ZTE eNodeB Solution

Security Target

ZTE CORPORATION
NO. 55, Hi-tech Road South, ShenZhen, P.R.China
Postcode: 518057
Tel: (86) 755 26770801
URL: http://ensupport.zte.com.cn
E-mail: support@zte.com.cn

LEGAL INFORMATION

Revision History

Version	Date	Comment
0.1	Oct 10 2011	First version
0.2	Oct 14 2011	Amendments based on comments from SERTIT
0.3	Oct 17 2011	Amendments on Figure 3
0.4	Oct 31 2011	Updates based on EORs
0.5	Dec 14 2011	Updates based on EORs
0.6	Dec 24 2011	Updates based on EORs
0.7	Jan 18 2012	Add acronym list
0.8	Feb 9 2012	Add L3 switch between eNodeB and backhaul network Add MAC address for user identification

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

1 ST Introduction

1.1 ST and TOE References

This is version 0.8 of the Security Target for the ZTE eNodeB solution v1.0. ZTE's eNodeB solution consists[1] of:

- The ZXSDR B8200 TL200 (v2.00) baseband unit (BBU)
- A remote RF unit (RRU), either[2]:
  - The ZXSDR R8962 L26A (v2.00), or
  - The ZXSDR R8964 (v5.00)
- An U31 R18 v11.12.40 Element Management System (EMS)
- A U31 R18 v11.12.40 EMS Client

See Figure 1 for the structure of the TOE. The remainder of this ST will refer to the TOE as eNodeB.

1.2 TOE Overview and usage

The TOE is a single node in the Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) for Long-Term Evolution (LTE) network plus an EMS and client. The node interfaces with User Equipment (UE) and implements such functions as radio resource management, data stream IP header compression and encryption, attach progress selection, user plane data routing, data scheduling and transmission, and mobility management. The EMS manages the node, and the client is used to access the EMS.

The TOE consists of four parts:

- ZXSDR B8200 TL200 consists of the following modules:
  - Control and Clock module (CC)
    - Active/standby switching.
    - GPS system clock and RF reference clock.
    - Supporting GE Ethernet interface (either fiber interface or electric interface)
    - GE Ethernet switching provides switching plane for signaling low and data
    - Rack management function.
    - Clock extension interface (IEEE1588 V2).
    - Communications extension interface (via local maintenance interface[3]).

[1] In real-life, one EMS will manage multiple eNodeBs, and one eNodeB can consist of one BBU and multiple RRUs. For the purpose of this evaluation, only one of EMS, BBU and RRU is considered.

[2] Note that these modules do not perform security-related functions and are therefore interchangeable for the purpose of this ST.

- TCA Baseband Processing module (BPL)
  - Providing interface connecting with RRU
  - User plane protocol processing and physical layer protocol processing, including PDCP, RLC, MAC, PHY
  - Providing IPMI interface.
- Site alarm Board (SA)
  - Fan alarm monitoring and rotation speed control.
  - Providing eight E1/T1 ports
  - Providing one RS485 and one RS232 full duplex interface for external monitoring equipment respectively.
  - Providing six dry-contact input ports and two dry-contact input/output ports.
- Site alarm Extension Board (SE)
  - Providing eight E1/T1 ports
  - Providing one RS485 and one RS232 full duplex interface for external monitoring equipment respectively
  - Providing six dry-contact input ports and two dry-contact input/output ports
- Power Module (PM)
  - Input over-voltage, under-voltage measurement and protection
  - Output over-current protection and overload power management
- Fan Array Module (FA)
  - Providing fan control function and interface
  - Providing a temperature sensor to detect temperature of air intake
  - Providing LED display of fan plug-in box

- One RRU, either the R8962 or the R8964 consisting of:
  - Send/receive signal board
    - Realizes D/A and A/D conversion, frequency conversion, amplifying, filter and RF functions of signal. Realizes the system control and interface functions of ZXSDR RRU
  - Power Module
    - Conducts the input DC or AC power to ZXSDR RRU , and convert the DC or AC power to particular power that will be used by hardware parts and modules.
  - Cavity Filter
    - Provides access RF filtering
  - Power Amplifier
    - Realizes the input signal power amplification of the send/receive signal board, provides forward & backward

[3] Pre-configuration of eNodeB is done using a local GUI interface via the Eth1 interface. This local interface is disabled when TOE is in operation.

power coupling output interface, and provides the power detection function.

