ZXUN USPP

Universal Subscriber Profile Platform

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

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

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

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

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

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

Revision History

Version	Date	Comment
0.1	May 09, 2011	First version
0.2	June 07, 2011	Updated
0.3	June 15, 2011	Update SFR and appendix
0.4	July 1, 2011	Update and incorporate ZTE comments
0.5	July 5, 2011	Update
0.6	July 18, 2011	Update
0.7	July 27, 2011	Update
0.8	August 5, 2011	Add AAA to certain networks and update according to EOR
0.9	August 16, 2011	Administrative update
0.91	August 17, 2011	Minor update Minor update
0.92	August 26, 2011	Minor updatex
0.93	September 15, 2011	Administrative update according to actual TOE
1.0	September 23, 2011	Final version
1.1	October 13, 2011	Fix for ETR meeting

Serial Number: SJ-20111014194032-001

Publishing Date: 2011-10-13(R1.1)

References

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

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

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

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

This page intentionally left blank.

Contents

Chapter 1
ST Introduction

Table of Contents

1.1 ST and TOE References

This is version 1.1 of the Security Target for the ZTE ZXUN USPP Universal Subscriber Profile Platform, version USPP V4.11.10.

1.2 TOE Overview and Usage

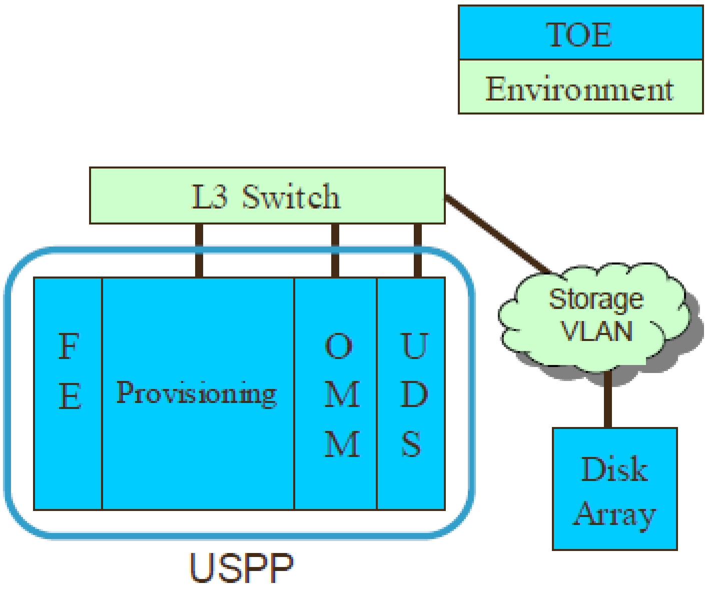
The TOE is a next generation home location register (HLR). It is a central database of a mobile core network which contains details of mobile phone subscribers that are authorized to use the mobile core network.

The TOE has the following general functionalities:

- Telecommunications functionality:
  - → It maintains the user subscription information and provides interface for operators to manage the subscription information.
  - → It provides subscriber data to various mobile core network to allow these mobile core network to authorise the subscribers to use the service of the mobile network according to their information.
  - → It can act as AAA server in various packet data service mobile network and fixed broadband network.
  - → It interacts with the signalling network to provide routing information for mobile terminal (MT) calls and short message service (SMS).
- Management functionality:
  - → Manage and configure the TOE
  - → Interact with EMS to be managed and configured

The TOE (depicted in Figure 1-1) consists of two parts.

Figure 1-1 The TOE

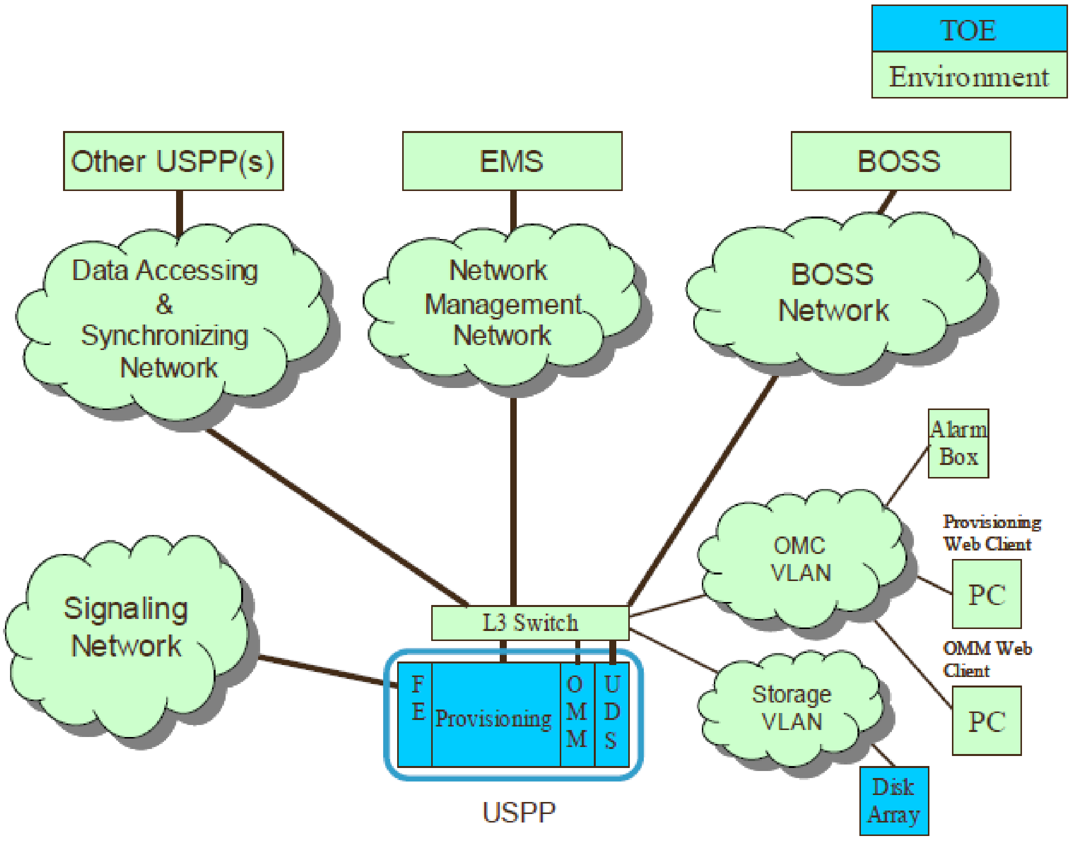


These entities are:

- A USPP, consisting of:
  - A front end (FE) subsystem, responsible for communicating with other network elements (NEs) by SS7 or IP signalling.
  - An Operations Maintenance Module (OMM) server, responsible for management and maintenance of the USPP. Users can use EMS or OMM web client to connect to it and perform management functionalities.
  - A Provisioning subsystem. Users can use the business operation support system (BOSS) or the provisioning web client to connect to it and perform subscribers' data management such as add/remove account, modify account properties, etc.
  - A Universal Directory Server (UDS), used to access and store the subscribers' information. It consists of three parts: DSA, DST, and a database. DSA stores the real-time subscriber database, and handles requests of subscriber data accessing and modifying from the Provisioning subsystem and FE. DST is used for data synchronization between DSA and the database on the disk array. If necessary (such as backup and restore database), DSA also gets subscribers' data from database by DST. Database is used to store the real-time data base in DSA for backup purpose.
- One or more disk arrays: Used to store the subscribers' data. They connect to the TOE through an operator-maintained VLAN "Storage VLAN". The Disk array is connected to the UDS via the L3 switch and is used as a backup of real-time subscribers' authentication data database in UDS. The disk array is located in the same room as the USPP.

The TOE is part of the mobile core network, thus it connects to various other network elements and networks, as shown in Figure 1-2.

Figure 1-2 The TOE in Its Environment



The additional[1] systems and networks are:

- One or more Management workstations. These use OMM web client or Provisioning web client running over a non-TOE web browser to access the OMM server or Provisioning server of the USPP. These workstations connect to the TOE via an operator-maintained VLAN "OMC VLAN".
- An Alarm box. Used to display alarms. It also connects to the operator-maintained "OMC VLAN".
- An EMS (Element Management System). This is a centralized management system that can be used to manage multiple TOEs. It connects to the OMM server of the TOE through an operator-maintained private network "Network Management (NM) Network".
- A BOSS (Business and Operation Support System). This is a unified platform that combines business support systems (BSS) and operations support systems (OSS). It is a comprehensive business operations and management platform, but also a real fusion of traditional IP data services and mobile value-added integrated business management platform. It's main function here is to manage and maintain user subscription information. BOSS is connected to the Provisioning subsystem of the TOE via an operator-maintained private network "BOSS Network".

[1] Additional to those described earlier.

- Signalling network (SN): This is a private IP-network or SS7 network of the operator. This network contains other network elements of the mobile core network such as mobile switching centre (MSC) in GSM mobile network or serving GPRS support node (SGSN) in GPRS mobile network which will request user account information from the USPP. In addition the mobile users can modify limited services (such as call blocking or call forward) of their own account using their user equipment via this network. The NEs in this network will connect to the FE subsystem of the USPP.
- Data accessing and synchronization network (DAS): This is a private IP-network of the operator. This network is used for a USPP to connect to other ZTE USPPs to form a virtual USPP cluster. This is mainly for performance and redundancy.
- An L3 switch: used to connect the disk array, management workstations, and the USPP. In addition, the Data Accessing & Synchronization Network, the Network Management Network, and the BOSS Network are connected to the USPP via the L3 switch.

