iManager U2000 Security Target

Version: 1.6
Last Update: 2014-12-04
Author: Huawei Technologies Co., Ltd.

Table of Contents

Table of contents

List of figures

Author

Version	Date	**Author**	Changes to previous version
0.1	2012-04-29	Wen WenJing	First release
0.2	2014-04-30	Wen WenJing	Review and update
0.3	2014-05-04	Lin Jing	Review and update
0.4	2014-05-04	Wen WenJing	Review and update
0.5	2014-05-05	Wen WenJing	Review and update
0.6	2014-05-06	Wen WenJing	Review and update
0.7	2014-05-07	Wen WenJing	Review and update
0.8	2014-05-08	Wen WenJing	Review and update
0.9	2014-05-09	Wen WenJing	Review and update
1.0	2014-07-24	Wen WenJing	Review and update
1.1	2014-08-04	Wen WenJing	Review and update
1.2	2014-08-13	Wen WenJing	Review and update
1.3	2014-09-28	Wen WenJing	Update according to EORs
1.4	2014-09-29	Wen WenJing	Final
1.5	2014-10-10	Wen WenJing	Update Guidance
1.6	2014-12-04	Wen WenJing	Update according to EORs

1 Introduction

This Security Target is for the evaluation of Huawei iManager U2000.

1.1 ST Reference

Title: Huwei iManager U2000 Security Target

Version: V1.6

Author: Huawei Technologies Co., Ltd.

Publication date: 2014-12-04

1.2 TOE Reference

TOE name: Huawei iManager U2000

TOE version: V100R009C00SPC301

TOE Developer: Huawei Technologies Co., Ltd.

TOE release date: 2014-05-21

1.3 TOE Overview

Huawei’s iManager U2000 (U2000) Element Management system is a software system which provides centralized operation and maintenance for Huawei’s fixed network element management solution. The U2000 manages the fixed network element including the Transport, Access and IP equipment, and provides external interfaces for interoperability with other systems. The core of Huawei iManager U2000 is the iMAP Platform, U2000 V100R009C00SPC301 is base on the iMAP Platform.

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

1.3.1 TOE usage and major security features

U2000 is the software to manage fixed network elements. 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 U2000 focuses on continuous efforts that telecom operators have made for network operation and maintenance and inherits the existing OM experience.

The major security features implemented by Huawei iManager U2000 and subject to evaluation are:

- User Role management
- Authentication
- Access Control
- Auditing
- IP-based ACL
- Encrypted transmission
- User session management
- Security function management

1.3.2 TOE Type

The U2000 is a centralized fixed network management software, containing a client and a server. The U2000 can manage NEs after the corresponding NE management component is installed. The U2000 adopts an open structure so that it can manage the devices such as Multi-Service Transmission Platform(MSTP), wavelength division multiplexing (WDM), optical transport network (OTN), Microwave, Router, Switch, Packet Transport Network(PTN), multiservice access node(MSAN), digital subscriber line access multiplexer(DSLAM) and fiber to the x(FTTx).

The protocols applied for different NEs are listed as followed:

- SNMPv3/SSH protocol are used to connect and manage DSLAM, FTTx, Router and Switch NEs
- Qx/Transaction Language 1(SSL) protocol are used to connect and MSTP, OTN ,WDM, Microwave, PTN and OTN NEs
- SFTP protocol can be used for all types of NE

The U2000 provides Message Request Broker (MRB), standard common object request broker architecture (CORBA), simple network management protocol (SNMP), Transaction Language 1(TL1), Extensible Markup Language (XML) and file interfaces. In addition, the U2000 allows for interoperability with OSS.

