iManager M2000 Security Target

Version: 1.20
Last Update: 2011-09-08
Author: Huawei Technologies Co., Ltd.

Table of Contents

Table of contents

List of figures

List of tables

Author

Version	Date	Author	Changes to previous version
V0.10	2010-12-16	**Huang Yunfang**	First release
V0.20	2011-1-29	**Huang Yunfang**	Update by the review result
V0.30	2011-2-21	**Huang Yunfang**	Modified the threats' definition
V0.40	2011-3-13	**Huang Yunfang**	Modifications in TOE reference
V0.50	2011-3-24	**Huang Yunfang**	Update by the review reports
V0.60	2011-3-29	**Huang Yunfang**	Update by the review reports
V1.0	2011-05-08	**Huang Yunfang**	Update by the review reports
V1.01	2011-05-09	**Huang Yunfang**	Update by the review reports
V1.04	2011-05-18	**Huang Yunfang**	Update by the review reports
V1.05	2011-05-20	**Huang Yunfang**	Update by the review reports
V1.06	2011-05-25	**Liu Jiwei**	Update by the review reports
V1.07	2011-07-11	**Huang Yunfang**	Update by the review reports
V1.08	2011-07-22	**Huang Yunfang**	Update by the review reports
V1.09	2011-08-22	**Huang Yunfang**	Update by the review reports
V1.10	2011-09-01	**Huang Yunfang**	Update by the review reports
V1.20	2011-09-08	**Huang Yunfang**	Update by the review reports

1 Introduction

1 This Security Target is for the evaluation of iManager M2000.

1.1 ST reference

2 **Title:** iManager M2000 Security Target

3 **Version:** V1.20

4 **Author:** Huang Yunfang

5 **Publication date:** 2011-09-08

1.2 TOE reference

6 **TOE name:** iManager M2000

7 **TOE version:** V200R011C01CP1301

8 **TOE Developer:** Huawei

9 **TOE release date:** 2011-8-22

10 Note: The TOE version is the above that is the result of applying the patch V200R011C01CP1301 to the product version V200R011C01SPC130 (that is also called main version).

11 Note: It is also used the acronym M2000 as TOE reference in the Security Target and ancillary documents for CC evaluation.

1.3 TOE overview

12 Huawei's iManager M2000 (M2000) Element Management system provides centralized operation and maintenance (OM) for Huawei's mobile network element management solution, provides external interfaces for interoperability with other systems. The core of iManager M2000 is the iMAP Platform, the software for managing the mobile network elements.

13 iMAP Platform provides extensive security features, including account based system access control that enforced only authenticated users can access authorized system features; auditing of security-relevant user activities; as well as the enforcement of network transmission against data peeking.

14 iManager M2000 provides additional security features. These include centralized users management for network elements (NE); auditing of security-relevant activities and users' operations; as well as encrypted transmission

between network elements and iManager M2000, between client and server of iManager M2000.

15 The ST contains a description of the security objectives and the requirements, as well as the necessary functional and assurance measures provided by the TOE. The ST provides the basis for the evaluation of the TOE according to the Common Criteria for Information Technology Security Evaluations (CC)

1.3.1 TOE usage

16 M2000 is the software for managing mobile networks. It provides a centralized network management platform for supporting telecom operators in their long-term network evolution and shielding the differences between various network technologies. The M2000 focuses on continuous efforts that telecom operators have made for network OM and inherits the existing OM experience.

17 The major security features implemented by iManager M2000 and subject to evaluation are:

I. User Role management

The iMAP platform can provide user management basing on role management. It has the default user groups including administrators, security managers, operators and guests. It also can define user groups for different user roles.

II. Authentication

The iMAP platform can authenticate all users accessing to the TOE by user name and password.

If the certificates are provided and deployed in network element and iManager M2000, the SSL connection between NE and M2000 can be selected through M2000 client, and also the authentication mode includes anonymous, single-direction and bi-direction. By default the authentication mode is anonymous.

III. Access Control

The iMAP platform can support that the administrator user and security operators can use the security management to authorize access to user accounts. The accessed objects authorized to user can have managed NEs, and then the user can only perform authorized operations to these authorized NEs.

In addition, the TOE also can authorize NE access of man machine language (MML) command group to user accounts, and the user can perform MML direct access to the authorized NEs.

IV. Auditing

The iMAP platform can generate audit records for security-relevant management actions and stores the audit records in database:

- User login / logout, a failed login attempt is also recorded.

- User account create / delete / modification
- Grant or revoke access right from user account
- User activities

The attempts of management operation regardless success or failure are logged, along with user name, source IP address, time stamp etc. The security operators can query, view and statistic the audit log through GUI client.

The TOE also collects the operation and security audit logs from managed network elements, and stores the logs in database.

Query and statics functionality for NE audit are provided via GUI interface, which allows authorized users to inspect the audit log.

V. IP-based ACL

The iMAP platform of TOE can offer a feature access control list (ACL) based on IP address for controlling which terminals can access to the TOE through the client of TOE. The ACL is based on IP address, the security role SMManagers and the super user admin can specify individual IP address or IP address range in ACL of a specified user account, the user then only can login to the TOE from terminals whose IP address is in the range of ACL.

VI. Encrypted transmission

The TOE support encrypted transmission between NEs and iManager M2000, client and server. It provides secure protocol, such as SSL, for the data transmission.

The TOE also provides a secure channel for the communication to the AT&NIC Website.

The communication between M2000 client and M2000 server is performed with a secure protocol (SSL).

SNMPv3 connections between the server and external SNMP clients.

VII. User session management

The iMAP platform provides all online user sessions and their latest behaviors are monitored and presented in the real-time. Once any of these sessions seems to be suspicious, the system administrator can immediately invalidate the sessions by kicking the sessions out of the system to prevent it from damages.

The iMAP platform also provides the user session management features including such as establishment, locking session.

VIII. Security function management

The iMAP platform offers security management for all management aspects of the TOE, which have user/role management, access control management and store security data in either databases or file system.

IX. Functionality without security claims

This evaluation does not make security claims with regard to the following functionality offered by the TOE:

- High availability (HA) features, such as the automatic switch-over to the stand-by server in case of hardware failure of active server, are not evaluated, but can be used.