1.2.1 Major Security Features

The TOE:

- Provides secure management of itself, to ensure that only properly authorised staff can manage the TOE
- Provides a flexible role-based authorisation framework with predefined and customisable roles
- Provides logging and auditing of user actions
- Provides secure communication channel between itself and EMS, OMM and Provisioning web clients
- Provides secure storage and access to its subscribers' authentication database so it cannot be maliciously read or altered.
- Provides identification and authentication data of subscribers to various mobile core network
- Provides multi-level load control to handle overload traffic, and ensure system reliability
- Can act as AAA server to various packet data service mobile network and fixed broadband network

1.2.2 Non-TOE Hardware/Software/Firmware

The TOE requires networking connectivity and an L3 switch to separate its various networks. It also requires several trusted networks (SN, DAS network, BOSS network, and Storage VLAN). Additionally, the OMM web client and the Provisioning web client requires:

Type	Name and version
Workstation	A PC suitable to run the OS (see below) and with at least 1 GB memory
OS	Any OS that supports the web browser (see below)

Type	Name and version
Web Browser	Internet Explorer 6.0 or higher with Adobe Flash Player 10.0 or higher

1.3 TOE Description

1.3.1 Physical Scope

The TOE consists of the following:

Type		Name and version
Hardware	OMM Server	1x DPBX1[2]
	Provisioning	1x DPBB2
	FE	
	DSA	1x DPBB1
	DST	
	Disk array	Fujitsu DX60
Software	OMM Server	ZTE CGS Linux V3.02.00_P01/32bit USPP V4.11.10 Apache 2.2.3 (with patch listed in appendix A installed)
	Provisioning	USPP V4.11.10
	DSA	USPP V4.11.10
	DST	ZTE CGS Linux V3.02.00_P01/64bit USPP V4.11.10
	FE	USPP V4.11.10
	Disk array	Oracle 10g se

The Provisioning, DSA, DST, FE may consist of more boards (DPBX1, DPBB1, and DPBB2). More board gives identical functionally, but provide better performance and more capacity.

The TOE is delivered with the following guidance:

Operational guidance is:

USPP V4.11.10
CC Guidance:
● ZXUN USPP Common Criteria Security Evaluation – Certified Configuration R1.2

[2] These are boards built by ZTE. The last two digits are the version number

USPP General:
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform Hardware Description (R1.2)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform Hardware Installation Guide (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform Software Installation Guide (R1.3)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform General Operation Guide (OMM Volume) (R1.3)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform Performance Management Operation Guide (OMM Volume) (R1.2)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform Alarm Management Operation Guide (OMM Volume) (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform Parts Replacement Guide (R1.2)
Home Location Register (HLR):
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLR Documentation Guide (R1.2)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLR Product Description (R1.2)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLR Data Configuration Guide (Basic Data Volume) (R1.2)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLR Data Configuration Guide (Service Data Volume I) (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLR Data Configuration Guide (Service Data Volume II) (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLR Agent Operation Guide (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLR Trace Management Operation Guide (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLR Routine Maintenance Guide (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLR Troubleshooting Guide (R1.2)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLR Performance Index Reference (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLR Performance Counter Reference I (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLR Performance Counter Reference II (R1.2)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLR Alarm Message Reference (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLR Notification Message Reference (R1.1)
Mobile Number Portability (MNP):

● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform MNP Documentation Guide (R1.3)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform MNP Product Description (R1.2)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform MNP Data Configuration Guide (Basic Data Volume) (R1.3)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform MNP Data Configuration Guide (Service Data Volume) (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform MNP Trace Management Operation Guide (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform MNP Agent Operation Guide (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform MNP Routine Maintenance Guide (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform MNP Troubleshooting Guide (R1.2)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform MNP Performance Counter Reference (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform MNP Alarm Message Reference (R1.2)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform MNP Notification Message Reference (R1.2)
Equipment Identity Register (EIR):
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EIR Documentation Guide (R1.2)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EIR Product Description (R1.2)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EIR Data Configuration Guide (R1.2)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EIR Trace Management Operation Guide (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EIR Agent Operation Guide (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EIR Routine Maintenance Guide (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EIR Troubleshooting Guide (R1.2)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EIR Performance Counter Reference (R1.2)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EIR Alarm Message Reference (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EIR Notification Message Reference (R1.1)
Evolved Packet Core Home Subscriber Server (EPC HSS)

● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EPC HSS Documentation Guide (R1.2)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EPC HSS Product Description (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EPC HSS Data Configuration Guide (Basic Data Volume) (R1.2)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EPC HSS Data Configuration Guide (Service Data Volume I) (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EPC HSS Data Configuration Guide (Service Data Volume II) (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EPC HSS Trace Management Operation Guide (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EPC HSS Agent Operation Guide (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EPC HSS Routine Maintenance Guide (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EPC HSS Troubleshooting Guide (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EPC HSS Performance Index Reference (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EPC HSS Performance Counter Reference I (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EPC HSS Performance Counter Reference II (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EPC HSS Alarm Message Reference (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform EPC HSS Notification Message Reference (R1.1)
IP Multimedia Subsystem Home Subscriber Server (IMS HSS)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform IMS HSS Documentation Guide (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform IMS HSS Product Description (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform IMS HSS Data Configuration Guide (Basic Data Volume) (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform IMS HSS Data Configuration Guide (Service Data Volume) (R1.0)

● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform IMS HSS Trace Management Operation Guide (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform IMS HSS Agent Operation Guide (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform IMS HSS Routine Maintenance Guide (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform IMS HSS Troubleshooting Guide (R1.1)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform IMS HSS Performance Index Reference (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform IMS HSS Performance Counter Reference (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform IMS HSS Alarm Message Reference (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform IMS HSS Notification Message Reference (R1.0)
Home Location Register emulator (HLRe)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLRe Documentation Guide (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLRe Product Description (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLRe Data Configuration Guide (Basic Data Volume) (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLRe Data Configuration Guide (Service Data Volume) (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLRe Trace Management Operation Guide (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLRe Agent Operation Guide (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLRe Routine Maintenance Guide (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLRe Troubleshooting Guide (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLRe Key Performance Index Reference (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLRe Performance Counter Reference I (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLRe Performance Counter Reference II (R1.0)

● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLRe Performance Counter Reference III (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLRe Alarm Message Reference (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform HLRe Notification Message Reference (R1.0)
Authentication, Authorization and Accounting (AAA)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform UniA Documentation Guide (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform UniA Product Description (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform UniA Data Configuration Guide (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform UniA Trace Management Operation Guide (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform UniA Agent Operation Guide (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform UniA Routine Maintenance Guide (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform UniA Troubleshooting Guide (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform UniA Performance Index Reference (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform UniA Performance Counter Reference (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform UniA Alarm Message Reference (R1.0)
● ZXUN USPP (V4.11.10) Universal Subscriber Profile Platform UniA Notification Message Reference (R1.0)
BOSS interface specification:
● ZXUN USPP V4.11.10_Interface specification of command line (general) (V4.11.10 2011-08-30)
● ZXUN USPP V4.11.10_Interface specification of command line(3g_EPC fascicule) (V4.11.10 2011-04-07)
● ZXUN USPP V4.11.10_Interface specification of command line(CDMA fascicule) (V4.11.10 2011-08-30)
● ZXUN USPP V4.11.10_Interface specification of command line(EIR fascicule) (V4.11.10 2011-08-30)
● ZXUN USPP V4.11.10_Interface specification of command line(HSS fascicule) (V4.11.10 2011-08-30)
● ZXUN USPP V4.11.10_Interface specifications of command line(NP fascicule) (V4.11.10 2011-08-30)

● ZXUN USPP V4.11.10_Interface specifications of command line(BNAS AAA Fascicule) (V4.11.10 2011-08-30)
● ZXUN USPP V4.11.10_Interface specifications of command line(CDMA AAA Fascicule) (V4.11.10 2011-08-30)
● ZXUN USPP V4.11.10_Interface specifications of command line(CDMA+BNAS AAA Fascicule) (V4.11.10 2011-08-30)
● ZXUN USPP V4.11.10_Interface specifications of command line(GPRS AAA Fascicule) (V4.11.10 2011-08-30)
● ZXUN USPP V4.11.10_Interface specifications of command line(WiMAX AAA Fascicule) (V4.11.10 2011-08-30)

1.3.2 Logical Scope

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

The USPP is a database of subscriber information which contains information such as account information, account status, subscriber preferences, features subscribed to by the subscriber, subscriber's current location, etc. It provides unified subscriber data management and centralized subscriber database to various mobile networks such as GSM, UMTS, IMS, LTE, and CDMA network, etc.. It provides subscribers' information to the mobile core network to authenticate and authorize a subscriber to access the network and use the allowed services. It also acted as AAA for certain packet data service mobile network and fixed broadband network. In addition, it provides routing information for mobile terminals calls and short message service (SMS). The USPP provides real-time query or modification on subscriber information, service provisioning, and subscriber mobility management.

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

- Provides subscriber data to various mobile core network
- Provides multi-level load control to handle overload traffic, and ensure system reliability
- Provides AAA to various packet data service networks
- Secure storage and management of the subscriber database, ensuring that only the properly authenticated and authorized staff / user can manage / access the subscriber database.
- Secure management of the TOE, to ensure that only properly authorized staff can manage the TOE.
- Provides logging and auditing of user actions
- Secure communication between itself and EMS, OMM web client, and Provisioning web client.

The TOE provides subscriber data to various mobile core networks

The TOE provides identification and authentication data to GSM, UMTS, CDMA, IMS, and LTE mobile networks to enable the subscribers to identify and authorise themselves to use the services provided by these networks.

