ZTE Optical Transmission Equipment

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

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.

Document history

Version	Date	Comment
0.1	January 3, 2012	First version
0.2	April 5, 2012	Added SDH, refined Traffic Policy, completed all sections, submitted to SERTIT
0.3	May 31, 2012	Update according to EOR
0.4	July 31, 2012	Update version information
1.0	Aug 6, 2012	Update EMS version
1.1	Aug 9, 2012	Update M720 guidance manuals
1.2	Aug 14, 2012	Synchronize WDM terms

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

Content

1 ST Introduction

1.1 ST and TOE References

This is version 1.2 of the Security Target for the ZTE Optical Transmission Equipment Series.

1.2 TOE Overview and usage

The TOE consists of:

- One ZTE Optical Transmission Equipment[1] (OTE), either:
  - SDH (ZXONE 5800, ZXMP S325 or ZXMP S385), or
  - WDM (ZXMP M720, ZXMP M820, ZXWM M920, ZXONE 8300 or ZXONE 8500)
- One EMS (Element Management System), consisting of a server plus software
- One EMS Client consisting of a Java application. This application is intended to run on a workstation. This client is a graphical user interface to the EMS Server.

The TOE is depicted in Figure 1, together with relevant entities in its environment.

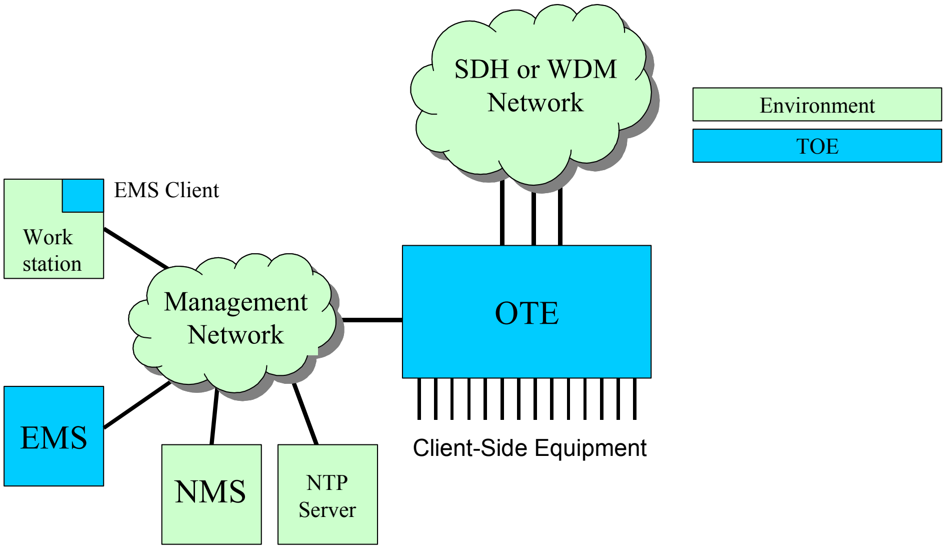


Figure 1: The TOE in its environment

These entities are:

- A Management network, which is used to manage the OTE. This management network is considered to be trusted, and contains (apart from the EMS):
  - An NMS: Network Management System[2]. This is a system that is used by a network operator to monitor its entire optical transmission network. The EMS sends performance data, alarm data, configuration data and similar information to the NMS.

[1] The major differences between different types of Optical Transmission Equipment is capacity and connections. See Appendix A for details

[2] Some operators refer to an NMS as an OSS (Operations Support System).

  - One or more management workstations with an EMS Client installed on them, which is used as a graphical user interface to the EMS Server.
  - An NTP-server, which serves as time source.
- An SDH or WDM network, consisting of other OTEs, connected to the TOE. The SDH/WDM network is considered to be trusted.

1.2.1 Major security features

The TOE:

- Transport data to/from client-side equipment across the SDH/WDM network in such a way that:
  - Only the intended recipients are able to read the signal
  - Nobody can modify the signals
- supports a flexible role-based authorization framework with predefined and customizable roles for management. These roles can use the TOE to manage the SDH/WDM network, and manage the TOE itself.
- supports a flexible authentication framework, allowing the TOE to accept/reject users based on: username/password and a configurable subset of IP/MAC-address and time of login.
- supports flexible logging and auditing of events.