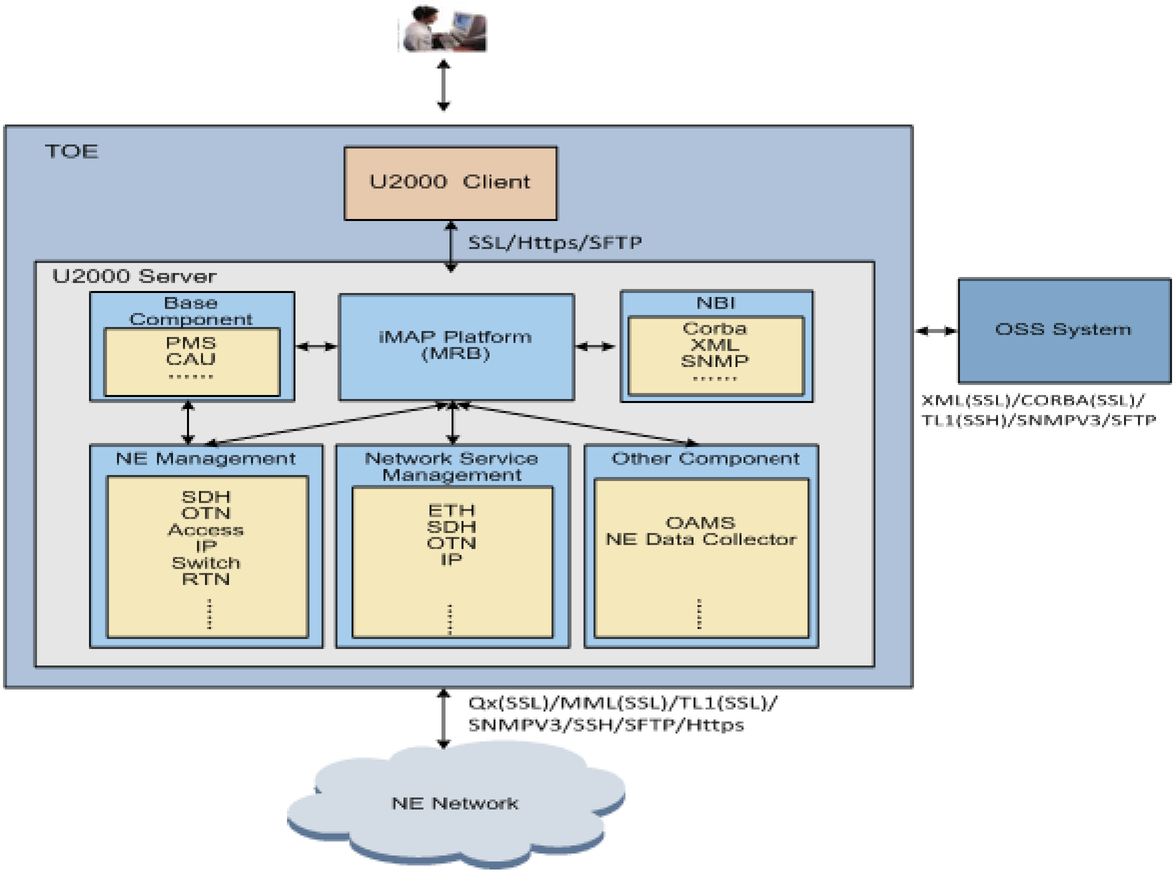

Figure 1:TOE Fixed Network

1.3.3 Non TOE Hardware and Software

The U2000 Client requires:

Device Type	Device Description	Quantity	Configuration Description
PC	**Client**	**1**	**CPU: Intel E2140** **Memory: 2 GB** **Hard disk: 160 GB** **Operating system:Windows7**

The U2000 Server requires:

Device Type	Device Description	Quantity	Configuration Description
Server	Server Module(SUN M4000, 4 CPU, Single Server)	1	Number of CPUs: 4 CPU clock frequency: 2.66 GHz Memory: 32 GB or above Local disk: 2 x 300GB or above Disk array: 6 x 300 GB Operating system: Solaris 10 Database: Sybase 15.0.3 with ESD#4+EBF18839
Server	Server Module(IBM X3850 X5, 8 CPU , Single Server)	1	Number of CPUs: 8 CPU clock frequency: 4*Xeon 8Core 2.0 GHz or above Memory: 32 GB Local disk: 8 x 300GB Operating system: Windows Server 2008 R2 Standard Database: MS SQL Server 2008 SP1 Standard
Server	Server Module(IBM X3850 X5, 8 CPU , Single Server)	1	Number of CPUs: 8 CPU clock frequency: 4*Xeon 8Core 2.0 GHz or above Memory: 32 GB Local disk: 8 x 300GB Operating system: SUSE Linux 10 SP4 Database: Oracle 11g Enterprise Edition Release 11.1.0.7.3

In addition, there are the following requirements :

a) The firewall should be provided by users.

b) 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.

c) The U2000 Server obtains a NTP time signal from one of its OMMs, using the standard MD5-authentication to protect against masquerading and modification (disclosure is not relevant as time is public).