The TOE provides multi-level load control to handle overload traffic, and ensure system reliability

The TOE provides 6-level overload control and allows adjustment of these control thresholds according to the actual running conditions. This can prevents Denial of Service (DoS) attack on call handing service, SMS service, and mobility management.

The TOE provides AAA to various packet data service networks

The TOE provides authentication, authorisation, and accounting to the following packet data service networks: CDMA2000 1x/EV-DO network, GPRS/UMTS network, WiMAX network, Fixed broadband network, and 3GPP network

The TOE provides secure storage and management of the subscribers' database and ensure only properly authenticated and authorised staff / user can manage / access the subscribers' data

The TOE shall provide secure storage of the subscribers' authentication data, and ensure only properly authenticated and authorised staff can manage the subscribers' data.

The TOE shall allow authorised subscribers limited access to their own subscriber data, to configure services that are defined in the telecommunication standards.

The TOE provides secure management to ensure that only properly authorized staff can manage the TOE (except the subscribe data).

There are two ways of managing the TOE (except the subscribe data):

- Through the OMM Client: This allows full access to management functionality except the provisioning functionality
- Through the EMS: This allows similar access as through the OMM Client[3]

Secure management means:

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

Note that authentication, authorisation, and auditing is out-of-scope for the EMS, since it is not part of the TOE. The protection of communication between EMS and OMM is in scope.

The TOE provides logging and auditing of user actions

[3] The difference is that the EMS is centralised while the OMM Web Client is local to the specific USPP instance.

The TOE provides logging and auditing of user actions from OMM web client, Provisioning web client, and BOSS server.

The TOE provides secure interaction between itself and the EMS, itself and the OMM Web Client, and itself and the Provisioning Web Client so that data cannot be read or modified in between

The TOE shall protect the communication between:

- Provisioning Web Client and Provisioning subsystem
- OMM Web Client and OMM server
- EMS and OMM server

against disclosure, undetected modification and masquerading.

1.3.3 Roles and External Entities

See 5.2 Definitions.

1.4 Excluded from the evaluation

The TOE has a Provisioning GUI client written in C++ with similar functionality to the Provisioning Web client. However this GUI client is not a part of the standard TOE configuration and therefore is not assessed at all during the evaluation and is not allowed to use.

In addition, the TOE can be used in conjunction with a N+K redundancy[4] to ensure the availability. This option was not assessed at all during the evaluation.

[4] ZXUN USPP supports N+K geographic redundancy mechanism, which allows the FEs and BEs to be deployed in different sites and allows N+K NEs to be active. When “K” NEs are down, the remaining “N” BEs take over all services of failed NEs.

This page intentionally left blank.

Chapter 2
Conformance Claims

This ST conforms to:

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

This ST conforms to no Protection Profile.

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

This page intentionally left blank.

Chapter 3
Security Problem Definition

Table of Contents

3.1 Organisational Security Policies

OSP.USERS

The TOE shall:

- authenticate Provisioning users, log their activities, and allow them to set-up and configure the Provisioning functionality
- authenticate OMM users, log their activities, and allow OMM users to set-up and configure the OMM functionality
- authenticate BOSS servers, log their activities, and allow them to set-up and configure the provisioning functionality

OSP.IDENTIFY_NE

The TOE shall identify

- VLR in the GSM network
- VLR/SGSN in the UMTS network
- MME in the LTE network
- S-CSCF in the IMS network
- MSC/VLR in the CDMA network

before providing identification and authentication data to these NEs.

OSP.SECURED_ENVIRONMENT

The TOE requires that:

- The EMS, BOSS, NEs from signaling network, and other USPPs are trusted, and will not be used to attack the TOE.
- The operator shall protect communication
  - → between the TOE and other USPPs against masquerading, disclosure, and modification
  - → between the TOE and BOSS against masquerading, disclosure, and modification
  - → between the TOE and other NEs in the signaling network against masquerading, disclosure, and modification

- An L3 switch will block all traffic from/to the external network except for:
  - → Selected traffic between EMS and OMM server
  - → Selected traffic between BOSS and Provisioning server
  - → Selected traffic between USPP and other USPPs

OSP.SUBSCRIBER

The TOE shall allow authenticated and authorised subscribers[5] limited access to modify some of the services

OSP.AAA

The TOE shall be able to act as AAA server in the following packet data service mobile network and fixed broadband network:

- CDMA2000 1x/EV-DO network
- GPRS/UMTS network
- WiMAX network
- Fixed broadband network
- 3GPP network

to accept/reject subscribers use the network based on their identities.

3.2 Threats

3.2.1 Assets and Threat Agents

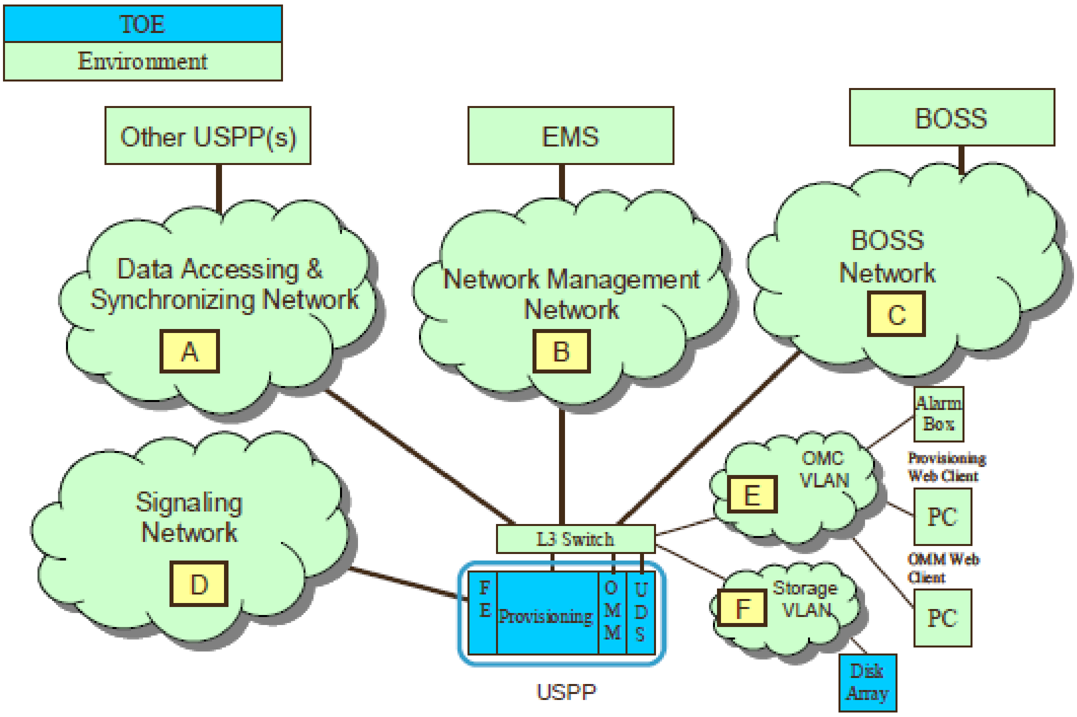
The assets are:

- The subscribers' authentication data.
- The ability to allow various users to manage various aspects of the TOE securely.

Figure 3-1 shows the possible sources of the threat agents. This asset is threatened by the following threat agents:

[5] The subscriber is authenticated and authorised by external entities such as VLR/SGSN of the UMTS network.

Figure 3-1 Possible threat agents



Source	Threat agents	Threat
A	No threat agent	No threat
B	TA.NETWORK_NM	An attacker who can access the network management network that is connected to the TOE
	TA.ROGUE_USER_EMS	An EMS user seeking to act outside his/her authorisation
C	TA.ROGUE_USER_BOSS	A BOSS Server user seeking to act outside his/her authorisation
D	TA.ROGUE_SUB	A subscriber seeking to access outside his/her authorisation
E	TA.OMC_VLAN	An attacker who can access the OMC_VLAN
	TA.ROGUE_USER_OMM	An OMM user seeking to access outside his/her authorisation
	TA.ROGUE_USER_PROV	A Provisioning user seeking to access outside his/her authorisation
F	TA.STORAGE_VLAN	An attacker who can access the STORAGE_VLAN
	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_USER

TA.ROGUE_USER_EMS, TA.ROGUE_USER_BOSS, TA.ROGUE_USER_OMM, or TA.ROGUE_USER_PROV tries to gain more access then he is entitled, to access the subscribers' authentication data.

T.AUTHORISED_USER

TA.ROGUE_USER_EMS, TA.ROGUE_USER_BOSS, TA.ROGUE_USER_OMM, or TA.ROGUE_USER_ PROV performs actions on the TOE that he is authorized to do, but these are undesirable[6] and it cannot be shown that this user was responsible.

T.UNAUTHORISED_SUB_MODIFY

TA.ROGUE_SUB seeking to gain more access then he is entitled, to access and modify subscribers' data than that he is allowed to.

T.UNKNOWN_ USER

TA.NETWORK_NM, TA.OMC_VLAN, or TA.STORAGE_VLAN tries to gain unauthorized access to the TOE to access the subscribers' authentication data.

T. NETWORK_AUT

TA.NETWORK_NM, TA.OMC_VLAN, or TA.STORAGE_VLAN is able to listen in / modify traffic to access subscribers' authentication data.

T.NETWORK_NM

TA.NETWORK_NM, TA.OMC_VLAN, or TA.STORAGE_VLAN is able to listen in / modify traffic to access management and subscriber data.

T.DOS

TA.ROGUE_SUB tries to overload the TOE to perform DoS attack.

