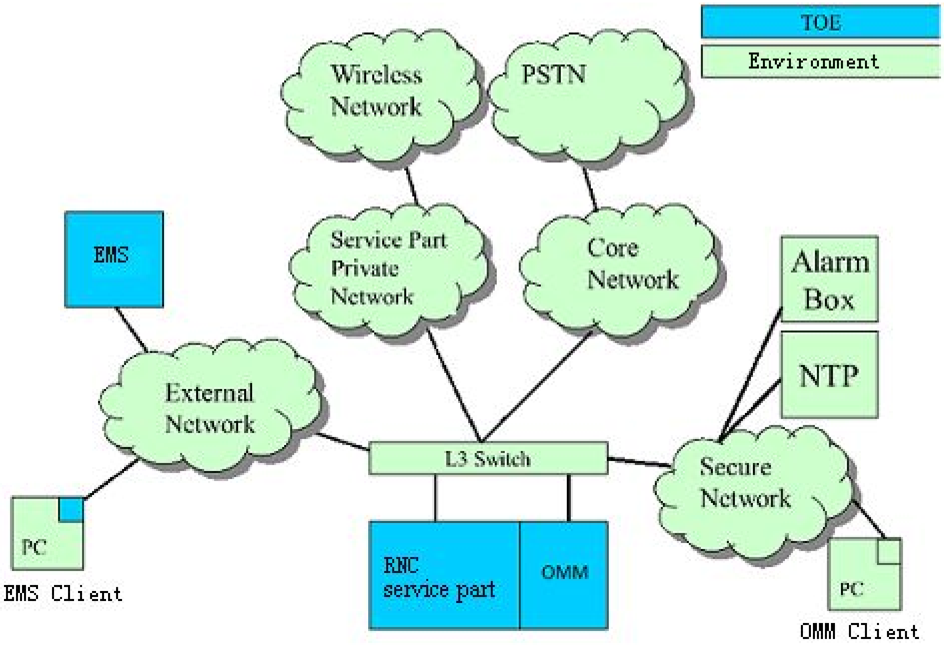
The iBSC has the following general functionalities:

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

Appendix B
RNC

The RNC is the radio access network controller part of the WCDMA system and is therefore connected to a wide variety of other systems and networks, as shown in Figure B-1.

Figure B-1 The TOE in its environment



The additional[15]systems and network are

- The OMM Client, a graphical user interface to the OMM, is not part of the TOE. This interface is only used in emergency cases and during pre-installation by ZTE
- 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 atrusted 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.

[15] Additional to those described earlier.

- The Wireless Network: This consists of NodeB and UE(User Equipment), which consists of mobile phones and similar equipment that uses WCDMA. Itis considered a trusted network in this evaluation.
- The Core Network: It is divided to CS domain and PS domain. It is the control center of the mobile core network ,and the gateway of the mobile network and internet. It is considered a trusted network in this evaluation.

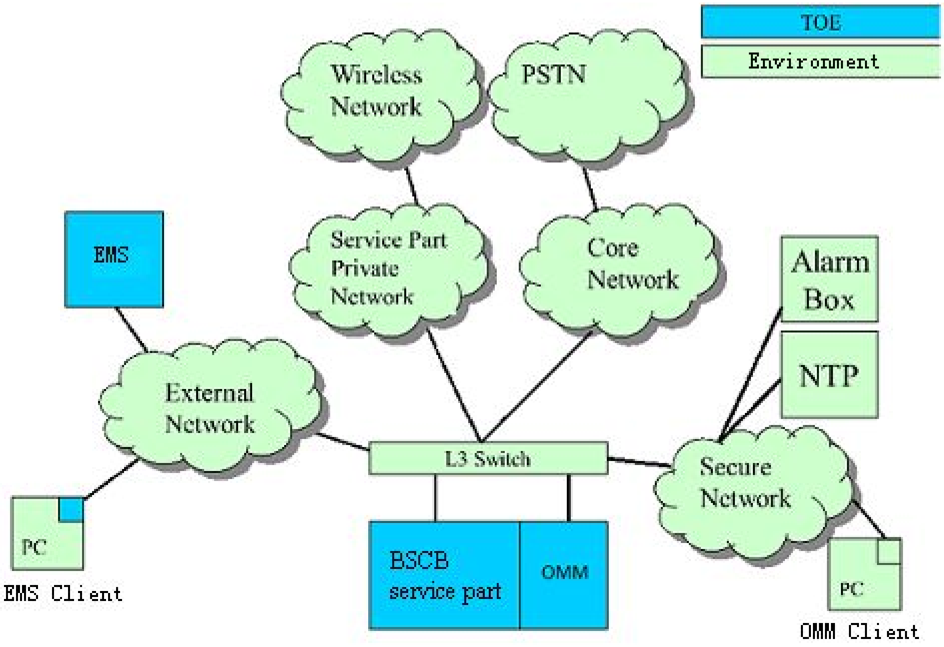
The RNC has the following general functionalities:

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

Appendix C
BSCB

The BSCB is the base station controller part of the CDMA2000 system and is therefore connected to a wide variety of other systems and networks, as shown in Figure C-1.

Figure C-1 The TOE in its environment



The additional[16]systems and network are

- The OMM Client, a graphical user interface to the OMM, is not part of the TOE. This interface is only used in emergency cases and during pre-installation by ZTE
- 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 atrusted 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.

[16] Additional to those described earlier.

- The Wireless Network: This consists of BTSs. These are part of the telecommunications network and ultimately (through CDMA2000 air interface) connect to MS (Mobile Station), which consists of mobile phones and similar equipment that uses CDMA2000. It is considered a trusted network in this evaluation.
- The Core Network: It is divided to CS domain and PS domain. It is the control center of the mobile core network, and the gateway of the mobile network and internet. It is considered a trusted network in this evaluation.

The BSCB has the following general functionalities:

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

Figures