- Backup and restore solution, providing to periodical backup, and restore the whole system if the fatal errors happen, is not evaluated, but can be used.

- Emergency system feature, such as the manual switch-over to the emergency system supporting alarm monitoring on NEs in case of the fatal errors in main system, is not evaluated, but can be used.

- Multi-Server Load Sharing (SLS) features, including the multiple ATAE blade servers networking and multiple SUN workstations networking, are not evaluated, but can be used.

- Digital signature for software package, providing to check the integrity for software package, is not evaluated, but can be used.

- The associated user management feature with NE local user, providing to start LMTs of NE without the input of user and password, is not evaluated, but can be used.

- The authentication on SSL connection between NEs and the TOE can be selected on the client of TOE if the X.509 certificates are deployed in NEs and the TOE. The authentication mode includes anonymous, single-direction and bi-direction. By default the authentication mode is anonymous. This feature is tested in NEs CC evaluations.

1.3.2 TOE type

18 The M2000 is a centralized wireless network management platform. The M2000 server software consists of the main version software and mediation software. The main version software implements system functions, and the mediation software is used for the adaptation of different NE interfaces. The M2000 can manage new NEs after the corresponding mediation software is installed. The M2000 adopts an open structure so that it can manage the devices of core network (CN), system architecture evolution (SAE), IP multimedia subsystem (IMS), and radio networks of various technologies such

as global system for mobile (GSM), wideband code division multiple access (WCDMA), code division multiple access(CDMA), worldwide interoperability for microwave access(WiMAX) and long term evolution (LTE).

19 The protocols with NEs are listed as followed:

- MML/BIN basing on Socket channel
- SOAP + MML

20 The M2000 provides standard common object request broker architecture (CORBA), simple network management protocol (SNMP), file, and alarm streaming interfaces. In addition, the M2000 allows for interoperability with other systems.

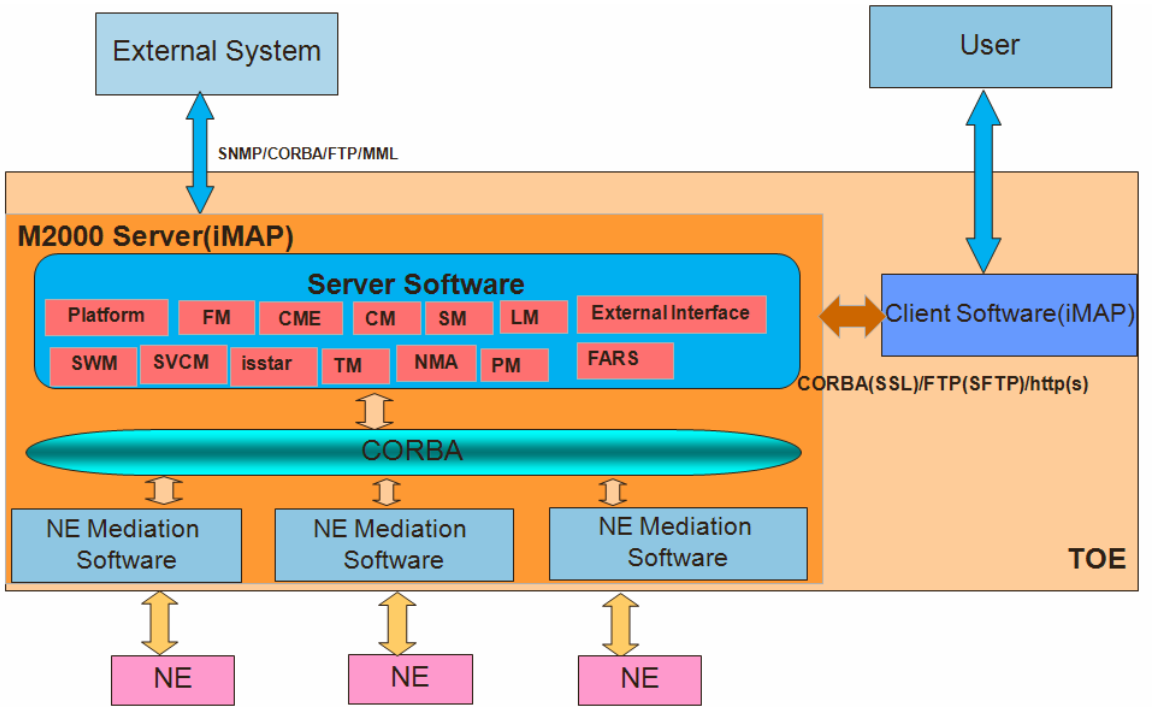

Figure 1:TOE network structure

1.3.3 Non TOE Hardware and Software

This section describes the Supported Platforms and hardware Environment of the iManager M2000.The physical environment includes the following parts:

- The Server
- The Client

The server provides physical platform for server software and NE mediation software of the TOE. The physical structure of M2000 server is composed of a third-party disk array and a workstation with either Unix or Linux operating system (OS) and database software.

The server can support Sun platform and advanced telecom application environment (ATAE):

- Sun platform: Sun workstation with Solaris OS and Sybase database
- ATAE platform: ATAE blade server with Suse Linux OS and Oracle database

The server has different physical structure, as followed:

- Single-server system on Sun platform
- Sharing load system on Sun platform
- High availability system on Sun platform
- Single-server system on ATAE platform
- Sharing load system on ATAE platform

Figure 2 shows the physical environment of M2000 single-server system, which is the typical environment.

The client provides physical platform for client software of the TOE. The physical structure is composed of Private Computer with Windows OS software.

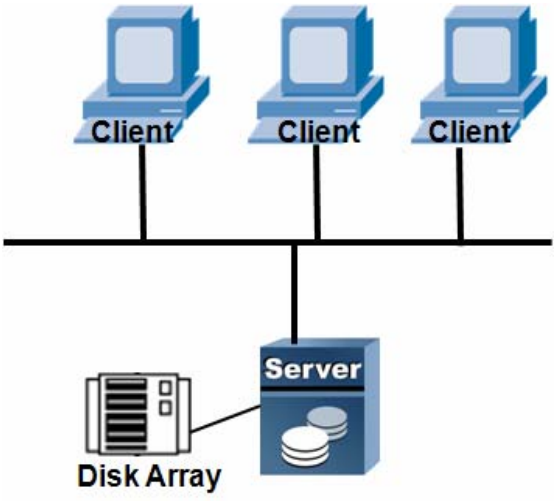

Figure 2:TOE Physical Environment

Table 1 shows the typical configuration of the hardware and software for the TOE physical environment.