T.PHYSICAL_ATTACK

TA.PHYSICAL gains physical access to the TOE (either USPP or disk array)and is able to perform actions on the TOE or access the subscribers' authentication data.

3.3 Assumptions

This Security Target uses one assumption:

A.AUTHORISED_SUBSCRIBER

It is assumed that if a subscriber wants to modify his own allowed service, he has be firstly identified and authorised by:

- VLR in the GSM network for the GSM subscribers
- VLR/SGSN in the UMTS network for the UMTS subscribers
- MSC/VLR in the CDMA network

[6] For example, the Provisioning user is allowed to modify subscribers' information based on the subscribers' request, but he misuses this to delete all subscribers.

Chapter 4
Security Objectives

Table of Contents

4.1 Overview

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 Rationales of this Security Target.

4.2 Security Objectives for the TOE

O.ENCRYPT_DATA

The TOE shall ensure that all the sensitive subscribers' authentication data (such as Ki and Opc in the GSM network) are encrypted while stored and transmitted between USPPs.

O.AUTHENTICATE_OMM

The OMM shall support OMM user authentication, allowing the OMM to accept/reject users based on username/password and a configurable subset of IP address and time of login.

O.AUTHENTICATE_PROV

The Provisioning server shall support provisioning user authentication, allowing the Provisioning server to accept/reject provisioning users based on username/password and a configurable subset of IP address and time of login.

O.IDENTIFY_NE

The TOE shall identify NEs in the GSM, UMTS, IMS, LTE, and CDMA network before providing subscribers' authentication data to these mobile networks.

O.AUTHENTICATE_SUB

The TOE shall support subscriber authentication for the cdma2000 1x/EV-DO, GPRS/UMTS network, WiMAX network, fixed broadband network, and 3GPP network, allowing the TOE to accept/reject subscribers based on NAI and IMSI.

O.AUTHORISE

The TOE shall support a flexible role-based authorisation framework with predefined and customizable roles. These roles can use the OMM server to manage the TOE or use the Provisioning functionality of 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.SEPARATE_USERS

The TOE shall

- Prohibit users with no OMM privilege to login the OMM Web Client and access the OMM functionalities
- Prohibit users with no Provisioning privilege to login the Provisioning Web Client or Provisioning server using the BOSS server to access the Provisioning functionalities

O.PROTECT_COMMUNICATION

The TOE shall:

- protect communication between the OMM server and the EMS against masquerading, disclosure and modification
- protect communication between the Provisioning web client and the Provisioning server against masquerading, disclosure and modification
- protect communication between the OMM web client and the OMM server against disclosure and modification

O.SUB_MODIFY

The TOE shall allow authorised subscribers limited access to their own subscriber data, to manage standard-defined services, based on standards.

O.PREVENT_DOS

The TOE shall provide load control mechanism to handle overload traffic, and ensure system reliability, to prevent DoS type attack.

4.3 Security Objectives for the Operational Environment

OE.CLIENT_SECURITY

The operator shall ensure that workstations that host one of the Clients are only connected to the OMC VLAN of the TOE, and 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 TOE or similar attacks

OE.PRIVATE_NETWORK

The operator shall maintain the following separated private network:

- Storage VLAN
- OMC VLAN
- BOSS network
- Data Accessing & Synchronization network
- Network Management network
- Signalling network

OE.PROTECT_COMMUNICATION

The operator shall configure the Secure Network to:

- protect communication between the TOE and other USPPs against masquerading, disclosure, and modification
- protect communication between the TOE and BOSS against masquerading, disclosure, and modification
- protect communication between the TOE and other NEs in the signaling networkagainst masquerading, disclosure, and modification

OE.SERVER_SECURITY

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

OE.TIME

The EMS shall supply the TOE with reliable time.

OE.TRUST&TRAIN_USERS

The operator shall ensure that OMM, Provisioningand BOSS roles are only assigned to users that are sufficiently trustworthy and sufficiently trained to fulfill those roles.

OE.TRUSTED_SYSTEMS

The operator shall ensure that the EMS, BOSS server, all the NEs in the signalling network (such as MSCS/VLR in GSM and UMTS network, S-CSF in IMS network, and MME in the LTE network), and other USPPs are trusted, and will not be used to attack the TOE. The operator shall configure the L3 switch to block all traffic from/to the external network except for[7]:

- Selected traffic between EMS and OMM server
- Selected traffic between BOSS and Provisioning server
- Selected traffic between USPP and other USPPs

OE.AUTHENTICATE_SUBSCRIBER

[7] Note that the traffic from the signalling network to FE does not go through the L3 switch, as Figure 1-2 shows.

The subscribers shall be authenticated and authorised by

- VLR in the GSM network for the GSM subscriber
- VLR/SGSN in the UMTS network for the UMTS subscribers
- MSC/VLR in the CDMA network for the CDMA subscribers

before they can access and modify his own allowed services (defined in 3GPP TS 22.004, Table 4.1 and 3GPP2 S.R0006).

Chapter 5
Security Requirements

Table of Contents

5.1 Extended Components Definition

This Security Target introduces one extended component: FAU_GEN.3 Simplified audit data generation. This component is a simplified version of FAU_GEN.1 and is therefore a suitable member of the FAU_GEN family. It was added to remove the need to log start and stop of auditing and to simplify the requirement.

FAU_GEN.3 Simplified audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

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

5.2 Definitions

The following terms are used in the security requirements:

Management related roles

- OMM Administrator
- OMM Operator
- OMM Maintainer
- OMM Monitoring
- Customizable roles

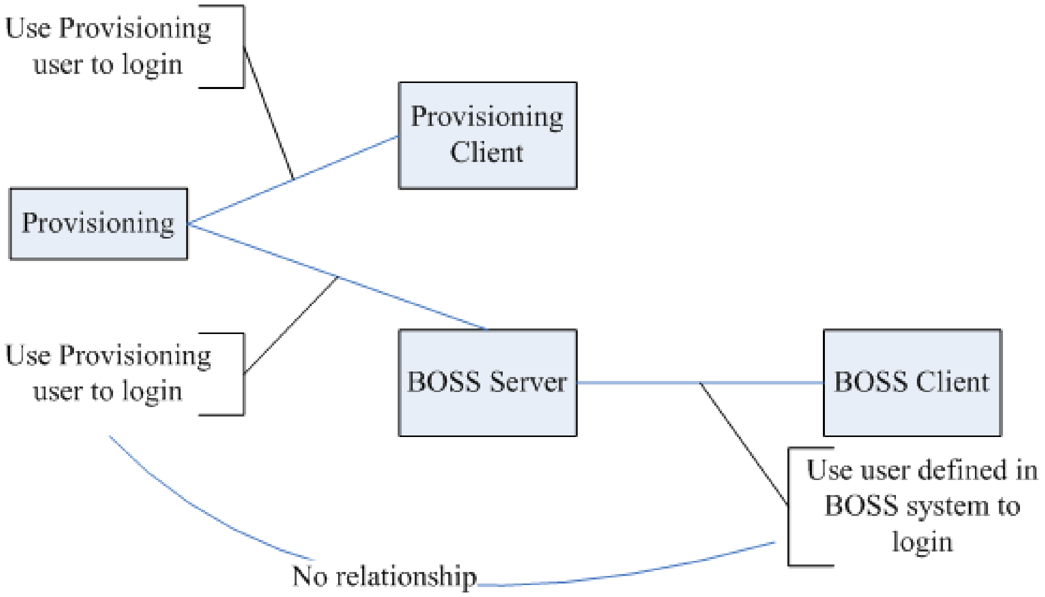
Management related external entities

- Element Management System (EMS)

Provisioning related roles

- There is no pre-defined provisioning roles. The provisioning roles are always customized and user who has provisioning role is defined as PROV user. These PROV users can login from the provisioning web client or can be used for BOSS server to login the Provisioning server, as Figure 5-1 illustrates. Note that BOSS server is a gateway for a mobile operator to access the Provisioning server. BOSS server has its own client and its own client account for mobile operator's personnel to perform provisioning actions at mobile operator side.

Figure 5-1 Relationship between user accounts for Provisioning Client, BOSS server, and BOSS Client


Use Provisioning user to login
Provisioning Client
Provisioning
Use Provisioning user to login
BOSS Server
BOSS Client
Use user defined in BOSS system to login
No relationship

Provisioning related external entities

- BOSS

Service related definitions:

Subscribers: A person who uses the service of the mobile network that TOE is part of

Subscriber data: subscriber's data such as phone number, authentication data, service setting.

Subscriber authentication data: subset of subscriber data that used in mobile network to authentication their subscribers.

Subscriber service data: subset of subscriber data that records what service does the subscriber have. Example of such data are call forwarding and call blocking. These data can be configured directly by the subscribers themselves.