1.2.2 Non-TOE Hardware/Software/Firmware

The EMS Client requires:

Type	**Name and version**
Workstation	A Workstation suitable to run the OS (see below)
OS	Windows, Linux or Solaris suitable to run 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)

The EMS Server does not require any non-TOE Hardware/Software/Firmware, but is always delivered with:

Type	**Name and version**
Anti Virus	A recent version of Trend Micro for CGS Linux (SPLX3.0 or higher with a recent virus library)

The Optical Transmission Equipment does not require any non-TOE Hardware/Software/Firmware.

1.3 TOE Description

1.3.1 Physical scope

The TOE consists of:

- One ZTE Optical Transmission Equipment (ZXONE 5800, ZXMP S325, ZXMP S385, ZXMP M720, ZXMP M820, ZXWM M920, ZXONE 8300 or ZXONE 8500)
- One EMS (Element Management System), consisting of a server plus software

- One EMS Client consisting of a Java application. This application is intended to run on a workstation. This client is a graphical user interface to the EMS Server.

1.3.1.1 Physical Scope Optical Transmission Equipment

ZXONE 5800 v1.10	
Hardware	ZXONE 5800
Software	ZXONE 5800 v1.10
Guidance	Installation Manual R1.2 Maintenance Manual (Volume I) Routine Maintenance R1.1 Maintenance Manual (Volume II) Alarm and Performance R1.2 Maintenance Manual (Volume III) Troubleshooting R1.1 Security Issue R1.1
ZXMP S325 v2.10	
Hardware	ZXMP S325
Software	ZXMP S325 v2.10
Guidance	Installation Manual R1.0 Maintenance Manual R1.0 Security Issue R1.1
ZXMP S385 v2.60	
Hardware	ZXMP S385
Software	ZXMP S385 v2.60
Guidance	Installation Manual R1.0 Maintenance Manual (Volume I) Routine Maintenance R1.0 Maintenance Manual (Volume II) Alarm and Performance R1.0 Maintenance Manual (Volume III) Troubleshooting R1.0 Security Issue R1.1
ZXMP M720 v1.00	
Hardware	ZXMP M720
Software	ZXMP M720 v1.00
Guidance	Hardware Descriptions R1.1 Installation Manual R1.1 Maintenance Manual R1.0 Security Issue R1.1
ZXMP M820 v2.51	
Hardware	ZXMP M820
Software	ZXMP M820 v2.51
Guidance	Hardware Descriptions (Volume I) R1.1 Hardware Descriptions (Volume II) R1.0 Installation Manual R1.1 Maintenance Manual (Volume I) Routine Maintenance R1.1 Maintenance Manual (Volume II) Alarm and Performance R1.1 Maintenance Manual (Volume III) Troubleshooting R1.1 Security Issue R1.1
ZXWM M920 V4.20P01	
Hardware	ZXWM M920
Software	ZXWM M920 V4.20P01
Guidance	Hardware Descriptions (Volume I) R1.0

	Hardware Descriptions (Volume II) R1.0 Installation Manual R1.0 Maintenance Manual (Volume I) Routine Maintenance R1.0 Maintenance Manual (Volume II) Alarm and Performance R1.0 Maintenance Manual (Volume III) Troubleshooting R1.0 Security Issue R1.1
ZXONE 8300 v1.00	
Hardware	ZXONE 8300
Software	ZXONE 8300 v1.00
Guidance	Hardware Descriptions (Volume I) R1.2 Hardware Descriptions (Volume II) R1.2 Installation Manual R1.1 Maintenance Manual (Volume I) Routine Maintenance R1.2 Maintenance Manual (Volume II) Alarm and Performance R1.2 Maintenance Manual (Volume III) Troubleshooting R1.1 Security Issue R1.1
ZXONE 8500 v1.00	
Hardware	ZXONE 8500
Software	ZXONE 8500 v1.00
Guidance	Hardware Description (Volume I) R1.3 Hardware Description (Volume II) R1.3 Installation Manual R1.2 Maintenance Manual (Volume I) Routine Maintenance R1.3 Maintenance Manual (Volume II) Alarm and Performance R1.3 Maintenance Manual (Volume III) Troubleshooting R1.2 Security Issue R1.1