1.4 TOE Description

1.4.1 TOE Definition Scope

This section will define the scope of the iManager U2000 to be evaluated.

1.4.1.1 Physical scope

As a software system, the TOE is a software to be installed on specified hardware server and do not contain any hardware itself.

The TOE contains the following software:

Application Software	Name and version
U2000 Client	Huawei iManager U2000 V100R009C00SPC301
U2000 Server	Huawei iManager U2000 V100R009C00SPC301

The TOE is delivered with the following guidance:

Document Name	Version
iManager_U2000_V100R009C00_Product_Documentation_03(hdx)-C	Issue 03
U2000_V100R009C00SPC301_Patch_Installation_Guide_03-A	Issue 03
Common Criteria Security Evaluation - Certified Configuration	V1.2

1.4.1.2 Logical scope

U2000 is the software for managing fixed networks. The major security features implemented by Huawei iManager U2000 and subject to evaluation are:

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, maintenance and guest. It also can define user groups for different user roles.

Authentication

The iMAP platform can authenticate all users accessing to the TOE by user name and password. This is the authenticate of the application layer.

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 be managed NEs, and then the user can only perform authorized operations to these authorized NEs.

Auditing

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

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

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

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.

Encrypted transmission

The TOE support encrypted transmission between NE and iManager U2000 server, between U2000 client and U2000 server, between operations support system and U2000 server.

User session management

The iMAP platform provides all online user sessions 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.

Security function management

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

1.4.2 Environment

The environment for TOE comprises the following components:

- The OSS or tools providing connection to the TOE through external interface including the protocols such as SNMP, CORBA, FTP, Transaction Language 1(TL1) , Extensible Markup Language (XML).
- 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, Suse, Linux and Windows Server within the TOE via a secure channel enforcing secure shell (SSH).
- The U2000 Server obtains a NTP time signal from one of its OMMs, using the standard MD5-authentication to protect against masquerading and modification

(disclosure is not relevant as time is public).

- Supports the use of SSL digital certificate security solutions, U2000 digital certificate using SSL certificate to ensure secure communications between U2000 server and client, U2000 and NEs, U2000 and the OSS.
- Firewall: all the accesses to the server of TOE are performed through a firewall.

2 CC conformance claims

This ST is CC Part 2 conformant [CC] and CC Part 3 conformant [CC]. The CC version of [CC] is 3.1R4.

This ST is EAL3-conformant + ALC_CMC.4 + ALC_FLR.2 as defined in [CC] Part 3.

The metohology to be used for evaluation is CEM3.1 R4.

No conformance to a Protection Profile is claimed.

3 Security Problem Definition

3.1 Assumptions

A.Physical The hardware that the TOE is running on is operated in a physically secure and well managed environment.

It is assumed that the software platform of the server that the TOE is running on (as listed in section 1.4.1) are protected against unauthorized physical access.

It is assumed that the database Sybase, MS SQL, or Oracle database is protected against data file damage.

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

It is assumed that the PC of TOE client are protected against unauthorized physical access.

A.NetworkSegregation It is assumed that the network interface of the server and client of the TOE will be accessed only through sub-network where the TOE hosts. The sub-network is separate from the public networks. The communications with the server of TOE are performed through a firewall. See section 1.4.2 Environment for more information

A.AdministratorBehaviour It is assumed that the super user admin, 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 in the TOE.

A.NTP It is assumed that operating environment should provide an accurate time source, in order to ensure the normal operation of the TOE server.