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 and operations: None

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 six major groups:

- Identification & Authentication
- Roles & Authorisation
- Logging & Auditing
- Communication
- Resource management
- Subscriber identification and authentication
- Management

5.3.1 Identification & Authentication

FIA_UID.2.OMM User identification before any action

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

- ***by username (in all cases), and***
- ***by IP-address (if 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.PROV User identification before any action

FIA_UID.2.1 The ***Provisioning server*** shall require each ***PROV-***user to be successfully identified

- **by username (in all cases), and**
- ***by IP-address (if 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_UAU.2.OMM User authentication before any action

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

FIA_UAU.2.PROV User authentication before any action

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

FTA_SSL.3.OMM TSF-initiated termination

FTA_SSL.3.1 The ***OMM*** shall terminate a ***OMM Web Client*** interactive session

- ***when[8] the allowed work time (if so configured for that user) expires, or***
- ***when the session is inactive for 20 minutes***
- ***when administrator terminates the session***

FTA_SSL.3.PROV TSF-initiated termination

FTA_SSL.3.1 The ***Provisioning server*** shall terminate a ***PROV Web Client*** interactive session

- ***when the session is inactive for 5 hours***

FTA_SSL.3.BOSS TSF-initiated termination

FTA_SSL.3.1 The ***Provisioning server*** shall terminate an interactive ***BOSS-*** session

- ***when the session is inactive in a configurable consecutive period within 6 minutes.***

FIA_AFL.1.OMM Authentication failure handling

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

FIA_AFL.1.2When the defined number of unsuccessful authentication attempts has been **met**, the ***OMM*** shall **lock the user account**[9]

- **until unlocked by the administrator, or**
- **until an administrator configurable positive integer within [1-72] of hours have passed, if the account has not been set to permanent locking.**

FIA_AFL.1.PROV Authentication failure handling

FIA_AFL.1.1 The ***Provisioning server*** shall detect when **an 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 ***Provisioning server*** shall **lock the user account**[10]

- **until unlocked by the administrator, or**
- **until an administrator configurable positive integer within [1-72] 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 ***OMM*** 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**

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

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

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

- **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 < 90 days**
- **can be configured to be different from the previous 5 or more passwords when changed**

FTA_MCS.1.OMM Basic limitation on multiple concurrent sessions

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

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of **1** sessions per ***user and a limit 10 sessions for OMM web client.***

FTA_MCS.1.PROV 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 ***PROV Web Client***.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of **512** sessions ***of all PROV Web Client together.***

FTA_MCS.1.BOSS 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 ***BOSS server***.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of **32** sessions per ***BOSS server and a limit of 3200 sessions of all BOSS servers together.***

5.3.2 Roles & Authorisation

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles:

- **OMM Administrator**
- **OMM Operator**
- **OMM Maintenance**
- **OMM Monitoring**
- **Customized**

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

FDP_ACC.2.SYS Complete access control

FDP_ACC.2.1 The TSF shall enforce the **Role Policy** on **all roles and the TOE** nd all operationsamong ***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.SYS Security attribute based access control

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

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

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, Maintenance, Operator and Monitoring, as defined in Appendix B**
- **for the EMS to perform TOE management same as those defined in Appendix B**
- **for the customized roles, as defined by their customization**[13]
- **the Administrator and appropriately customized roles can perform the functions in FMT_SMF.1**[14]
- **if a user has multiple roles, it is sufficient if only one role is allowed to do the operation**

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:

- **Users without roles that have operation permissions on Provisioning**[15] **cannot manage subscribers data**
- **Users without roles that have operation permissions on OMM cannot manage the TOE itself**

5.3.3 Logging & Auditing

FAU_GEN.3.NE Simplified audit data generation

FAU_GEN.3.1 The TSF shall be able to generate an ***NE-record*** of the following auditable events**:**

(in the OMM security log):

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

FAU_GEN.3.2 The TSF shall record within audit ***NE-record***:

- Date and time of the event,
- **Security log ID**
- **Operator IP address**
- **Security operation**
- **Operation time**
- **Access mode**
- **Operation details**

[13] Provisioning role is one of the customized roles

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

[15] Provisioning command sets are command sets that can perform provisioning tasks.

FAU_GEN.3.PROV Simplified audit data generation

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

- **User information provision**

FAU_GEN.3.2 The TSF shall record within ***Provision-record***:

- Date and time of the event,
- **Client type**
- **Client node number**
- **Operation User name**
- **Error code (if error occurs)**
- **Serial number of a UDS operation log**
- **Operation Results**
- **MML commands for agent operations**

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **Administrator and suitably customized roles** with the capability to read **security log, and Provision log** from the TSF 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 unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to **prevent** unauthorized 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**[16] if the audit trail is full.

5.3.4 Communication

FDP_ITT.1 Basic internal transfer protection

FDP_ITT.1.1 The TSF shall[17] prevent the **disclosure or modification** of **subscribers' authentication** data when it is transmitted between the ***Provisioning server***, ***UDS***, ***and Disk Array***.

FDP_UCT.1 Basic data exchange confidentiality

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

[17] 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

FDP_UCT.1.1 The TSF shall[18] **transmit and receive** the ***subscribers' authentication*** data ***to and from other USPPs*** in a manner protected from unauthorised disclosure.

FTP_ITC.1.Web Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between ***(web browser*** and ***OMM) and (web browser and the Provisioning server)*** 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 TSF shall permit the ***web browser*** to initiate communication via the trusted channel.

FTP_ITC.1.3 ***(refined away)***[19]***.***

FTP_ITC.1.EMS Inter-TSF trusted channel

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

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

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

5.3.5 Resource management

FRU_PRS.1 Limited priority of service

FRU_PRS.1.1 The TSF shall assign a priority to the

- ***supplementary service message***
- ***short message service message***
- ***basic call handling service message***
- ***location management service message***
- ***Mobility management***[20] ***message***

in the TSF

FRU_PRS.1.2 The TSF shall ensure that each access to

- **CPU**

shall be mediated on the basis ***according to appendix C***.

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

[19] Because web server never initiate communication.

[20] For example, handover messages

5.3.6 Subscriber authentication

FIA_UID.2.NE User identification before any action

FIA_UID.2.1 The TSF shall require each ***NE*** to be successfully identified

- ***By IP-address***

before allowing ***accessing subscriber authentication data*** on behalf of that ***NE***.

FDP_ACC.1.SUB_MOD Subset access control

FDP_ACC.1.1 The TSF shall enforce the **Subscriber Access Control policy** on ***the FE to grant (GSM/UMTS Subscribers and CDMA 2000 subscribers)*** to access ***GSM/UMTS and CDMA 2000 Subscriber service data***

FDP_ACF.1.SUB_MOD Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **Subscriber Access Control** to objects based on the following: **GSM/UMTS subscribers and CDMA 2000 subscribers**, **the FE**.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among ***GSM/UMTS subscribersand CDMA 2000 subscribers*** and ***Subscriber service data*** is allowed:

- **As specified in 3GPP TS 22.004, Table 4.1 (for GSM/UMTS subscribers) (see appendix D)**
- **As specified in 3GPP2 S.R0006 (for CDMA subscribers) (see appendix D)**

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

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

FIA_UID.2.SUB_MOD User identification before any action

FIA_UID.2.1 The TSF shall require each ***Subscriber*** to be successfully identified

- ***By IMSI***[21] ***and MSISDN***[22] ***in the GSM/UMTS network***
- ***By the MIN, MDN, ESN, and MEID***[23] ***in the CDMA network***

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

FIA_UID.2.SUB_AAA User identification before any action

FIA_UID.2.1 The TSF shall require each ***subscriber*** to be successfully identified

- ***By NAI***[24] ***and IMSI in the CDMA2000 1X/EDVO network***
- ***By NAI and IMSI in GPRS/UMTS network***

[21] IMSI: International Mobile Subscriber Identity

[22] MSISDN: Mobile Subscriber Integrated Services Digital Network Number, IMSI and MSISDN are defined in 3GPP TS 23.003. It is the telephone number of the GSM or UMTS subscriber

[23] MIN: Mobile Identification number, MDN: Mobile Directory Number, ESN: Electronic Serial Number, MEID: Mobile Equipment Identity. MIN, MDN, and ESN are defined in TIA/EIA-41-D, and MEID is defined in X.S0008-0_v2.0_051018

[24] NAI: Network Access Identifier, defined in RFC 4282

- ***By NAI in the WiMAX network***
- ***By NAI in the fixed broadband network***
- ***By NAI and IMSI in the 3GPP network (For Wireless LAN, only NAI is used)***

before ***granting access right to the corresponding network*** on behalf of that ***subscriber.***

FIA_UAU.2.SUB_AAA User authentication before any action

FIA_UAU.2.1 The TSF shall require every ***subscriber*** to be successfully authenticated ***by methods defined in***

- ***X.S0011 for CDMA2000 1X/EDVO network;***
- ***3GPP TS 29.061 for GPRS/UMTS network;***
- ***NWG 1.3 for WiMAX network;***
- ***YD 1340.1-2005 part 1 to part 3 for fixed broadband network***
- ***3GPP TS 23.234, 3GPP TS 29.234, 3GPP TS 32.252, 3GPP TS 23.402, 3GPP TS 29.273, 3GPP TS 33.402, 3GPP TS 32.820 for 3GPP network***

before ***granting access right to the corresponding network*** on behalf of that ***subscriber.***

5.3.7 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
Set whether an user can only login from certain IP-addresses, and if so, which IP addresses	FIA_UID.2.OMM FIA_UID.2.PROV
Set the time that an user may remain logged in while inactive	FTA_SSL.3.BOSS
Logout user	FTA_SSL.3.OMM
Set whether an user is only allowed to work at certain times, and if so, at which times	FIA_UID.2.OMM FIA_UID.2.PROV FTA_SSL.3.OMM
Set the number of allowed unsuccessful authentication attempts	FIA_AFL.1.OMM FIA_AFL.1.PROV
Set the number of hours that an account remains locked	FIA_AFL.1.OMM FIA_AFL.1.PROV
Set whether an user account should be: ● unlockable, or ● locked (either permanently or temporarily) when it exceeds the number of allowed consecutive unsuccessful authentication attempts	FIA_AFL.1.OMM FIA_AFL.1.PROV

Management function	**Related to SFR**
Unlock an user account	**FIA_AFL.1.OMM** **FIA_AFL.1.PROV**
Set whether an user password expires after a certain time, and if so, after how long	**FIA_SOS.1**
Set whether the new password of an user must be different from the last n passwords when the password is changed by the user and configure n	**FIA_SOS.1**
Create, edit and delete customized roles	**FMT_SMR.1**
Add or remove roles to/from users	**FMT_SMR.1**
Assign priority to incoming messages	**FRU_PRS.1**
Configure a log can exist how many days before it can be cleared	**FAU_STG.4**
Create, edit and delete user accounts	-

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

Assurance Class	Assurance Components	
	Identifier	**Name**
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.