- A U31 R18 v12.11.40 EMS, consisting of:
  - A Sun Server running Solaris and Java
  - Java EMS software, which provides the management functionality of the system

- A U31 EMS Client R18 v12.11.40 EMS Client, consisting of:
  - Java software, running on top of a non-TOE platform, which allows administrative personnel access to the management functionality of the EMS server

These are connected by three networks:

- Core network: This is the internal network of the provider, and is considered secure in this evaluation.
- A backhaul network: This is an external network and is considered insecure in this evaluation.
- An IP Management network: This also an external network (for management) and is considered insecure in this evaluation.

The TOE and these networks are shown in Figure 1.

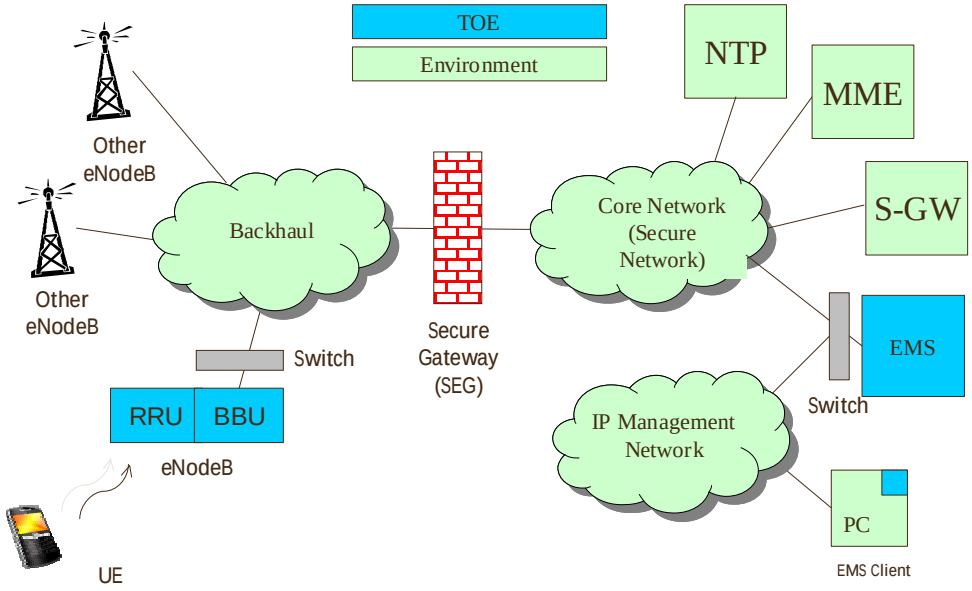

Figure 1: The TOE in its environment

The additional[4] systems are:

- L3 Switch: a switch providing filtering services to the EMS Server and BBU part of the TOE.

[4] Additional to those described earlier.

- Secure Gateway: The eNodeB connects to a secure gateway (SEG) using IPSec[5]. The SEG then connects to a secure network (Core) where MME/S-GW/EMS connects to.
- MME function
    - Allocating paging message to eNodeB.
    - Security control.
    - Idle state mobility control
    - S-GW bearer control
    - NAS signaling encryption and integrity protection
- S-GW function
    - Supporting UE's mobility switching user plane data
    - Downlink packet data buffer and paging support in E-UTRAN idle mode.

The eNodeB has the following general functionalities:

- Radio resource management: radio bearer control, radio admission control,
- Access mobility management, uplink/downlink dynamic resource allocation.
- IP header compression and user data stream encapsulation.
- Selecting MME during UE attaching progress
- Routing user plane data to S-GW
- Paging message scheduling and transmission
- Broadcast message scheduling and transmission.
- Measurement used for mobility and scheduling, and configuration of measurement report.