1.3.1.2 Physical Scope EMS Server

EMS U31 R22 v12.12.20	

Hardware	SUN M5000，CPU 4x2.53GHz SPARC64 VII four-core Processors;
	Memory 32GB(8*4GB);Disks 2x300GB;
	4*1000Mbps Ethernet ports

Software	EMS Server version NetNumen U31 R22 v12.12.20 Java version 1.6.0_21 Java(TM) SE Runtime Environment (build 1.6.0_21-b06) Java HotSpot(TM) Server VM (build 17.0-b16, mixed mode) Oracle Solaris 10 update 8 Oracle Database 10g Enterprise Edition Release 10.2.0.4.0 - (64bit)
Guidance (common)	Operation Guide (General Operations) R1.0 Operation Guide (System Management) R1.0 Routine Maintenance Guide R1.0 User Guide (Northbound CORBA Interface) R1.0 User Guide (Northbound SNMP Interface) R1.0 User Guide (Northbound XML Interface) R1.0
Guidance (SDH-specific)	Operation Guide (SDHCTN End-to-End Management) R1.0 Operation Guide (SDH NE Management) R1.0 SDH Security Issues (in preparation)
Guidance	Operation Guide (WDMOTN End-to-End Management) R1.0

(WDM-specific)	Operation Guide (WDMOTN NE Management) R1.0 WDM Security Issues (in preparation)

1.3.1.3 Physical Scope EMS Client

EMS Client	**Name and version**
Software	EMS Client version NetNumen U31 R22 V12.12.20

1.3.2 Logical scope

The primary[3] functions of the TOE are to:

- transport input to/from client-side equipment across the SDH/WDM network in such a way that:
  - Only the intended recipients are able to read the signal
  - Nobody can modify the signals
- and manage the SDH/WDM network by providing the following services:
  - *Topology Management*: viewing, editing, and operating on the location, network structure, link connection and service distribution of the network resources in the network.
  - *Fault Management*: monitor the running status of all devices in the network
  - *Performance Management*: monitoring and analyzing the performance of the network
  - *Configuration Management*: managing network elements and network services

To protect access to these management services, the TOE provides four groups of security functionality:

Authentication: The EMS supports a flexible authentication framework, allowing the EMS to accept/reject users based on: username/password and a configurable subset of IP/MAC-address and time of login.

Whenever a user of the EMS wishes to manage the TOE or the SDH/WDM Network, the user needs to log-in on the graphical EMS-client

The EMS allows the Administrator[4] to configure (for each user), how that user must log-in:

- The user must always provide a username/password
- Whether the user can only login from a predefined IP-addresses and/or MAC-address
- Whether the user is only allowed to be logged in during a certain time (e.g. office hours)
- How the account is locked when the user repeatedly fails authentication (until unlocked by an Administrator[5] or until a predefined time elapses)

Authorization: The EMS supports a flexible role-based authorization framework with predefined and customizable roles. These roles can use the TOE to manage the SDH/WDM network, and manage the TOE itself.

[3] Note that the security-relevant functions are included in boxes.

[4] Or a customisable role that has been assigned this right.

[5] Or a customisable role that has been assigned this right.

The EMS allows management of the OTE equipment and itself by different users. The EMS can be configured to give each user precisely the access to the TOE and the resources of the SDH/WDM network that user needs to do his job. To assist in this, the role has a number of pre-defined roles:

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

and can assign these roles to specific users. The last three roles can also be assigned per resource, that is: a user can have the Maintenance role for one resource, but Operator role for another, and no role at all for all other resources.

In addition, the TOE allows the Administrator[6] to define, modify and name customized roles and assign rights to these roles.

Note that none of the roles above has full "root" access to the TOE. This is reserved for ZTE maintenance staff that regularly services the TOE using the systems console, but this is out of scope for this ST.

Accounting: The EMS supports flexible logging and auditing of security, operation and system events.

The EMS maintains 3 separate logs:

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

The logs are only accessible to the Administrator[7], who is only able to read the logs (not modify/delete them). Once logs become full, the oldest records are overwritten.

[6] Or a customisable role that has been assigned this right.

[7] Or a customisable role that has been assigned this right.