Chapter 6
TOE Summary Specification

The TOE provides subscriber data to various mobile core networks

FIA_UID.2.NE

The TOE will provide VLR in the GSM network, VLR/SGSN in the UMTS network, S-CSCF in the IMS network, MME in the LTE network, and MSC/VLR in the CDMA network subscriber data to allow these networks authorise subscribers to use their service. These network elements shall identify themselves before request the subscriber authentication data.

The TOE provides multi-level load control to handle overload traffic, and ensure system reliability

FRU_PRS.1

The TOE will prioritise the incoming messages and handle them according to the operator configured rules.

The TOE provides AAA to various packet data service networks

FIA_UID.2.SUB_AAA, FIA_UAU.2.SUB_AAA

Whenever a subscriber of CDMA2000 1X/EV-DO network, GPRS/UMTS network, WiMAX network, fixed broadband network, and 3GPP network wishes to use the packet data service provided by these networks, the user needs to be identified and authenticated according to methods defined in the corresponding standards.

The TOE provides secure storage and management of the subscribers' database and ensure only properly authenticated and authorised staff / user can manage / access the subscribers' data

The TOE provides secure management of the TOE, to ensure that only properly authorized staff can manage the TOE (except the subscriber data).

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

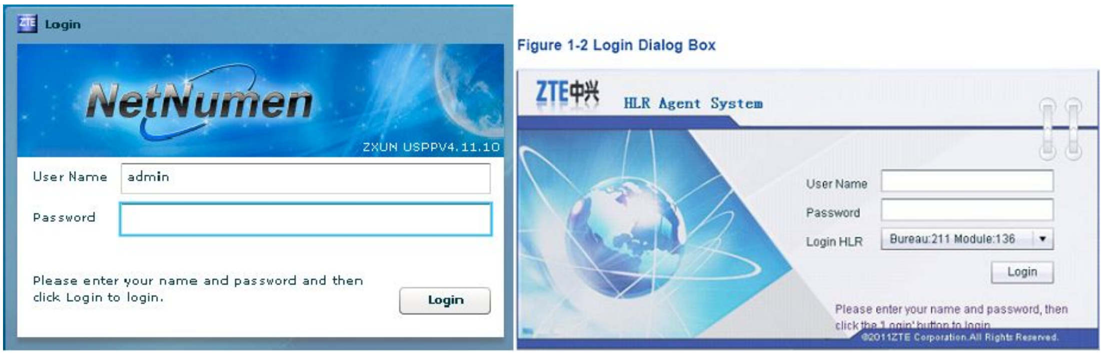
FDP_ITT.1, FDP_UCT.1

The subscribers' authentication data are encrypted with TDES during the data exchange between the database of the TOE and the USPP part of the TOE.

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

Whenever a user of the TOE wishes to manage the TOE itself or the subscribers' data, the user needs to use one of the clients of the TOE or through the BOSS. The first action required by the user is then to log-in. Note that while the OMM and the Provisioning provides normal user login interface (Figure 6-1), to allow BOSS server to login the operator need to write a configuration file on the BOSS server (Figure 6-2).

Figure 6-1 OMM and Provisioning Web client login



User Name: admin

Password:

Please enter your name and password and then click Login to login.

Figure 1-2 Login Dialog Box

User Name:

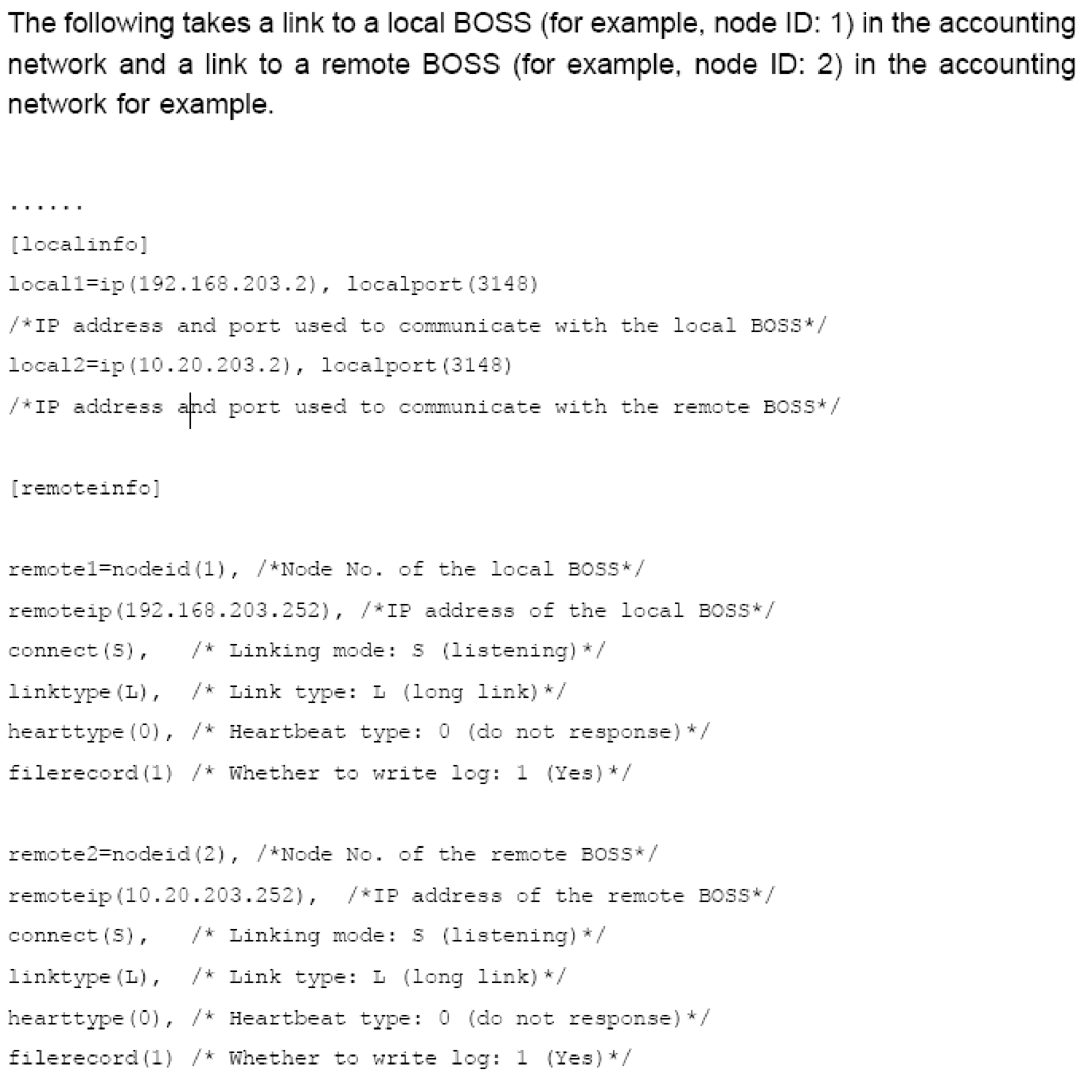
Password:

Login HLR: Bureau:211 Module:136

Please enter your name and password, then click the 'Login' button to login.

©2011ZTE Corporation.All Rights Reserved.

Figure 6-2 Configuration file on the BOSS server



The following takes a link to a local BOSS (for example, node ID: 1) in the accounting network and a link to a remote BOSS (for example, node ID: 2) in the accounting network for example.

```
......
[localinfo]
local1=ip(192.168.203.2), localport(3148)
/*IP address and port used to communicate with the local BOSS*/
local2=ip(10.20.203.2), localport(3148)
/*IP address and port used to communicate with the remote BOSS*/

[remoteinfo]

remote1=nodeid(1), /*Node No. of the local BOSS*/
remoteip(192.168.203.252), /*IP address of the local BOSS*/
connect(S),   /* Linking mode: S (listening)*/
linktype(L),  /* Link type: L (long link)*/
hearttype(0), /* Heartbeat type: 0 (do not response)*/
filerecord(1) /* Whether to write log: 1 (Yes)*/

remote2=nodeid(2), /*Node No. of the remote BOSS*/
remoteip(10.20.203.252),  /*IP address of the remote BOSS*/
connect(S),   /* Linking mode: S (listening)*/
linktype(L),  /* Link type: L (long link)*/
hearttype(0), /* Heartbeat type: 0 (do not response)*/
filerecord(1) /* Whether to write log: 1 (Yes)*/
```

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

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

FTA_MCS.1.*

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

- the user is already logged in

- too many other users are already logged in

FTA_SSL.3.*

The TOE will log a user out when:

- The administrator terminates the session of the user
- The allowed work time expires (OMM web client only)
- The BOSS-user session is inactive in a configurable consecutive time period within 6 minutes

FIA_SOS.1

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

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

Each client 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 or provisioning actions) allowed by the roles.

FDP_ACC.1.SUB_MOD, FDP_ACF.1.SUB_MOD

The services that subscriber can configure is specified in various telecommunications standards and protocols. The subscribers are only allowed to configure services based on these protocols, and cannot perform any other actions to the TOE.