Device Type	**Device Description**	**Quantity**	**Configuration Description**
Server	Server Module(SUN M4000, 4 CPU, Single Server)	1	Number of CPUs: 2 CPU clock frequency: 2.53 GHz Memory: 16 GB Local disk: 2 x 146 GB Disk array: one S2600 (each S2600 consists of twelve 450 GB hard disks) Operating system: Solaris 10 Database: Sybase 15.0.2
PC	Client	1	CPU: E5300 or above Memory: 2 GB Hard disk: 160 GB

			Accessories: DVDRW-Integrated Ethernet adapter-Integrated audio adapter-Built-in sound box-19" LCD Operating system: Windows XP professional (or a later version)

Table 1:Hardware and software

The NEs which can be managed by the TOE and supports different communication protocols with the TOE, are part of the environment of the TOE.

21 During the evaluation, the NEs tested have been SAE-HSS and BSC6900 UMTS.

1.4 TOE description

1.4.1 TOE Definition Scope

22 This section will define the scope of the iManager M2000 to be evaluated.The iManager M2000 is developed basing on the iMAP software platform.

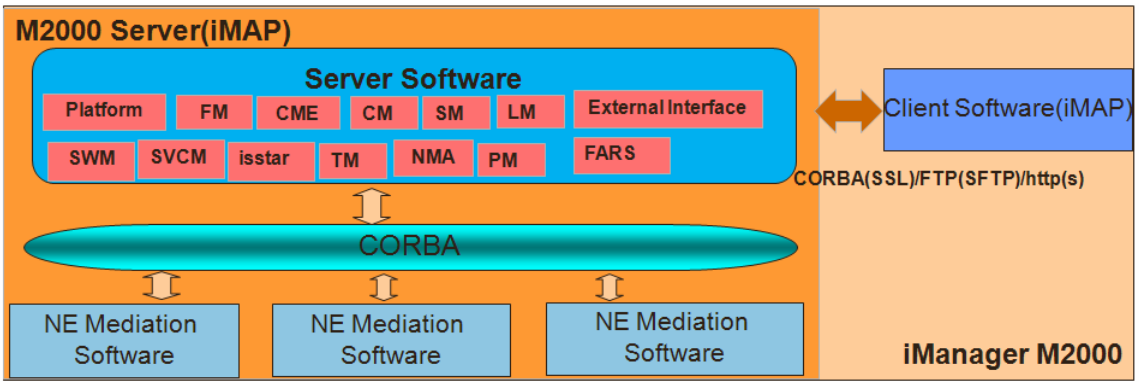

Figure 3:TOE Scope

As illustrated in the figure above, the TOE consists of three parts to support centralized network management.

- NE mediation software
- Server software
- Client software

Note that the **NE mediation software** is to communicate with network elements and adapt the different interface for different network elements. The interface with network elements includes such as SSL connection, file transfer protocol(FTP), FTPS. The adapted network elements can include the elements of the CN, IMS, GSM, WCDMA, SAE, CDMA, WiMAX and LTE networks, which are developed by Huawei.

During the evaluation, the NEs mediation software tested have been SAE-HSS and BSC6900 UMTS.

The **server software** is to provide the services for client software, and external

interfaces for the external system.

The **client software** is responsible for providing Graphic User Interface (GUI) to access to M2000 server.

23 The **iMAP** is operation and support system (OSS) platform that has server and client software. It contains a **Software Bus** layer for communications between different system components, including CORBA, Event Manager (EM) for event broadcasting. It also provides security management, audit management, topology management, alarm management, other non-TSF and TSF sub-systems.

24 Moreover, the component CM Express is also included in the TOE.

1.4.2 Environment

The environment for TOE comprises the following components:

- The underlying platform for the evaluation is limited to single-server system on Sun Platform;The databases and tools(including such as sftp/ftp/ftps server) should be contained in the underlying platform.
- Network element developed by Huawei, providing secure sockets layer (SSL) connect and supporting file transfer protocol over SSL (FTPS).
- The third party system or tools providing connection to the TOE through external interface including the protocols such as SNMP, CORBA, FTP, MML.
- Remote PCs used by administrators to install the client part of the TOE and connect to the TOE for access through GUI interfaces.
- Remote PCs used by administrators to connect to the TOE for access to the command line interface through interfaces on Sun workstation within the TOE via a secure channel enforcing secure shell (SSH).
- Physical networks, such as Ethernet subnets, interconnecting various networking elements.
- Firewall: all the accesses to the TOE are performed through a firewall. Only the following communications are allowed by the firewall:
    - TCP interface(with SSL enabled): this interface is used in communication between GUI client and the server of the TOE (Corba and XRPC protocol).
    - AT&NIC Website.
    - OMMonitor communication.
    - SFTP interface: the TOE use this interface to communicate between the GUI and the Server.
    - SNMPv3 interface: the TOE use this interface to communicate with upper management system and act as SNMPv3 client.
    - CAU interface for updating the software.
    - Hedex interface for providing on-line help.
    - Communications with the NEs.

1.4.3 Configuration

Based on TOE scope described so far, a list of configuration is to be added:

- SSL connection and secure file transfer protocol (SFTP) for file transfer via the GUI interface between M2000 server and client should be activated.
- Encrypted transmission between network elements and M2000 should be activated.
- For secure transmission to M2000 server via GUI, the SSL should be used to connect the M2000 server.

2 CC conformance claims

25 This ST is *CC Part 2 conformant* [CC] and *CC Part 3 conformant* [CC]. The CC version of [CC] is 3.1R3.

This ST is EAL3-conformant + ALC_CMC.4 + ALC_CMS.4 as defined in [CC] Part 3.