1.2.1 Major security features

The TOE:

- Secure management and usage of the TOE, to ensure that only properly authorized staff can manage and/or use the TOE.
- Provides secure interaction between various parts of the TOE and between the TOE and various machines in the environment, so that user data and/or management commands cannot be read or modified in between

1.2.2 Non-TOE Hardware/Software/Firmware

The TOE requires networking connectivity, an NTP server, a L3 switch to protect the EMS and one L3 switch to protect BBU S1/X2 interface.

Each EMS Client requires:

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

[5] The IPSec configuration of eNodeB is pre-configured before it is put into operation. IPSec uses digital certification or pre-shared key.

1.3 TOE Description

1.3.1 Physical scope

The TOE consists of the following:

BBU	Name and version
Hardware	B8200（V2.00）
Software	TD-LTE V2.00.041

RRU	Name and version
Hardware	R8964 （V5.00）or R8962 (v2.00)

EMS	Name and version
Hardware[6]	Sun M4000, 2*4 Core CPUs, 32GB Memory 2 146G SAS Disks, Dual-port HBA cards ST6180 8*300G FC15K Disk Array
Software	EMS Server version NetNumen U31 R18 V12.11.40 Java(TM) SE Runtime Environment (build 1.6.0_21-b06) Java HotSpot(TM) 64-bit Server VM (build 17.0-b16, mixed mode) Solaris 10 U9 SPARC Oracle 11.2.0.2 EE 64 bit for Solaris SPARC

EMS Client	Name and version
Hardware	-
Software	EMS Client NetNumen U31 R18 v12.11.40

Manuals
Certified Configuration ZTE eNodeB Common Criteria Security Evaluation – Certified Configuration R1.0

[6] Many other platforms are supported: larger Sun/Solaris combinations, IBM/AIX versions, HP/Linux and redundant version of some of these platforms. In this evaluation, only this platform was examined.

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 ZXSDR R8962 L26A(V1.00)TDD LTE RRU Hardware Installation ZXDSR R8962 L26A(V1.00)TDD LTE RRU User Manual ZXSDR R8964(V5.00)TD-LTE Remote Radio Unit Hardware Installation ZXSDR R8964(V5.00) TD-LTE Remote Radio Unit User Manual ZXSDR B8200 TL200(V2.00) TD-LTE Baseband Resource Unit System Description ZXSDR B8200 TL200(V2.00) TD-LTE Baseband Resource Unit Hardware Installation ZXSDR B8200 TL200(V2.00) TD-LTE Baseband Resource Unit Hardware Description IPSec configuration guide

1.3.2 Logical scope

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

The functionalities and threats are related to:

- Secure management and usage of the TOE, to ensure that only properly authorized staff can manage and/or use the TOE.
- Provides secure interaction between various parts of the TOE and between the TOE and various machines in the environment, so that user data and/or management commands cannot be read or modified in between

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

Secure management means proper authentication (who is the user), authorization (what is the user allowed to do) and auditing (what has the user done).

Provides secure interaction between various parts of the TOE and between the TOE and various machines in the environment, so that user data and/or management commands cannot be read or modified in between.

The TOE shall protect the communication between:

- BBU and SEG
- BBU and other BBU
- BBU and UE

- EMS Client and EMS Server

against disclosure, undetected modification and masquerading.

1.3.3 Roles and external entities

See section 5.2.

2 Conformance Claims

This ST conforms to:

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

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

3 Security Problem Definition

3.1 Organizational Security Policies

OSP.USERS
The TOE shall authenticate EMS 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 EMS users to use the TOE and/or manage various aspects of the TOE securely
- The confidentiality and integrity of the communication between:
  - BBU and SEG
  - BBU and other BBU
  - BBU and UE
  - EMS Client and EMS Server

These assets are threatened by the following threat agents:

- TA.ROGUE_USER A user of the EMS seeking to act outside his/her authorization.
- TA.NETWORK An attacker with access to the backhaul Network that is connected to the TOE and/or with access to the air network between UE and RRU
- 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.