FIA_UID.2.SUB_MOD

Whenever a GSM/UMTS or CDMA subscriber wants to modify their own allowed supplementary services, they must be identified by IMSI and MSISDN in the GSM/UMTS network or by the MIN, MDN, ESN, and MEID in the CDMA network

The TOE provides logging and auditing of user actions

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

Activities of the users are logged, and only certain roles are allowed to view the logs. 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. For provisioning log, up to six million logs can be stored in the database. When more provisioning logs are to be stored in the database, the system automatically exports the existing ones to a file, and then delete the exported logs from the database.

The TOE provides logging and auditThe TOE provides secure interaction between itself and the EMS, itself and the OMM Web Client, and itself and the Provisioning Web Client so that data cannot be read or modified in betweening of user actions

FTP_ITC.1.Web

The connection between the OMM Web client and Provisioning Web client and the TOE is protected by SSL.

FTP_ITC.1.EMS

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

This page intentionally left blank.

Chapter 7
Rationales

Table of Contents

7.1 Security Objectives Rationale

Assumptions/OSPs/Threats	Objectives
OSP.USERS The TOE shall: ● authenticate Provisioning users, log their activities, and allow them to set-up and configure the provisioning functionality ● authenticate OMM users, log their activities, and allow OMM users to set-up and configure the OMM functionality ● authenticate BOSS servers, log their activities, and allow them to set-up and configure the provisioning functionality	This OSP is primarily implemented by: ● O.AUTHENTICATE that restates the authentication of users ● O.AUTHORISATION that restates the authorisation of different users with different privilege ● O.AUDITING that states the activities of users will be logged.
OSP.IDENTIFY_NE The TOE shall identify ● VLR in the GSM network ● VLR/SGSN in the UMTS network ● MME in the LTE network ● S-CSCF in the IMS network ● MSC/VLR in the CDMA network before providing identification and authentication data to these NEs.	This OSP is primarily implemented by: ● O.IDENTIFY_NE that restates this.

Assumptions/OSPs/Threats	Objectives
OSP.SECURED_ENVIRONMENT The TOE requires that: ● The EMS, BOSS, NEs from signaling network, and other USPPs are trusted, and will not be used to attack the TOE. ● The operator shall protect communication → between the TOE and other USPPs against masquerading, disclosure, and modification → between the TOE and BOSS against masquerading, disclosure, and modification → between the TOE and other NEs in the signaling network against masquerading, disclosure, and modification ● An L3 switch will block all traffic from/to the external network except for: → Selected traffic between EMS and OMM server → Selected traffic between BOSS and Provisioning server → Selected traffic between USPP and other USPPs	This OSP is primarily implemented by: ● OE.PROTECT_COMMUNICATION that protects the communication between TOE and other USPPs, TOE and BOSS, and TOE and NEs in the signaling network ● OE.TRUSTED_SYSTEMS that ensures the EMS, BOSS, NEs from the signaling network, and other USPPs are trusted and will not be used to attack the TOE, and an L3 switch is used to block all traffic from/to the external network except for selected traffic between EMS and OMM server, BOSS and Provisioning server, and USPP and other USPPs.
OSP.SUBSCRIBER The TOE shall allow authenticated and authorised subscribers limited access to modify some of the services	This OSP is primarily implemented by: ● O.SUB_MODIFY that restates this.
OSP.AAA The TOE shall be able to act as AAA server in the following packet data service mobile network and fixed broadband network: ● CDMA2000 1x/EV-DO network ● GPRS/UMTS network ● WiMAX network ● Fixed broadband network ● 3GPP network to accept/reject subscribers use the network based on their identities.	This OSP is primarily implemented by: ● O.AUTHENTICATE_SUB that restates this.

Assumptions/OSPs/Threats	Objectives
T.UNAUTHORISED_USER TA.ROGUE_USER_* tries to gain access to the subscribers' authentication data that is outside their authorisation.	This threat is countered by the following security objectives: ● OE.TRUST & that ensures that only users that are properly trusted and trained will be able to gain access to certain roles ● OE.TRUSTED_SYSTEMS preventing other USPPs, EMS, BOSS, and other NEs to be used to attack the TOE ● O.AUTHENTICATE that ensures users are properly authenticated so the TOE knows which roles they have ● O.AUTHORISE that ensures users need certain roles with rights to do certain actions for a certain group of functionality (OMM and PROVISIONING). ● Should this prove insufficient, O.AUDITING will ensure that the actions of user can be trace backed to him. To perform O.AUDIT, the TOE must have a time source, OE.TIME states that this time source will be an external NTP Server connected to the TOE Together these security objectives ensures that 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. And no NEs can be used to attack the TOE. The log ensures that even if someone performed unwanted actions, it is possible to trace back to him. Therefore this threat is countered.
T.AUTHORISED_USER TA.ROGUE_USER_* performs actions on the TOE that he is authorized to do, but these are undesirable and it cannot be shown that this user was responsible.	This threat is countered by: ● OE.TRUST & TRAIN that ensures that only users that are properly trusted and trained will be able to gain access to certain roles. This should go a long way to prevent the threat from being realized. ● Should this prove insufficient, O.AUDITING will ensure that the actions of the user can be traced back to him. Together these security objectives counter the threat.

Assumptions/OSPs/Threats	Objectives
T.UNAUTHORISED_SUB_MODIFY TA.ROGUE_SUB seeking to gain more access then he is entitled, to access and modify subscribers' data than that he is allowed to.	This threat is countered by ● O.SUB_MODIFY that ensures the subscriber can only modify their own allowed services according to the standards. ● OE.AUTHENTICATE_SUBSCRIBER that ensures subscribers have to be authenticated and authorised before they can perform any actions on their own allowed services. Together these security objectives counter the threat.
T.UNKNOWN_USER_* TA.NETWORK_NM, TA.OMC_VLAN, or TA.STORAGE_VLAN tries to gain unauthorized access to the TOE and is able to perform actions on the TOE or access subscribers' authentication data of the TOE.	This threat is countered by: ● OE.CLIENT_SECURITY, preventing the attacker to gain access to the clients ● O.AUTHENTICATE, preventing the attacker to gain access to the servers ● O.ENCRYPT_DATA prevents attacker to obtain the subscribers' authentication data from the database. Together these security objectives counter the threat.
T. NETWORK_AUT TA.NETWORK_NM, TA.OMC_VLAN, or TA.STORAGE_VLAN is able to listen in/ modify to access the subscribers' authentication data	This threat is countered by ● O.ENCRYPT_DATA That prevents TA.STORAGE_VLAN to access the subscribers' authentication data, and ● OE.PROTECT_COMMUNICATION that protects traffic between: ● Other USPPs and the TOE ● the NEs in the signaling network and the TOE and ● OE.PRIVATE_NETWORK That prevents TA.NETWORK_NM and TA.OMC_VLAN to access subscribers' authentication data. Therefore this threat is countered.

Assumptions/OSPs/Threats	Objectives
T. NETWORK_NM TA.NETWORK_NM, TA.OMC_VLAN, or TA.STORAGE_VLAN is able to listen in/ modify to access the management and provisioning data	This threat is countered by ● OE.PROTECT_COMMUNICATION ● O.PROTECT_COMMUNICATION that protects traffic between: ● the OMM server and the EMS ● the Provisioning server and the BOSS ● the OMM server and the OMM Web Client ● the Provisioning server and the Provisioning Web Client that prevents TA.NETWORK_NM and TA.OMC_VLAN access management data, and ● OE.PRIVATE_NETWORK that prevents TA.STORAGE_VLAN access management data. Therefore this threat is countered.
T.DOS TA.ROGUE_SUB tries to overload the TOE to perform DoS attack.	This threat is countered by ● O.PREVENT_DOS which uses load control mechanism to handle system overload situation, 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 must be protected from physical attack ● OE.CLIENT_SECURITY stating that the workstations that are used as client must be protected from physical attack. Together these two counter the entire threat.
A.AUTHORUSED_SUBSCRIBER It is assumed that if a subscriber wants to modify his own allowed service, he has be firstly identified and authorised by: ● VLR in the GSM network for the GSM subscribers ● VLR/SGSN in the UMTS network for the UMTS subscribers ● MSC/VLR in the CDMA network	This assumption is upheld by OE.AUTHENTICATE_SUBSCRIBER which restate this assumption.