The metohology to be used for evaluation is CEM3.1 R3

No conformance to a Protection Profile is claimed.

3 Security Problem Definition

3.1 Assumptions

A.Physical The TOE is operated in a physically secure and well managed environment.

It is assumed that the software platform of the TOE including such as Solaris OS, Sybase are protected against unauthorized physical access.

It is assumed that the database Sybase is protected against data file damage.

It is assumed that secured connections to Solaris OS are always enabled to access to Sun server.

A.NetworkElement It is assumed that the managed network elements can support the SSL connection with the TOE, and the private interface defined by Huawei.

A.NetworkSegregation It is assumed that the network interface in the TOE will be accessed only through sub-network where the TOE hosts. The sub-network is separate from the application (or, public) networks. The communications with the TOE are performed through a firewall. See section 1.4.2 Environment for more information

A.Connection It is assumed that the connection between the external system (also NEs) and the TOE is secured in a trusted network which is protected against attacks.

A.AdministratorBehaviour It is assumed that the super user admin and the users that belong to the SMManagers and Administrator groups will behave correctly and will not perform any harmful operation in the TOE. Also, the users of the underlying operating system.

3.2 Threats

The threats described in this chapter are addressed by the TOE.

3.2.1 Assets and Agents

Asset	Description	Type of Data
TSF data	The integrity and confidentiality of TSF data (such as user account information and passwords, audit records, etc), should be protect against the threat agents.	User data
OM data	The confidentiality and integrity of the OM data of NE including such as	OM data

	configuration data should be protected against the threat agents	

Table 2:Assets

Agent	Description
Attacker	An external attacker, who is not user of the TOE, accesses to the TOE and modifies the information and compromises the confidentiality of the TSF and OM data.
Eavesdropper	An eavesdropper, who has access to communication channel over which the OM data and TSF data are transferred, is able to intercept, and potentially modify or re-use information assets and TSF data that are exchanged during network transfer.
Unauthorized user	An authenticated user of the TOE gains unauthorized accesses to the TOE and compromises the confidentiality and the integrity of the TSF data and OM data or performs non-authorized operations in the NEs.

Table 3:Agents

3.2.2 Threats addressed by the TOE

I. T.UnauthenticatedAccess

Threat: T.UnauthenticatedAccess	
Attack	An attacker who is not a user of the TOE, gains access to the TOE, modifies and compromises the confidentiality of the TSF data and the OM data.
Asset	TSF data, OM data
Agent	Attacker

II. T.UnauthorizedAccess

Threat: T.UnauthorizedAccess	
Attack	An unauthorized user may gain unauthorized accesses to the TOE and compromises the confidentiality and the integrity of the TSF data and OM data. Also perform non-authorized operations in the NEs.
Asset	TSF data, OM data
Agent	Unauthorized user

III. T. Eavesdrop

Threat: T.Eavesdrop

Attack	An eavesdropper (remote attacker) in the management network served by the TOE is able to intercept, and potentially modify or re-use information assets that are exchanged between TOE and NEs, between the client and server of the TOE and between the server and the SNMP client.
Asset	OM data; TSF data
Agent	Eavesdropper

3.3 Organizational Security Policy

- **P.Audit**

The TSF shall be able to generate an audit record of the auditable events, which associate with the identity of the user that caused the event. The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

4 Security Objectives

4.1 Security Objectives for the TOE

The following objectives must be met by the TOE:

- **O.Communication** The TOE must implement logical protection measures for network communication between the TOE and network elements from the operational environment, also for the communication between the GUI and the server of the TOE and between the server and the SNMP client.
- **O.Authorization** The TOE shall implement different authorization levels that can be assigned to administrators in order to restrict the functionality that is available to individual administrators, including limitations to the session establishment. Also limitation to the actions that may be performed in a Network Element.
- **O.Authentication** The TOE must authenticate users of its user access; The TOE shall provide configurable system policy to restrict user session establishment.
- **O.Audit** The TOE shall provide functionality to generate and review audit records for security-relevant administrator actions.

4.2 Objectives for the Operational Environment

- **OE.NetworkElements** The operational environment shall ensure that the managed network elements can support the SSL connection with the TOE, and the private interface defined by Huawei .
- **OE.Physical** The TOE (i.e., the complete system including attached peripherals, such as Sun workstation, disk array) shall be protected against unauthorized physical access.
- **OE.NetworkSegregation** The operational environment shall provide protection to the network in which the TOE hosts by separating it from the application (or public) network. A firewall shall be installed in the environment.
- **OE.NetworkCommunication** The operational environment should provide secured network for the communication between the TOE and external systems.
- **OE.Database** The operational environment shall protection to the database for storage of security data against unauthorized physical access.
- **OE.AdministratorBehaviour** The super user admin and the users that belong to the SMManagers and Administrator groups will behave correctly and will not perform any harmful operation in the TOE. Also, the users of the underlying operating system.

4.3 Security Objectives Rationale

4.3.1 Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective is at least covered by one threat or policy.

Objective	Threat/Policy
O.Communication	T.Eavesdrop T.UnauthenticatedAccess T.UnauthorizedAccess
O.Authentication	T.UnauthenticatedAccess T.UnauthorizedAccess
O.Authorization	T.UnauthorizedAccess
O.Audit	P.Audit

Table 4:Mapping Objectives to Threats

The following table provides a mapping of the objectives for the operational environment to assumptions, threats and policies, showing that each objective is at least covered by one assumption, threat or policy.

Environmental Objective	Threat / Assumption
OE. NetworkElements	A. NetworkElement
OE.Physical	A.Physical T.UnauthenticatedAccess T. UnauthorizedAccess
OE.NetworkSegregation	A.NetworkSegregation
OE.NetworkCommunication	A.Connection
OE.Database	A.Physical T.UnauthenticatedAccess T. UnauthorizedAccess
OE. AdministratorBehaviour	A.AdministratorBehaviour

Table 5:Mapping Objectives for the Environment to Threats/Policies, Assumptions

4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat:

Threat/Policy	Rationale for security objectives
T.UnauthenticatedAccess	The threat of unauthenticated access to the TOE is countered by requiring the TOE to implement an authentication mechanism for its users (O.Authentication) , the threat also is countered by requiring encrypted communications (O.Communication). And the threat is countered by the OE.Physical and OE.Database.
T.UnauthorizedAccess	The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism checking the operations that may be performed in the TOE and also in the NEs (O.Authorization), the threat also is countered by requiring encrypted communications (O.Communication) and authenticating the users in the TOE (O.Authentication). And the threat is countered by the OE.Physical and OE.Database.
T.Eavesdrop	The threat of eavesdropping is countered by requiring security communications: - Securing network communication to M2000 server - Through SSL protocols between M2000 server and NEs - Ciphering the communications between the server and the SNMP client (O.Communication).
P.Audit	The policy of auditing is for generating, storing and viewing the audit trails(O.Audit).