A.NetworkElements It is assumed that the managed network elements are trusted and can support the SSL /SNMPv3 /SSH /SFTP /HTTPS connection with the TOE, and the private interface defined by Huawei .

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 protected against the threat agents.	User data
OM data	The confidentiality and integrity of the OM data of NE including such as configuration data should be protected against the threat agents	OM data

Agent	Description
Attacker	An external attacker, who is not user of the TOE,.
Eavesdropper	An eavesdropper, who has access to communication channel over which the OM data and TSF data are transferred.
Unauthorized user	An authenticated user of the TOE gains unauthorized accesses to the TOE.

3.2.2 Threats addressed by the TOE

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

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

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 OSS client.
Asset	OM data; TSF data
Agent	Eavesdropper

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 server of 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 OSS .
- **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 are trusted can support the SSL /SNMPv3/SSH/SFTP/HTTPS 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, Suse Linux workstation, windows Server workstation, disk array, client PC) 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 between the server of TOE and non trust domain, filter the unused communication port.
- **OE.Database** The operational environment shall protect the database against unauthorized physical access and data file damage.
- **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 to the TOE. Also, the users of the underlying operating system will not perform any harmful operation to the TOE.

- **OE.NTP** The operational environment shall provide an accurate time source, in order to ensure the normal operation of the server of TOE.

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
O.Authentication	T.UnauthenticatedAccess T.UnauthorizedAccess
O.Authorization	T.UnauthorizedAccess
O.Audit	T.UnauthorizedAccess

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.Physical	A.Physical T.UnauthenticatedAccess
OE.NetworkSegregation	A.NetworkSegregation
OE.Database	A.Physical T.UnauthenticatedAccess T.UnauthorizedAccess
OE. AdministratorBehaviour	A.AdministratorBehaviour
OE.NTP	A.NTP

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). And the threat is countered by requiring the system and database to implement an authentication mechanism for its users(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 authenticating the users in the TOE (O.Authentication). The threat also is countered by audit records show that if someone indeed performed unauthorized operation he can be traced to(O.Audit). In addition, OE.Database ensures that the user account data stored in the database will not be altered maliciously.
T.Eavesdrop	The threat of eavesdropping is countered by requiring security communications: - Securing network communication between GUI client and U2000 server through SSL/SFTP/HTTPS (O.Communication). - Through SSL/SNMPv3/SSH/SFTP/ HTTPS protocols between U2000 server and NEs (O.Communication). - Through SSL/SNMPv3/SSH/SFTP/ HTTPS protocols between U2000 server and the OSS client. (O.Communication).

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.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.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.
A.NTP	The assumption that operating environment should provide an accurate time source is addressed by OE.NTP.
A.NetworkElements	The assumption that the managed network elements are trusted and can support the SSL /SNMPv3 /SSH/ SFTP /HTTPS is addressed by OE.NetworkElements

The following table provides a matrix of TOE objectives and threats.

	T.Eavesdrop	T.Unauthenticated Access	T.Unauthorized Access
O.Communication	X		
O.Authentication		X	X
O.Authorization			X
O.Audit			X

5 Security Requirements for the TOE

5.1 Conventions

The following conventions are used for the completion of operations:

- ~~Strikethrough~~ indicates text removed as a refinement
- (underlined text in parentheses) indicates additional text provided as a refinement.
- **Bold text** indicates the completion of an assignment.
- ***Italicised and bold text*** indicates the completion of a selection.
- Iteration/N indicates an element of the iteration, where N is the iteration number/character.

5.2 Security Requirements

5.2.1 Security Audit (FAU)

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 [***not specified***] level of audit; and
c) [

a) **user login, logout**

b) **user account management**
   - i. **user account create, delete, modify**
   - ii. **change user password**
   - iii. **grant access right to user account**

c) **user group(role) management**
   - i. **user group create, delete, modify**
   - ii. **grant access right to user group**

d) **security policy management**
   - i. **modify password policy**
   - ii. **modify user account policy**

e) **user session management**
   - i. **Kick out individual user session**

f) **ACL management**
   - i. **ACL create, delete, modify**
   - ii. **Specify ACL for individual user account.**

g) **Operation set and Object set management**

h) **SSL connection management**

i) **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, [**none**].