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 Organisational Security Policies

The TOE is intended to be used by many different telecom operators. Each operator will have a different optical transmission network structure and a different organizational structure with different roles. The TOE must be able to support all of these operators. This leads to the following organizational security policy:

OSP.FLEXIBLE_MANAGEMENT

The TOE must be able to support:

- a flexible role-based authorization framework with predefined and customizable roles, both to manage the wireless telecommunications network, and manage the TOE itself.
- a flexible authentication framework, allowing the TOE to accept/reject users based on username/password and a configurable subset of IP/MAC-address and time of login.
- flexible logging and auditing of events.

3.2 Threats

3.2.1 Assets and threat agents

The assets are:

1. The ability of administrators to manage various aspects of the TOE securely
2. Confidentiality and integrity of communication of client-side equipment over the SDH/WDM network

These assets are threatened by the following threat agents:

1. TA.CLIENT-SIDE An attacker with access to some client-side equipment.
2. TA.PHYSICAL An attacker with physical access to the TOE
3. TA.ROGUE_USER A TOE user seeking to act outside his/her authorization

3.2.2 Threats

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

T.CONFIDENTIALITY

TA.CLIENT-SIDE is able to read traffic that he is not allowed to read

T.INTEGRITY

TA.CLIENT-SIDE is able to modify traffic that he is not allowed to modify

T.PHYSICAL_ATTACK

TA.PHYSICAL gains physical access to the TOE (OTE, EMS or machine running the EMS Client) and is able to perform actions on the TOE.

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[8] and it cannot be shown that this user was responsible.

3.3 Assumptions

This Security Target uses one assumption:

A.TRUSTED_NETWORK

It is assumed that the Management Network and the SDH/WDM network are trusted. It is also assumed that the NMS and NTP Server are trusted and will not be used to attack the TOE.

[8] For example, the user is allowed to modify settings all over the telecommunications network to ensure that the network keeps functioning properly, but he misuses this to randomly change all settings thereby ensuring the network no longer operates properly.

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. ACCESS

The TOE shall ensure that client-side equipment can:

- Only send data across the network to certain other client-side equipment
- Only receive data across the network from that client-side equipment
- Is not able to modify data that is not created by it or sent to it.

O.AUTHORISE

The TOE shall support a flexible role-based authorization framework with predefined and customizable roles. These roles can use the TOE to manage the SDH/WDM network[9], and manage the TOE itself. 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.AUTHENTICATE

The TOE shall support a flexible authentication framework, allowing the TOE to accept/reject users based on: username/password and a configurable subset of IP/MAC-addressand time of login.

O.AUDITING

The TOE shall support flexible logging and auditing of events.

4.2 Security objectives for the Operational Environment

OE.SERVER_SECURITY

The customer shall ensure that the EMS Server and the Optical Transmission Equipment shall be protected from physical attacks.

OE.CLIENT_SECURITY

The customer shall ensure that management workstations that host the EMS Client, are protected from physical and logical attacks that would allow attackers to subsequently:

- Disclose passwords or other sensitive information
- Hijack the client

[9] E.g. modify the access described in O.ACCESS.

- Execute man-in-the-middle attacks between client and EMS Server or similar attacks.

OE.TRUST&TRAIN_USERS

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

OE.TIME

There shall be a correctly configured NTP-server available on the Management Network to supply the TOE with time.

OE.TRUSTED_NETWORKS

The customer shall ensure that:

- The Management Network and SDH/WDM Network are trusted, and will not be used to attack the TOE
- The NMS and NTP are trusted, so that they will not be used to attack the TOE

5 Security Requirements

5.1 Extended components definition

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

FAU_GEN.3 Simplified audit data generation
Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps
FAU_GEN.3.1 The TSF shall be able to generate an audit record of the following auditable events**: [assignment:** *defined auditable events***].**
FAU_GEN.3.2 The TSF shall record within each audit record: Date and time of the event, **[assignment:** *other information about the event***].**

5.2 Definitions

The following terms are used in the security requirements:

Roles:

- Administrator

Subjects/External Entities

- Services (on a Network)
- Ports (any physical Port to Client Equipment)

Objects:

- Traffic

Operations:

- Receive
- Send
- Modify

None of the subjects or objects have attributes.

Subjects

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

- Customized roles: these roles can be defined in the TOE by the Administrator (or by a configurable role who has the right to create roles) and have customizable rights.

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

Operations

Operations in the TOE are divided into

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

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

5.3 Security Functional Requirements

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.