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

T. NETWORK

TA.NETWORK is able to modify/read external network traffic originating from / destined for the TOE and thereby:

- perform actions on the TOE
- gain unauthorized knowledge about traffic between parts of the TOE and/or between the TOE and the SEG, another BBU and/or UE. .

T.PHYSICAL_ATTACK

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

3.3 Assumption

This Security Target uses two rassumptions:

A.TRUSTED_SYSTEMS

It is assumed that:

- the SEG and other BBU are trusted, and will not be used to attack the TOE.
- The L3 switch will block all traffic between EMS and Core Network/IP Management network except for:
  - Selected traffic between EMS and EMS Client
  - Selected traffic between EMS and BBU

A.NETWORK

It is assumed that the backhaul network, the Core Network and IP Management Network are separated and the Core Network is trusted.

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

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:

- BBU and SGE
- BBU and other BBU
- BBU and UE
- EMS Client and EMS Server

against disclosure, undetected modification and masquerading.

4.2 Security objectives for the Operational Environment

OE.CLIENT_SECURITY

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

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

OE.SERVER_SECURITY

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

OE.TIME

The NTP Server shall supply the TOE with reliable time.

OE.TRUST&TRAIN_USERS

The operator shall ensure 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 SEG and other BBU are trusted, and will not be used to attack the TOE.
- The L3 switch will block all traffic between EMS and Core Network/IP management network except for:
  - Selected traffic between EMS and EMS Client
  - Selected traffic between EMS and BBU
- The L3 switch will block all traffic between BBU and backhaul except for IPSec communications.

OE.NETWORK

The operator shall ensure that the backhaul network, the Core Network and IP Management Network are separated and ensure the security of the Core Network.

5 Security Requirements

5.1 Extended components definition

There are no extended components defined.

5.2 Definitions

The following terms are used in the security requirements:

Roles:

- Administrator
- Supervisor
- Maintenance
- Operator
- Customizable roles

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.

External entities:

- UE
- Other BBU
- SEG

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[8])***
- ***by MAC-address (if so configured for that user)***

and ensure that the EMS 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[9]**

- **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 ***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[10], the username in reverse[11] 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 passwords when changed**

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[12] the allowed work time (if so configured for that user) expires, or***

[8] For administrator, the IP range can directly be configured. For normal users the IP range can be configured via the roles.
[9] Unless this account has been set to unlockable.
[10] If the username is chang, “changchang” is not allowed.
[11] If the username is chang, “gnahc” is not allowed
[12] The sentence was refined to make it more readable.

- ***when one of the user roles is being locked while the user 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 ***EMS 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 TSF shall maintain the roles:

- **Administrator**
- **Supervisor**
- **Maintenance**
- **Operator**
- **Customizable 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 **EMS** shall be able to generate an audit record of the following auditable events**:**

a) Start-up and shutdown of the audit functions;
b) All auditable events for the **not specified** level of audit; and
c) **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:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, ***Type of event and Detailed Information.***

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **Administrator** 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**[13] if the audit trail is full.

Application note: Audit records can be exported to a backup server.

FDP_ITT.1.CLI Basic internal transfer protection
FDP_ITT.1.1 The TSF shall[14] prevent the **disclosure or modification** of ***all*** data when it is transmitted between the ***EMS and the EMS Client***.