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.

FAU_SAR.1 Audit review

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

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.

FAU_SAR.3 Selectable audit review

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

FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall [**store the audit record in database, and export them into file**] if the audit trail exceeds [**pre-defined limit**].

5.2.2 User Data Protection (FDP)

FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the [**iMAP access control policy**] on [**users as subjects, domain as objects**] and all operations among subjects and objects covered by SFP.

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.

FDP_ACF.1 Security attribute based access control

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

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: [**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: [**none**].

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

5.2.3 Identification and Authentication (FIA)

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [***an administrator configurable positive integer within[1 to 99]***] unsuccessful authentication attempts occur related to [**the last successful authentication of the user name**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [**lock the user account for default 30 minutes**].

FIA_ATD.1 User attribute definition

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

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)**].

FIA_SOS.1 Verification of secrets

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

1. **For user's password, they are case sensitive**
2. **not contain the user name and user name written in inverted**
3. **contain one special character, one uppercase letter and one digit at least**
4. **the whole word is not in password dictionary and it is not a repeated string**
5. **The length of password should be more than 8 characters**].

FIA_UAU.2 User authentication before any action

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

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.2.4 Security Management (FMT)

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [**iMAP access control policy**] to restrict the ability to [***query, modify***] the security attributes [**all the security attributes**

defined in FDP_ACF.1] to [**the security administrators SMManagers and the super user admin**].

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [**iMAP access control policy**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 The TSF shall allow [**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.

FMT_SMF.1 Specification of Management Functions

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

a) **authentication, authorization**
b) **ACL policy**
c) **user management**
d) **management of Command Groups**
e) **audit management for export**
f) **SSL/SNMPv3 connection management**
g) **Configuration of the time interval of user inactivity for terminating an interactive session**
h) **Security policy management**].

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: [

a) **the super user admin**
b) **the default groups:**
c) **SMManagers,**
d) **Administrators,**
e) **Operators,**
f) **Maintenances,**
g) **Guests,**
h) **NBI User**].

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

5.2.5 Protection of the TSF (FPT)

FPT_ITT.1 Basic internal TSF data transfer protection

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

5.2.6 TOE access (FTA)

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

FTA_SSL.1 TSF-initiated session locking

FTA_SSL.1.1 The TSF shall lock an interactive session after [**administrator configured time interval, default 30 minutes of user inactivity**] by:
(a) clearing or overwriting display devices, making the current contents unreadable;
(b) disabling any activity of the user’s data access/display devices other than unlocking session.
FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [**user re-authentication**]

FTA_TSE.1 TOE session establishment

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

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**].

5.2.7 Trusted Path/Channels (FTP)

i. 5.1.7.1 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and **[*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 **[*disclosure, modification*]**
FTP_TRP.1.2 The TSF shall permit **[*remote*]** users to initiate communication via the trusted path.
FTP_TRP.1.3 The TSF shall require the use of the trusted path for [**performance data bulk collection, backup, update about all NEs software and transmission performance and inventory text files and configuration files to the OSS.**]

ii. 5.1.7.2 FTP_ITC.1.OSS Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2 The TSF shall permit ***[the TSF and OSS]*** to initiate communication via the trusted channel.
FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**transporting network performance data, inventory data and alarms to the OSS.**].

iii. 5.1.7.3 FTP_ITC.1.NE Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2 The TSF shall permit ***[the TSF and NE]*** to initiate communication via the trusted channel.
FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **[**

a) **command the NE**
b) **request and receive data or file from the NE.**
c) **Upload software or file to the NE].**