5.4 Security Functional Requirements

The SFRs have been divided into five major groups:

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

5.4.1 Access

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the **Traffic Policy** on

- Ports
- Traffic
- Receive, Send, Modify.

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the **Traffic Policy** based on the following types of subject and information security attributes:

- Ports
- Traffic

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- Ports can Receive Traffic from other Ports on the SDH/WDM Network, if so allowed by the Traffic Policy rules
- Ports cannot Receive Traffic not destined for that port
- Ports can Send Traffic to other Ports on the SDH/WDM Network, if so allowed by the Traffic Policy rules
- Ports cannot Modify Traffic on other Ports

FDP_IFF.1.3, FDP_IFF.1.4, FDP_IFF.1.5 (refined away)

5.4.2 *Identification & Authentication*

FIA_UID.2 User identification before any action

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

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

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

FIA_UAU.2 User authentication before any action

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

FIA_AFL.1 Authentication failure handling

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

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

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

FIA_SOS.1 Verification of secrets

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

- At least 6 characters including three of the four types: number, small letter, capital letter, other characters
- cannot be the same as the user name, the user name twice[11], the username in reverse[12] or a common dictionary word
- can be configured to expire after a configurable amount of time < 180 days
- can be configured to be different from the previous 5 or more passwords when changed

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

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

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

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

- *when[13] the allowed work time (if so configured for that user) expires, or*
- *when one of the user roles is being locked while he is logged in.*

FTA_MCS.1 Basic limitation on multiple concurrent sessions

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

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

5.4.3 Roles & Authorisation

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles:

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

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

FDP_ACC.2 Complete access control

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

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

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **Role Policy** to objects based on the following: **all roles, all resources and the TOE[14].**

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

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

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

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

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

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

5.4.4 Logging & Auditing

The TOE maintains 3 separate logs:

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

FAU_GEN.3 Audit data generation

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

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.3.2 The TSF shall record within each audit record:

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

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **Administrator and suitably customized roles** with the capability to read **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**[16] if the audit trail is full.

5.4.5 Management

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

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[17]
Manage the Traffic Policy Rules	FDP_IFF.1
Set whether a user can only login from certain IP-addresses, and if so, which IP addresses	FIA_UID.2
Set whether a user can only login from certain MAC-addresses, and if so, which MAC-addresses	FIA_UID.2
Set whether a user can only login at certain times, and if so, at which times	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	FTA_SSL.3
Set the number of allowed unsuccessful authentication attempts	FIA_AFL.1
Set the number of hours that an account remains locked	FIA_AFL.1
Set whether a user account should be: ○ unlockable, or ○ locked (either permanently or temporarily) when it exceeds the number of allowed consecutive unsuccessful authentication attempts	FIA_AFL.1
Unlock a user account	FIA_AFL.1
Set whether a user password expires after a certain time, and if so, after how long	FIA_SOS.1
Set whether the new password of a user must be different from the last n passwords when the password is changed by the user and configure n	FIA_SOS.1
Set the maximum number of concurrent sessions for the same user	FTA_MCS.1
Create, edit and delete customized roles	FMT_SMR.1
Add or remove roles to/from users	FMT_SMR.1
Add or delete types of events to be logged in the security log	FAU_GEN.3.1
Create, edit and delete user accounts	-
Disable/enable[18] user accounts	-
Lock/unlock[19] roles	-
Adding, deleting and modifying rules in the Communication Policy	FDP_IFC.1, FDP_IFF.1

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

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

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

5.5 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

5.6 Security Assurance Requirements Rationale

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

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

6 TOE Summary Specification

Transport input to/from client-side equipment across the SDH/WDM network in such a way that:

- Only the intended recipients are able to read the signal
- Nobody can modify the signals

FDP_IFC.1, FDP_IFF.1

The TOE uses several mechanisms to enforce the Traffic Policy:

- Ports are physically isolated from each other, and can only talk to each other through a switch in the TOE.
- The TOE supports VLANs, to ensure that certain ports can only talk to certain other ports (either in the TOE or elsewhere in the SDH/WDM Network).
- The TOE supports ACL rules, both on Layer 2 (Ethernet) and Level 3 (IP), allowing fine-grained access control on MAC-address (source and destination), IP (destination) and ports.
- The TOE provides MAC Source Guard to prevent subscribers from modifying their own MAC addresses to circumvent the ACL rules

Authentication: The TOE supports a flexible authentication framework, allowing the TOE to accept/reject users based on: username/password and a configurable subset of IP/MAC-address and time of login.