7.2 Security Functional Requirements Rationale

Security objectives	SFRs addressing the security objectives
O.ENCRYPT_DATA The TOE shall ensure that all the sensitive subscribers' authentication data (such as Ki and Opc in the GSM network) are encrypted while stored and transmitted between USPPs.	This objective is met by FDP_ITT.1 and FDP_UCT.1, which states that the subscriber authentication data are encrypted while stored locally or transmitted between USPPs.
O. AUTHENTICATE_OMM The TOE shall support user authentication, allowing the TOE to accept/reject users based on username/password and a configurable subset of IP address and time of login.	This objective is met by: ● FIA_UID.2.OMM stating that identification will be done by username, but also IP-address and login time ● FIA_UAU.2.OMM stating that the users must be authenticated ● FIA_SOS.1 stating that passwords must have a minimum quality ● FIA_AFL.1.OMM stating what happens when authentication fails repeatedly ● FTA_SSL.3.OMM logging OMM users off when they are no longer allowed to work, when the session is inactive for 20 minutes, or when administrator terminates the session ● FTA_MCS.1.OMM limiting the number of logins per OMM user ● FMT_SMF.1 configuring all of the above. Together, these SFRs meet the objective and provide further detail.
O.AUTHENTICATE_PROV	● FIA_UID.2.PROV stating that identification will be done by username, but also IP-address and login time ● FIA_UAU.2.PROV stating that the users must be authenticated ● FIA_SOS.1 stating that passwords must have a minimum quality ● FIA_AFL.1.PROV stating what happens when authentication fails repeatedly ● FTA_SSL.3.PROV logging PROV-users off when the session is inactive for 5 hours ● FTA_SSL.3.BOSS logging the BOSS server off when the session is inactive for 6 minutes ● FTA_MCS.1.PROV limiting the number of logins of total Provisioning web clients

Security objectives	SFRs addressing the security objectives
	● FTA_MCS.1.BOSS limiting the number of logins of total BOSS servers ● FMT_SMF.1 configuring all of the above. Together, these SFRs meet the objective and provide further detail.
O.IDENTIFY_NE	This objective is met by FIA_UID.2.NE stating that the identification will be done by IP address.
O.AUTHENTICATE_SUB	This objective is met by: ● FIA_UID.2.SUB_AAA stating that identification will be done by NAI, IMSI, or both, depending on different standards ● FIA_UAU.2.SUB_AAA stating that the subscribers must be authenticated Together these SFRs meet the objective.
O. AUTHORISE The TOE shall support a flexible role-based authorisation framework with predefined and customizable roles. These roles can use the OMM server to manage the TOE or use the Provisioning functionality of 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.	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 roles manage the TOE. ● FMT_SMF.1 configuring all of the above. Together, these SFRs support a flexible authorisation framework.
O.SEPARATE_USERS The TOE shall ● Prohibit users with no OMM privilege to login the OMM Web Client and access the OMM functionalities ● Prohibit users with no Provisioning privilege to login the Provisioning Web Client or Provisioning server using the BOSS server to access the Provisioning functionalities	This objective is met by FDP_ACC.2 and FDP_ACF.1.
O.AUDITING The TOE shall support logging and auditing of user actions.	This objective is met by: ● FAU_GEN.3.* 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 FAU_STG.4.

Security objectives	SFRs addressing the security objectives
	Together, these SFRs support a flexible logging and auditing framework.
O.PROTECT_COMMUNICATION The TOE shall: ● protect communication between the TOE and the EMS against masquerading, disclosure and modification ● protect communication between the Provisioning web client and the Provisioning server against masquerading, disclosure and modification ● protect communication between the OMM web client and the OMM server against disclosure and modification	This objective is met by: ● FTP_ITC.1.EMS restating the first bullet ● FTP_ITC.1.web restating the second and third bullet together these SFRs meet the requirement.
O.SUB_MODIFY	This objective is met by: ● FDP_ACC.1.SUB_MOD and FDP_ACF.1.SUB_MOD states what services can subscriber modify according to which standard ● FIA_UID.2.SUB_MOD states that the subscriber identification is done by IMSI and MSISDN for the GSM/UMTS network, and MIN, MDN, ESN, and MEID for the CDMA network together these SFRs meet the requirement.
O.PREVENT_DOS The TOE must provide load control mechanism to handle overload traffic, and ensure system reliability, to prevent DoS type attack.	This objective is met by: ● FRU_PRS.1 stating the priority of the subjects and the access to the resources is controlled ● FMT_SMF.1 configures the priority of the subjects. together these SFRs meet the requirement.

7.3 Dependencies

SFR	Dependencies
FIA_UID.2.OMM	-
FIA_UID.2.PROV	-
FIA_UAU.2.OMM	FIA_UID.1: met by FIA_UID.2.OMM

SFR	Dependencies
FIA_UAU.2.PROV	FIA_UID.1: met by FIA_UID.2.PROV
FTA_SSL.3.OMM	-
FTA_SSL.3.PROV	-
FTA.SSL.3.BOSS	-
FIA_AFL.1.OMM	FIA_UAU.1: met by FIA_UAU.2.OMM
FIA_AFL.1.PROV	FIA_UAU.1: met by FIA_UAU.2.PROV
FIA_SOS.1	-
FTA_MCS.1.OMM	FIA_UID.1: met by FIA_UID.2.OMM
FTA_MCS.1.PROV	FIA_UID.1: met by FIA_UID.2.PROV
FTA_MCS.1.BOSS	FIA_UID.1: met by FIA_UID.2.PROV
FMT_SMR.1	FIA_UID.1: met by FIA_UID.2.OMM
FDP_ACC.2.SYS	FDP_ACF.1: met by FDP_ACF.1.SYS
FDP_ACF.1.SYS	FDP_ACC.1: met by FDP_ACC.2.SYS 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
FMT_SMF.1	-
FTP_ITC.1.web	-
FTP_ITC.1.EMS	-
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1: not met, since the policy was refined away the dependency is unnecessary
FDP_UCT.1	FTP_ITC.1 or FTP_TRP.1: not met, because the communication channel is secured by the external environment. FDP_ACC.1 or FDP_IFC.1: not met, since the policy was refined away the dependency is unnecessary
FRU_PRS.1	-
FRU_RSA.1	-
FIA_UID.2.NE	-
FDP_ACC.1.SUB_MOD	FDP_ACF.1: met by FDP_ACF.1.SUB_MOD

SFR	Dependencies
FDP_ACF.1.SUB_MOD	FDP_ACC.1: met by FDP_ACC.1.SUB_MOD FMT_MSA.3: not met, as the policy does not use security attributes, management of these attributes is unnecessary.
FIA_UID.2.SUB_MOD	-
FIA_UID.2.SUB_AAA	-
FIA_UAU.2.SUB_AAA	-
SAR	**Dependencies**
EAL 2	All dependencies within an EAL are satisfied
ALC_FLR.2	-

Chapter 8
Appendix

Table of Contents

8.1 Appendix A Installed Apache Patches

2006	CVE-2006-5752
2007	CVE-2007-1863, CVE-2007-3304 CVE-2007-3847 CVE-2007-4465, CVE-2007-5000, CVE-2007-6388, CVE-2007-6421
2008	CVE-2008-2939 CVE-2008-1678, CVE-2009-1195 CVE-2009-1890, CVE-2009-1891
2009	CVE-2009-3094, CVE-2009-3095, CVE-2009-3555, CVE-2009-2412, CVE-2009-0023, CVE-2009-3720, CVE-2009-3560, CVE-2009-1956
2010	CVE-2010-1623, CVE-2010-1452, CVE-2010-0434, CVE-2010-0408
2011	CVE-2011-0419

8.2 Appendix B List of Default Roles and Command Sets

Role	**Command set**
Administrator role	Administrator command set
	Operator command set
	Maintenance command set
	Monitoring command set
Operator role	Operator command set
	Maintenance command set
	Monitoring command set

Role	Command set
Maintenance role	Maintenance command set
	Monitoring command set
Monitoring role	Monitoring command set

8.3 Appendix C HLR Overload Control

Prior-ity Low ↓ High	Service type	Load level (load percentage corresponding to each level					
		0	1	2	3	4	5
		(0%~ 50%)	(50%~ 60%)	(60%~ 70%)	(70%~ 80%)	(80%~ 90%)	(90%~ 100%)
		Message pass rate					
	Supplementary services and location services	100%	0%	0%	0%	0%	0%
	Call services and short message services	100%	100%	75%	50%	25%	0%
	Mobility management	100%	100%	100%	75%	50%	0%

8.4 Appendix D Subscriber modifiable services

GSM/UMTS subscriber modifiable services (3GPP TS 22.004)

Supplementary Service							
Spec/section		Reg	Eras	Act	Deact	Inv	Int
22.067 eMLPP		x					
22.072, Call Deflection SS							
	CD						
22.081. Number Identif. SS							
	CLIP						
	CLIR						
	CoLP						
	CoLR						
22.082. Call Offering SS							
	CFU	x	x	x	x		

Supplementary Service							
Spec/section		**Reg**	**Eras**	**Act**	**Deact**	**Inv**	**Int**
	CFB	x	x	x	x		
	CFNRy	x	x	x	x		
	CFNRc	x	x	x	x		
22.083. Call Completion SS							
	CW			x	x		
	HOLD						
22.084. Multi Party SS							
	MPTY						
22.085. Comm. of Interest SS							
	CUG						
22.087. User-to-User SS							
	UUS						
22.086. Charging SS							
	AoCI						
	AoCC						
22.088. Call Restriction SS							
	BAOC	x		x	x		
	BOIC	x		x	x		
	BOIC-exHC	x		x	x		
	BAIC	x		x	x		
	BAIC-Roam	x		x	x		
22.067	eMLPP	x	x				
22.091. Call Transfer SS							
	ECT						
22.093. Completion of Calls to Busy Subscribers							
	CCBS SS						
	CCBS Requests			x	x		
22.096 Name Identification SS							
	CNAP						
22.135 Multicall							

Supplementary Service							
Spec/section		Reg	Eras	Act	Deact	Inv	Int
	MC	x					

CDMA subscriber modifiable services (3GPP2 S.R0006)

	Registration	De-registration	Activation	De-activation	Invocation
CD			x	x	
CFB	x	x	x	x	
CFD	x	x	x	x	
CFNA	x	x	x	x	
CFU	x	x	x	x	
CW			x	x	x
CNIR			x	x	x
CC					x
DND			x	x	
FA	x	x	x	x	
MWN			x	x	x
MAH	x	x	x	x	
PCA	x	x	x	x	
PL	x				
PACA					x
SCA	x	x	x	x	
SPINA	x		x	x	
SPINI	x		x	x	x
OTASP					x
VMR	x	x	x	x	x

Figures