FTP_ITC.1.SEG Inter-TSF trusted channel
FTP_ITC.1.1 The ***BBU*** shall provide a communication channel between itself and ***SEG*** 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 ***BBU*** shall permit the ***BBU and the SEG*** to initiate communication via the trusted channel.
FTP_ITC.1.3 The ***BBU*** shall initiate communication via the trusted channel for **transmission of user and signalling data.**

FTP_ITC.1.BBU Inter-TSF trusted channel
FTP_ITC.1.1 The ***BBU*** shall provide a communication channel between itself and ***another BBU*** 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 ***BBU*** shall permit the ***BBU and the other BBU*** to initiate communication via the trusted channel.
FTP_ITC.1.3 The ***BBU*** shall initiate communication via the trusted channel for **handovers.**

FTP_ITC.1.UE Inter-TSF trusted channel
FTP_ITC.1.1 The TSF shall provide a communication channel between itself and ***UE*** 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.

[13] The operation was completed to “take no other actions”, and this was subsequently refined away to make the sentence more readable.
[14] 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.

FTP_ITC.1.2 The TSF shall permit the ***TSF and the UE*** to initiate communication via the trusted channel.
FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **transmission of user data.**

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**
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: o **unlockable, or** o **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.2.1 The TSF shall enforce the **Role Policy** on **all roles and the TOE** and all operations 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, the TOE**.
FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among ***roles*** and ***the TOE*** is allowed:

- **for the roles Administrator, Supervisor, Maintenance, Operator and Customizable roles 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**
- **if a user has multiple roles, it is sufficient if one of the roles is allowed to perform 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
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.

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 various parts of the TOE and between the TOE and various machines in the environment, so that user data and/or management commands cannot be read or modified in between

FDP_ITT.1.CLI
Communication between the EMS and the EMS Client is protected by ssh and sftp.

FTP_ITC.1.SEG
The connection between the BBU and SEG is protected by IPSEC.

FTP_ITC.1.BBU
The connection between the BBU and another BBU is protected by IPSEC.

FTP_ITC.1.UE
The connection between the TOE and UE is protected by EPS Encryption Algorithm.

7 Rationales

7.1 Security Objectives Rationale

Assumptions/OSPs/Threats	Objectives
OSP.USERS	This OSP is implemented by: o O.AUTHENTICATE, which ensures users are authenticated o O.AUTHORISE, which ensures only authorized users can do actions (including management actions) o 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.
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: • BBU and SEG • BBU and other BBU • BBU and UE • EMS Client and EMS Server Since these are all the network connections of the TOE, this threat is countered.
T.PHYSICAL_ATTACK	This threat is countered by the following 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 counter the entire threat.
A.TRUSTED_SYSTEMS	This assumption is upheld by OE.TRUSTED_SYSTEMS, which directly restates the assumption.
A.NETWORK	This assumption is upheld by OE.NETWORK, 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, but also 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 • 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: 5 FMT_SMR.1 stating the predefined and customizable roles. 5 FDP_ACC.2 and FDP_ACF.1 defining a Role Policy, which states how the various roles manage the TOE. 5 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.CLI for the protection of communication between EMS and EMS Client • FPT_ITC.1.SEG, BBU and UE for the protection of communication between BBU and UE, SEG and other BBU. Since these are all five connections mentioned in the objective, the objective is achieved.

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	-
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 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	-
FTP_ITC.1	-
FDP_ITT.1	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	-

A Abbreviations

AC	Alternating Current
BBU	baseband unit
BPL	Baseband Processing module
CC	Control and Clock module
DC	Direct Current
EMS	Element Management System
EPS	Evolved Packet System
eNode B	Evolved Node B
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FA	Fan Array Module
IP	Internet Protocol
IPSEC	Internet Protocol Secure
LTE	Long-Term Evolution
LED	Light Emitting Diode
LTE	Long Term Evolution
L3	Layer 3
MME	Mobility Management Entity
MAC	Media Access Control
NAS	Non-Access Stratum
NTP	Network Time Protocol
PDCP	Packet Data Convergence Protocol
PHY	Physical Layer
PM	Power Module
RF	Radio Frequency
RLC	Radio Link Control
RRU	Remote Radio Unit
SA	Site alarm Board
SE	Site alarm Extension Board
S-GW	Serving Gateway
SEG	Security gateway
UE	User Equipment
UMTS	Universal Mobile Telecommunications System