General:

This functionality is implemented through a standard login screen.

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 either the graphical EMS-client or the CLI. The first action required by the user is then to log-in.

The TOE allows the Administrator[20] 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-addresses and/or MAC-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:

[20] Or a customisable role that has been assigned this right. Note that this footnote applies to all uses of the term “Administrator” in this section.

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

FTA_SSL.3

The TOE will log a user out when:

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

FIA_SOS.1

Whenever the user has to provide a new password to the TSF (all passwords expire in 6 months or less), 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.

Authorization: The TOE supports a flexible role-based authorization framework with predefined and customizable roles. These roles can use the TOE to manage the wireless telecommunications network, and manage the TOE itself.

General

This functionality is implemented by the TOE not providing access to certain actions by graying them out in the EMS Client or certain resources by not displaying these resources in the EMS Client for users whose roles do not allow this.

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

The TOE allows management of the telecommunications network by different users. The TOE can be configured to give each user precisely the access to the resources of the telecommunication network that user needs to do his job. To assist in this, the TOE has a number of pre-defined roles:

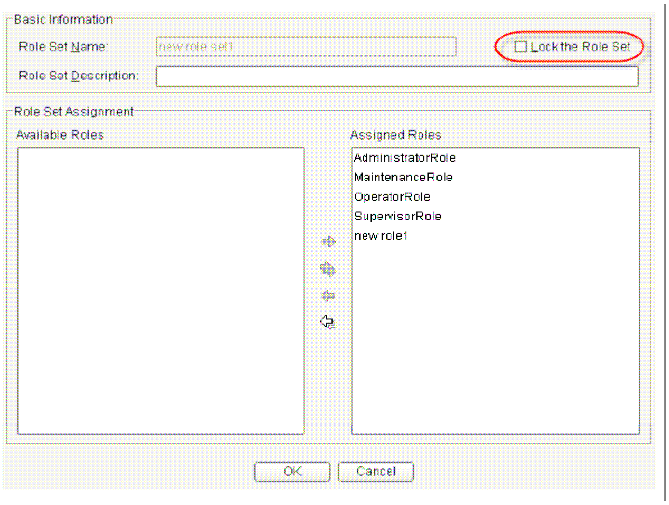
- Administrator: a role with unrestricted access rights over all resources,
- Maintenance: a role with high access rights, but only to resources assigned to him.
- Operator: a role with limited access rights, but only to resources assigned to him.
- Supervisor: a role with only viewing rights, but only to resources assigned to him

and can assign these roles to specific users.

The role of Administrator is a global role: he has all rights for all resources. The other three roles are assigned per resource, that is: a user can have the Maintenance role for one resource, but Operator role for another, and no role at all for all other resources.

Finally, the Administrator[21] can manage the TOE itself (see section 5.4.5 for a list of management functions), through a series of configuration and management screens. An example (how to lock a role) is given here:

[21] Or a customisable role that has been assigned this right.



Basic Information

Role Set Name: new role set1

☐ Lock the Role Set

Role Set Description:

Role Set Assignment

Available Roles

Assigned Roles

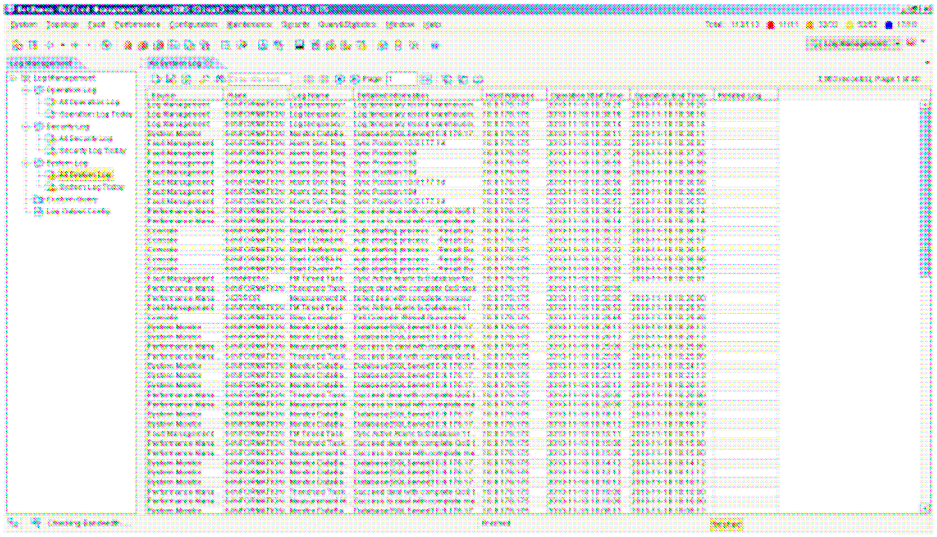
AdministratorRole
MaintenanceRole
OperatorRole
SupervisorRole
new role1