Table 6:Sufficiency analysis for threats/polices

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the

intended usage is supported:

Assumption	Rationale for security objectives
A. NetworkElement	The assumption that the managed network elements can support the SSL connection with the TOE, and the private interface defined by Huawei is addressed by requiring just this in OE.NetworkElement.
A.Physical	The assumption that the TOE will be protected against unauthorized physical access is expressed by a corresponding requirement in OE.Physical and a corresponding database in OE.Database.
A.NetworkSegregation	The assumption that the TOE is not accessible via the application networks hosted by the networking device is addressed by requiring just this in OE.NetworkSegregation and installing a firewall.
A.Connection	The assumption that the communication between the TOE and external systems (also NEs) is addressed by OE.NetworkCommunication.
A.AdministratorBehaviour	The assumption that super user admin and the users that belong to the SMManagers and Administrator groups and the users of the underlying operating system will behave correctly and will not perform any harmful operation is addressed by OE.AdministratorBehaviour.

Table 7:Sufficiency analysis for assumptions

5 Security Requirements for the TOE

5.1 Security Requirements

5.1.1 Security Audit (FAU)

I. **FAU_GEN.1 Audit data generation**

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [selection, choose one of: not specified] level of audit; and
c) [assignment:

1. user login, logout
2. user account management
    i. user account create, delete, modify
    ii. change user password
    iii. grant access right to user account
3. user group(role) management
    i. user group create, delete, modify
    ii. grant access right to user group
4. security policy management
    i. modify password policy
    ii. modify user account policy
5. user session management
    i. Kick out individual user session
6. ACL management
    i. ACL create, delete, modify
    ii. Specify ACL for individual user account.
7. Operation set and Device set management
8. SSL connection management
9. MML command operations
10. Log management].

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: none].

II. FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

III. FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [assignment: users of the security administrators SMManagers and the super user admin] with the capability to read [assignment: all information] 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.

IV. FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

V. FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [assignment: selection] of audit data based on [assignment: filter condition set of audit fields including operator, terminal, outcome, level, generation time segment and activity name].

5.1.2 User Data Protection (FDP)

I. FDP_ACC.2/iMAP Complete access control

26 FDP_ACC.2.1 The TSF shall enforce the [assignment: iMAP access control policy] on [assignment: users as subjects, domain as objects; The domain as objects can contain network element, device set, network element types, and sub networks].

27 FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

II. FDP_ACC.2/MML Complete access control

28 FDP_ACC.2.1 The TSF shall enforce the [assignment: MML command access control policy] on [assignment: users as subjects, network elements as objects].

29 FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

III. FDP_ACF.1/iMAP Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [assignment: iMAP access control policy] to objects based on the following: [assignment:

a) Users and their following security attributes:

i. User ID
ii. User Group

b) Objects, and their attributes:
i. Object Id].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:
An operation from GUI shall be authorized to a subject wanting to execute an operation over an object if this operation right has been granted by the security administrators SMManagers or the super user admin to the User ID or User Group to the specific Object Id and operation.].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment:none].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment:none].

IV. FDP_ACF.1/MML Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [assignment: MML command access control policy] to objects based on the following: [assignment:

a) Users and their following security attributes:
i. User ID
ii. User Group

b) Network Element and their following security attributes:
i. MML Command Group
].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: An operation shall be authorized to a subject wanting to execute an operation over a Network Element if if this operation right has been granted by the security administrators SMManagers or the super user admin to the User ID or User Group for the specific MML Command Group].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment:none].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based

on the following additional rules: [assignment:none].

5.1.3 Identification and Authentication (FIA)

I. FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [selection: an administrator configurable positive integer within[assignment: 1 to 99]] unsuccessful authentication attempts occur related to [assignment: the last successful authentication of the user name].
FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: met], the TSF shall [assignment: lock the authentication user for default 30 minutes].

II. FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment:

a) User ID
b) User group
c) Password
d) Time segment for login
e) ACL
f) Maximum online sessions
g) Disable status
h) Password validity period (days)].

III. FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet: [assignment: For user's password, they are case sensitive, contain no whitespace, not contain the user name, the whole word is not in password dictionary and it is not a repeated string. The length of password should be more than 8 characters].

IV. FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [assignment: upload files through the web AT&NIC] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

V. **FIA_UID.1 Timing of identification**

FIA_UID.1.1 The TSF shall allow [assignment: upload files through the web AT&NIC] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.4 Security Management (FMT)

I. **FMT_MSA.1/iMAP Management of security attributes**

FMT_MSA.1.1 The TSF shall enforce the [assignment: iMAP access control policy] to restrict the ability to [selection: query, modify [assignment: none]] the security attributes [assignment: all the security attributes defined in FDP_ACF.1/iMAP] to [assignment: the security administrators SMManagers and the super user admin].

II. FMT_MSA.1/MML Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [assignment: MML access control policy] to restrict the ability to [selection: query, modify [assignment: none]] the security attributes [assignment:user Id, user group and MML command group] to [assignment: the security administrators SMManagers and the super user admin].

III. **FMT_MSA.3/iMAP Static attribute initialization**

FMT_MSA.3.1 The TSF shall enforce the [assignment: the iMAP access control policy] to provide [selection: restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 The TSF shall allow [assignment: the security administrators SMManagers and the super user admin] to specify alternative initial values to override the default values when an object or information is created.