Note that 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 for this ST.

Accounting: The TOE supports flexible logging and auditing of events.

General

This functionality is implemented by a set of screens like this log viewing screen:



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

The TOE maintains a security log for authentication events

The log is only accessible to the Administrator[22], who is only able to read the log (not modify/delete them). Once the log becomes full, the oldest records are overwritten.

[22] Or a customisable role that has been assigned this right.

7 Rationales

7.1 Security Objectives Rationale

Assumptions/OSPs/Threats	Objectives
OSP.FLEXIBLE_MANAGEMENT The TOE must be able to support: • a flexible role-based authorization framework with predefined and customizable roles, both to manage the wireless telecommunications network, and to manage the TOE itself. • a flexible authentication framework, allowing the TOE to accept/reject users based on username/password and a configurable subset of: IP/MAC-address, time of login. • flexible logging and auditing of events.	This OSP is primarily implemented by the combination of three security objectives: • O.AUTHORISE that restates the first item of the OSP, • O.AUTHENTICATE that restates the second item of the OSP, and • O.AUDITING that restates the third bullet of the OSP Additionally, to perform logging (part of the third item), the TOE must have a time source. OE.TIME states that this time source will be one of the OMMs connected to the TOE.
T.CONFIDENTIALITY TA.CLIENT-SIDE is able to read traffic that he is not allowed to read	This threat is countered by the first two bullets of O.ACCESS, which directly prevent access to this traffic
T.INTEGRITY TA.CLIENT-SIDE is able to modify traffic that he is not allowed to modify	This threat is countered by the third bullet of O.ACCESS, which directly prevents modification of this traffic
T.PHYSICAL_ATTACK TA.PHYSICAL gains physical access to the TOE (OTE, EMS or EMS Client) and is able to perform actions on the TOE.	This threat is countered by: • OE.SERVER_SECURITY, preventing attackers physical access to the EMS and OTE, and • OE.CLIENT_SECURITY, preventing attackers physical access to the EMS Client
T.UNAUTHORISED TA.ROGUE_USER performs actions on the TOE that he is not authorized to do.	This threat is countered by four security objectives: • OE.TRUST&TRAIN_USERS 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 can do certain actions. • OE.CLIENT_SECURITY, which prevents TA.ROGUE_USER from bypassing the client. So the only way that a user can perform a management action is when he has a role, and the only way he can get this role is if he is properly trained and trusted. Therefore this threat is countered.

T.AUTHORISED TA.ROGUE_USER performs actions on the TOE that he is authorized to do, but these are undesirable[23] and it cannot be shown that this user was responsible.	This threat is countered by: • OE.TRUST&TRAIN_USERS 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 two security objectives counter the threat.
A.TRUSTED_NETWORK It is assumed that the Management Network and the SDH/WDM network are trusted. It is also assumed that the NMS and NTP Server are trusted and will not be used to attack the TOE.	This assumption is upheld by OE.TRUSTED_NETWORK, which restates the assumption.

[23] For example, the user is allowed to modify settings all over the telecommunications network to ensure that the network keeps functioning properly, but he misuses this to randomly change all settings thereby ensuring the network no longer operates properly.

7.2 Security Functional Requirements Rationale

Security objectives	SFRs addressing the security objectives
O. ACCESS The TOE shall ensure that client-side equipment can: • Only send data across the network to certain other client-side equipment • Only receive data across the network from that client-side equipment • Is not able to modify data that is not created by it or sent to it.	This objective is met by FDP_IFF.1 and FDP_IFC.1 specifying that there are rules regulating the access and FMT_SMF.1 allowing management of these rules.
O.AUTHORISE The TOE shall support a flexible role-based authorization framework with predefined and customizable roles. These roles can use the TOE to manage the SDH/WDM network[24], and manage the TOE itself. 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 various roles manage the network and the TOE. These also state that only roles can perform actions (operations on resources) and therefore users can only do this when they have the correct role □ FMT_SMF.1 configuring all of the above. Together, these SFRs support a flexible, role-based authorization framework.
O.AUTHENTICATE The TOE shall support a flexible authentication framework, allowing the TOE to accept/reject users based on: username/password and a configurable subset of IP/MAC-address and time of login.	This objective is met by: • FIA_UID.2 stating that identification will be done by username, password, IP/MAC-address, login time • FIA_UAU.2 stating that 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 preventing a user of having too many sessions or all users together having too many sessions • FMT_SMF.1 configuring all of the above. Together, these SFRs support a flexible authentication framework.
O.AUDITING The TOE shall support flexible logging and auditing of events.	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 all of the above Together, these SFRs support a flexible logging and auditing framework.

[24] E.g. modify the access described in O.ACCESS.

7.3 Dependencies

SFR	Dependencies
FAU_GEN.3	FPT_STM.1: met in the environment by OE.TIME
FAU_SAR.1	FAU_GEN.1: met by FAU_GEN.3, which is similar enough to meet the dependency
FAU_STG.1	FAU_GEN.1: met by FAU_GEN.3, which is similar enough to meet the dependency
FAU_STG.4	FAU_STG.1: met
FDP_ACC.2	FDP_ACF.1: met
FDP_ACF.1	FDP_ACC.1: met by FDP_ACC.2 FMT_MSA.3: unnecessary, since there are no security attributes
FDP_IFC.1	FDP_IFF.1: met
FDP_IFF.1	FDP_IFC.1: met FMT_MSA.3: unnecessary, since there are no security attributes
FIA_AFL.1	FIA_UAU.1: met by FIA_UAU.2
FIA_SOS.1	-
FIA_UAU.2	FIA_UID.1: met by FIA_UID.2
FIA_UID.2	-
FMT_SMF.1	-
FMT_SMR.1	FIA_UID.1: met by FIA_UID.2
FTA_MCS.1	FIA_UID.1: met by FIA_UID.2
FTA_SSL.3	-
SAR	**Dependencies**
EAL 2	All dependencies within an EAL are satisfied
ALC_FLR.2	-

A The different TOEs

The different TOEs can be distinguished by capacity (number of ports/cards) and by the protocols they support.

The protocols supported by the SDH TOEs are listed in Table 1. These are divided into NNI Protocols (to the SDH Network) and UNI protocols (to Client-Side Equipment.

NNI Protocols	S325	S385	5800
STM 64	▨		
STM 16			
STM 4			
STM 1			
10GE	▨		
GE			
FE			▨
UNI Protocols	**S325**	**S385**	**5800**
STM 16			
STM 4			
STM 1			
10GE	▨		
GE			
FE			▨
E3/ T3			▨
E1/ T1			▨
SAN	▨		

Table 1: SDH Protocols

The protocols supported by the WDM TOEs are listed in Table 2. Each protocoal can be used for connecting to Client-Side Equipment or WDM network equipment.

Protocols	M720	M820/M920	8300/8500
FE		▨	▨
GE			
10GE			
OC-3/STM-1		▨	▨
OC-12/STM-4		▨	▨
STM-16			
STM-64			
FC-100/200		▨	
FC-400			▨
FC-800	▨		▨
FC-1200		▨	▨

Table 2: WDM Protocols

B List of Acronyms

CWDM	Coarse WDM
DWDM	Dense WDM
FE	Fast Ethernet
GE	Gigabit Ethernet
EMS	Element Management System
NMS	Network Management System
pNNI	Network-to-network Interface
OC	Optical Carrier
OTE	Optical Transmission Equipment
SDH	Synchronous Digital Hierarchy
SDH/WDM	SDH or WDM
STM	Synchronous Transport Module
WDM	Wave Division Multiplexing
UNI	User Network Interface