I. **FMT_MSA.3/MML Static attribute initialization**

FMT_MSA.3.1 The TSF shall enforce the [assignment: MML access control policy] to provide [selection: restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 The TSF shall allow [assignment: the security administrators SMManagers and the super user admin] to specify alternative initial values to override the default values when an object or information is created.

II. **FMT_SMF.1 Specification of Management Functions**

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

a) authentication, authorization
b) ACL policy
c) user management
d) management of Command Groups
e) audit management for export
f) SSL connection management
g) Configuration of the time interval of user inactivity for terminating an interactive session
h) Security policy management].

III. **FMT_SMR.1 Security roles**

FMT_SMR.1.1 The TSF shall maintain the roles: [assignment**:**

i. the super user admin
ii. the default groups:

SMManagers,
Administrators,
Operators,
Guest].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.5 Protection of the TSF (FPT)

I. **FPT_ITT.1 Basic internal TSF data transfer protection**

FPT_ITT.1.1 The TSF shall protect TSF data from [selection: disclosure] when it is transmitted between separate parts of the TOE.

5.1.6 TOE access (FTA)

I. **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 [assignment: number defined by security administrators, none by default] sessions per user.

II. **FTA_TSE.1 TOE session establishment**

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [assignment:

a) The following security attributes associated by users:

i. date and time
ii. ACL
iii. Maximum online sessions
iv. Disable status

b) System security policy

i. System login mode
ii.].

5.1.7 Trusted Path/Channels

I. 5.1.7.1 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and **[selection:** remote **]** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **[selection:** disclosure**.]**

FTP_TRP.1.2 The TSF shall permit **[selection:** remote **]** users to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for **[selection: [assignment: Antenna Tune** for antenna management and **Network Information Collector (NIC)** for collecting informations about connection status of NEs in the AT&NIC Website**].]**

5.1.8 Cryptographic operation (FCS)

I. FCS_COP.1/SNMP Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: communication channel encryption/decryption] in accordance with a specified cryptographic algorithm [assignment: DES] and cryptographic key sizes [assignment: 56 bits] that meet the following: [assignment: None].

Application Note: DES algorithm is used to encrypt/decrypt the communication between the server and a SNMP client.

II. FCS_COP.1/NE Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: communication channel encryption/decryption] in accordance with a specified cryptographic algorithm [assignment: the algorithms supported by SSL] and cryptographic key sizes [assignment: the key sizes supported by SSL] that meet the following: [assignment: None].

Application Note: The algorithms supported by SSL are used to encrypt/decrypt the communication between the server and a NEs.

III. FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: the algorithms supported by SSL] and specified cryptographic key sizes [assignment: the key sizes supported by SSL] that meet the following: [assignment: None].

5.2 Security Functional Requirements Rationale

5.2.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Security Functional Requirements	Objectives
FAU_GEN.1	O.Audit
FAU_GEN.2	O.Audit
FAU_SAR.1	O.Audit
FAU_SAR.2	O.Audit
FAU_SAR.3	O.Audit
FDP_ACC.2/iMAP	O.Authorization
FDP_ACC.2/MML	O.Authorization
FDP_ACF.1/iMAP	O.Authorization
FDP_ACF.1/MML	O.Authorization
FIA_AFL.1	O.Authentication
FIA_ATD.1	O.Authentication O.Authorization
FIA_SOS.1	O.Authentication
FIA_UAU.1	O.Authentication O.Authorization
FIA_UID.1	O.Audit O.Authentication O.Authorization
FMT_MSA.1/iMAP	O.Authorization
FMT_MSA.1/MML	O.Authorization

FMT_MSA.3/iMAP	O.Authorization
FMT_MSA.3/MML	O.Authorization
FMT_SMF.1	O.Audit O.Authentication O.Authorization O.Communication
FMT_SMR.1	O.Authorization
FPT_ITT.1	O.Communication
FTA_MCS.1	O. Authentication
FTA_TSE.1	O. Authentication
FCS_COP.1/NE	O.Communication
FCS_CKM.1	O.Communication
FCS_COP.1/SNMP	O.Communication
FTP_TRP.1	O.Communication

Table 8:Mapping SFRs to objectives

5.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Security objectives	Rationale
O.Audit	The generation of audit records is implemented by FAU_GEN.1. Audit records are supposed to include user identities (FAU_GEN.2) where applicable, which are supplied by the identification mechanism (FIA_UID.1). Audit records are stored in database, and are filtered to read and search with conditions, restricted audit review requires authorised users (FAU_SAR.1, FAU_SAR.2, FAU_SAR.3). Management functionality for the audit mechanism is spelled out in FMT_SMF.1.
O.Communication	Communications security is implemented by the establishment of a secure communications channel between TOE parts in FPT_ITT.1, and a inter-TSF trusted channel between the TOE and other NEs is implemented ciphering the communications in FCS_COP.1/NE. The key is generated for the communication following SSL protocol (FCS_CKM.1). Also a inter-TSF trusted channel between the TOE and SNMP clients is implemented ciphering the communications in FCS_COP.1/SNMP.

	The communication to the AT&NIC Website is performed through a secure channel (FTP_TRP.1). Management functionality to configure the trusted channel for NEs communication is provided in FMT_SMF.1.
O.Authentication	User authentication is implemented by FIA_UAU.1 and supported by individual user identifies in FIA_UID.1. The necessary user attributes (passwords) are spelled out in FIA_ATD.1. The authentication mechanism supports authentication failure handling (FIA_AFL.1), restrictions as to the validity of accounts for logon (FTA_TSE.1), and a password policy (FIA_SOS.1). Management functionality is provided in FMT_SMF.1. Basic limitation on multiple concurrent sessions of the same user is met by FTA_MCS.1. The session establishment shall be denied based on security attributes (FTA_TSE.1).
O.Authorization	The requirement for access control is spelled out in FDP_ACC.2/iMAP, and the access control policies are modeled in FDP_ACF.1/iMAP for accessing the M2000 server. The requirement for access control is spelled out in FDP_ACC.2/MML, and the access control policies are modeled in FDP_ACF.1/MML for accessing the NEs. Unique user IDs are necessary for access control provisioning (FIA_UID.1), also authenticating the users (FIA_UAU.1) and user-related attributes are spelled out in FIA_ATD.1. Access control is based on the definition of roles as subject and functions as object(FMT_SMR.1). Management functionality for the definition of access control policies is provided (FMT_MSA.1/iMAP, FMT_MSA.3/iMAP, FMT_MSA.1/MML,FMT_MSA.3/MML, FMT_SMF.1).

Table 9: SFR sufficiency analysis

5.2.3 Security Requirements Dependency Rationale

Dependencies within the EAL3 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again.

The security functional requirements in this Security Target do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in this Security Target introduce dependencies on any security functional requirement.

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies:

Security Functional Requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	Not resolved. The audit time is depended on the reliable time stamp. Reliable time stamp is depended on external time sources
FAU_GEN.2	FIA_UID.1	FIA_UID.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FDP_ACC.2/iMAP	FDP_ACF.1/iMAP	FDP_ACF.1/iMAP
FDP_ACC.2/MML	FDP_ACF.1/MML	FDP_ACF.1/MML
FDP_ACF.1/iMAP	FDP_ACC.2/iMAP FMT_MSA.3/iMAP	FDP_ACF.1/iMAP FMT_MSA.3/iMAP
FDP_ACF.1/MML	FDP_ACC.2/MML FMT_MSA.3/MML	FDP_ACF.1/MML FMT_MSA.3/MML
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	None	
FIA_SOS.1	None	
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UID.1	None	
FMT_MSA.1/iMAP	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.2/iMAP FMT_SMR.1 FMT_SMF.1
FMT_MSA.1/MML	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.2/MML FMT_SMR.1 FMT_SMF.1
FMT_MSA.3/iMAP	FMT_MSA.1/iMAP FMT_SMR.1	FMT_MSA.1/iMAP FMT_SMR.1
FMT_MSA.3/MML	FMT_MSA.1/MML FMT_SMR.1	FMT_MSA.1/MML FMT_SMR.1
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_ITT.1	None	
FTA_MCS.1	FIA_UID.1	FIA_UID.1
FTA_TSE.1	None	

FCS_COP.1/NE	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 Not resolved. The key is not zeroized given that it is not accessible for any attacker.
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1 Not resolved. The key is not zeroized given that it is not accessible for any attacker.
FTP_TRP.1	None	
FCS_COP.1/SNMP	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Not resolved. The key used to cipher the communication is configured in the TOE during the installation process. Therefore, no mechanism is provided in the TOE neither to import the key nor to generate it. The key is never zeroized given that it is necessary for the operative of the TOE.

Table 10:Dependencies between TOE Security Functional Requirements

5.3 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 components as specified in [CC] Part 3 + ALC_CMC.4 + ALC_CMS.4. The following table provides an overview of the assurance components that form the assurance level for the TOE.

Assurance class	Assurance components
Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_OBJ.2 Security objectives
	ASE_TSS.1 TOE summary specification
Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability assessment	AVA_VAN.2 Vulnerability

Table 11:Security Assurance Components

5.4 Security Assurance Requirements Rationale

The evaluation assurance level has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

6 TOE Summary Specification

6.1 TOE Security Functionality

6.1.1 User Role management

The TOE can support role management, and have some default roles, which have predefined access control policy. The default roles are Administrators, SMManagers, Operators and Guests. The role Administrators is to administer the TOE; the role SMManagers is the security role of the TOE, who can complete the security management of TSF data, user management, audit review and authorization.

The TOE also has a default and super user admin, who belongs to the role Administrators and SMManagers. The super user admin can complete all the functions, including security functions and administering functions.

Note: The role is the same as user group in TOE.

(FMT_MSA.1/iMAP, FMT_MSA.3/iMAP, FMT_SMF.1, FMT_SMR.1)

6.1.2 Authentication

The TOE can identify administrators by a unique ID and enforces their authentication before granting them access to any TSF management interfaces.

The TOE authenticates the users of its user interfaces based on individual user IDs and passwords, extended security attributes associated by user ID, which have login start and end time, ACL, maximum online sessions. The individual user IDs and passwords are mandatory when authenticated, extended security attributes shall be enforced to authenticate if having been configured by the security administrator SMManagers.

The passwords should meet the defined password policy; otherwise the input of password shall be refused. When the user use an expired password to login, the system will refuse the login request, the user must request the administrator to reset his password (the Administrator can deactivate the password expiration policy).

User IDs are unique within the TOE and stored together with associated passwords and other attributes including extended security attributes in the TOE's configuration database. If the user is in disable status, its login will be refused.

Authentication based on security attributes is enforced prior to any other interaction with the TOE for all interfaces of the TOE, typically via the client of TOE.

The TOE also can provide the authentication failure handling mechanism that the TSF shall terminate the session of the authentication user and lock the authentication user for default 30 minutes when three continuing and unsuccessful authentication attempts occur.

The number of online sessions shall not exceed the maximum sessions, otherwise the user login request after the maximum online sessions shall be refused by TOE.

(FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UID.1, FTA_TSE.1, FTA_MCS.1)

6.1.3 Access control

The TOE enforces an authorization policy by defining access rights that are assigned to users and roles by the security roles or the super user admin.

The TOE shall enforce the iMAP access control policy on users and groups as subjects, domain as objects, functional operations issued by the subjects targeting the objects. The domain as objects shall define the scope of network elements. The network elements not contained in domain shall not be performed the operations on.

The iMAP access control bases on users or groups and objects; And the security attribute object id of objects shall have the domain, including specified network elements, device types and network elements contained in subnetwork.

The iMAP access control is used to identify all the operations over objects through M2000 client if the operation rights have been assigned by security administrators SMManagers or the super user admin, the operations except executing MML commands to accessed NEs.

(FDP_ACC.2/iMAP, FDP_ACF.1/iMAP, FMT_SMR.1, FMT_MSA.1/iMAP, FMT_MSA.3/iMAP)

The MML commands defined by the managed NEs, are used to directly perform the operations on the corresponding NE through the channel between the NE and TOE. The access rights with MML command group (containing some MML commands) can be assigned to users and roles. The MML command access control is only used to identify the commands through the MML client function of the M2000 client.

And before any operations through the client of TOE, the access rights related with these operations shall be authenticated with the token of corresponding user session.

(FDP_ACC.2/MML, FDP_ACF.1/ MML, FMT_SMR.1, FMT_MSA.1/ MML, FMT_MSA.3/ MML)

6.1.4 IP-base ACL

The iMAP platform of TOE can offer a feature access control list (ACL) based on IP address for controlling which terminals can access to the TOE through the client of TOE. The ACL is based on IP address, the security role SMManagers and the super user admin can specify individual IP address or IP address range in ACL of a specified user ID, the user then only can login to the TOE from terminals whose IP address is in the range of ACL.

(FMT_SMF.1, FTA_TSE.1)

6.1.5 Encrypted communication

The TOE support encrypted transmission between NEs and TOE, client and server of the TOE. It provides secure protocol, such as SSL, FTPS and SFTP, for the data transmission.

- The secured connection between M2000 client and M2000 server includes message channel. The SSL connection is used for message channel, and https protocol can be used between Web explorer and M2000 server. If the X.509

certificates are deployed on client and server, the SSL connect with authentication can be used. The secured connection can be initiated from M2000 client if the SSL connection is selected on M2000 client by user. (FPT_ITT.1)

- The encrypted communication also includes message channel between network elements and TOE. The SSL connection is used for message channel. The key used for cipher the communication between the NEs and M2000 is generated following the SSL protocol (FCS_CKM.1).The SSL connection can be used with mutual authentication based on X.509 certificates. If the SSL connection between NEs and TOE is configured through M2000 client, the TOE will initiate the SSL connection with NEs. (FCS_COP.1/NE)
- SNMPv3 connections between the server and external SNMP clients (FCS_COP.1/SNMP)
- The TOE also provides a secure channel for the communication to the AT&NIC Website.(FTP_TRP.1)

6.1.6 User session management

The TOE also offers the user sessión management function. The function includes the following functions:

1) Session Locking

The lock policy of the terminal has automatic lock and manual lock. The client will be locked automatically without operations during the time interval until the unlock operation is initiated manually by user. The time interval can be configured, whose default value is 3 minutes.

And also the lock of the client can be initiated manually by user.

2) Session establishment

The session establishment will be denied basing on the below policy:

a) Users and their following security attributes:

i. Time segment for login, which means that the user shall login the TOE with time segment.

ii. ACL, addressed in the previous section.

iii. Maximum online sessions, which mean that the number of online sessions shall not exceed the maximum sessions, otherwise the user login request after the maximum online sessions shall be refused by TOE.The default is none.

iv. Disable status, which means the user can not login the TOE if the user in disable status.

b) System security policy, which prior to the security attributes of individual user

i. System login mode, which have two modes, the multi-user login mode and the sinlge-user login mode. The single-user login mode is a special mode. When system login mode is the single-user login mode, the TOE shall refuse all the logins including online sessions and login requests except the login of the super user admin. The multi-user login mode is a

normal mode and has no special limits.

(FTA_MCS.1, FTA.TSE.1)

6.1.7 Auditing

The TOE can generate audit records for security-relevant events, including the following security-relevant events:

a) user login, logout
b) user account management
1. user account create, delete, modify
2. change user password
3. grant access right to user account
c) user group(role) management
1. user group create, delete, modify
2. grant access right to user group
d) security policy management
1. modify password policy
2. modify user account policy
e) user session management
1 Kick out individual user session
f) ACL management
1 ACL create, delete, modify
2 Specify ACL for individual user account
g) Operation set and Device set management
h) SSL connection management
i) MML command operations
j) Log management

The audit record has the following information: activity name, level, user id, operation type, operation date and time, terminal, object, operation result, details.

The audit review can be completed with filter on M2000 client by the security role SMManager and the super admin, any user can not delete and modify the audit records.

When the exceeding three unsuccessful login attempts are detected since the last successful login, The TOE will generate an alarm.

The audit record is stored in database, and exported into file if the size of audit record exceeds the configured maximum size.

(FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3)

6.1.8 Security management function

The TOE offers management functionality for its security functions, where appropriate. This is partially already addressed in more detail in the previous sections of the TSS, but includes the following definition of security attributes:

a) Users and their following security attributes:

i. User ID, which is a user identifier, defined as user name in TOE.

ii. User Group, which is the same as role definition.

iii. Password, which should meet the predefined password policy, is encrypted with AES-128 and stored in database.

iv. Time segment for login, addressed in the previous section.

v. ACL, addressed in the previous section.

vi. Maximum online sessions, addressed in the previous section.

vii. Disable status, addressed in the previous section.

b) System security policy, which prior to the security attributes of individual user

i. System login mode, addressed in the previous section.

ii. Password policy, which has basic parameters and advanced parameters. Basic parameters have follow items: Min. Length of common user password, Min. Length of super user password, Max. Length of password, Max. period for password repetition (months), Password validity period (days), Minimum validity period of the password (days), Number of days warning given before password expiry, The Password Cannot Be Similar to History Passwords.

Advanced parameters have such as Min. Different characters between new and old password, Min. Letter, Min. Lowercase, Min. Numbers.

iii. Account policy, which has such as Illegal login times which caused locked, Super user not allowed to be locked. All the users should meet the account policy defined in TOE.

(FMT_MSA.1/iMAP, FMT_MSA.3/iMAP, FMT_SMF.1)

7 Abbreviations, Terminology and References

7.1 Abbreviations

CC	Common Criteria
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
PP	Protection Profile
SFR	Security Functional Requirement

7.2 Terminology

30 This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

31 Administrator: An administrator is a user of the TOE who may have been assigned specific administrative privileges within the TOE. This ST may use the term administrator occasionally in an informal context, and not in order to refer to a specific role definition – from the TOE's point of view, an administrator is simply a user who is authorized to perform certain administrative actions on the TOE and the objects managed by the TOE.

32 Operator See User.

33 User: A user is a human or a product/application using the TOE.

7.3 References

34 [CC] Common Criteria for Information Technology Security Evaluation. Part 1-3. July 2009. Version 3.1 Revision 3.

35 [CEM] Common Methodology for Information Technology Security Evaluation. July 2009. Version 3.1 Revision 3.