5.3 Security Functional Requirements Rationale

5.3.1 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_STG.3	O.Audit
FAU_SAR.1	O.Audit
FAU_SAR.2	O.Audit
FAU_SAR.3	O.Audit
FAU_STG.3	O.Audit
FDP_ACC.2	O.Authorization
FDP_ACF.1	O.Authorization
FIA_AFL.1	O.Authentication
FIA_ATD.1	O.Authentication O.Authorization
FIA_SOS.1	O.Authentication
FIA_UAU.2	O.Authentication O.Authorization
FIA_UID.2	O.Audit O.Authentication O.Authorization
FMT_MSA.1	O.Authorization
FMT_MSA.3	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_SSL.1	O.Authentication
FTA_TSE.1	O. Authentication
FTP_TRP.1 FTP_ITC.1.OSS	O.Communication O.Communication
FTP_ITC.1.NE	O.Communication

5.3.2 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.2). 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). The audit record is stored in database, and exported into file if the size of audit record exceeds the configured maximum size.(FAU_STG.3)
O.Communication	Communications security is implemented by the establishment of a secure communications channel between client and server,in (FPT_ITT.1), and two kinds of inter-TSF trusted channel between the TOE and other OSS/NE in (FTP_ITC.1.OSS/ FTP_ITC.1.NE). The communication to NEs performance data bulk collection and backup, update software through the secure channel. (FTP_TRP.1) The communication to the OSS transmit performance and inventory text files .(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.2) and supported by individual user identifies in (FIA_UID.2). 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) and the TOE locks session when they are inactive for a configured period of time (by default 30 minutes) (FTA_SSL.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), and the access control policies are modeled in (FDP_ACF.1) for accessing the U2000 server. Unique user IDs are necessary for access control provisioning (FIA_UID.2), also authenticating the users (FIA_UAU.2) 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, FMT_MSA.3, FMT_SMF.1).

The following table provides a matrix of SFRs and the security objectives.

	O.Audit	O.Authorization	O.Authentication	O.Communication
FAU_GEN.1	X			
FAU_GEN.2	X			
FAU_STG.3	X			
FAU_SAR.1	X			
FAU_SAR.2	X			
FAU_SAR.3	X			
FAU_STG.3	X			
FDP_ACC.2		X		
FDP_ACF.1		X		
FIA_AFL.1			X	
FIA_ATD.1		X	X	
FIA_SOS.1			X	
FIA_UAU.2		X	X	
FIA_UID.2	X	X	X	
FMT_MSA.1		X		
FMT_MSA.3		X		
FMT_SMF.1	X	X	X	X
FMT_SMR.1		X		
FPT_ITT.1				X
FTA_MCS.1			X	
FTA_SSL.1			X	
FTA_TSE.1			X	
FTP_TRP.1				X
FTP_ITC.1.OSS				X
FTP_ITC.1.NE				X

5.3.3 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	Resolved by external time source. 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_STG.3	FAU_STG.1	FAU_STG.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	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.2 FMT_MSA.3	FDP_ACF.1 FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	None	None
FIA_SOS.1	None	None
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UID.1	None	None
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.2 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_ITT.1	None	None
FTA_MCS.1	FIA_UID.1	FIA_UID.1
FTA_SSL.1	FIA_UAU.1	FIA_UAU.2
FTA_TSE.1	None	None

FTP_TRP.1	None	None
FTP_ITC.1.OSS	None	None
FTP_ITC.1.NE	None	None

5.4 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_FLR.2. 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.3 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_FLR.2 Flaw reporting procedures
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

5.5 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, Maintenance, NBI User and Guest. 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, FMT_MSA.3, 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).

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.

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.2, FIA_UID.2, 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 U2000 client if the operation rights have been assigned by security administrators SMManagers or the super user admin,

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

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, SNMPv3 and SFTP, for the data transmission, and also support to password encrypted transmission between client and server in the common communicate channel.

- The secured connection between U2000 client and U2000 server includes message channel. The SSL connection is used for message channel, and HTTPS protocol can be used between Web explorer and U2000 server. If the

X.509 digital certificates are deployed on client and server, the SSL connect with authentication can be used. The secured connection can be initiated from U2000 client if the SSL connection is selected on U2000 client by user. (FPT_ITT.1)

- The passwords are encrypted between U2000 client and U2000 server if the public-private key is generation and deployed on server. (FPT_ITT.1)

- The encrypted communication also includes message channel between network elements and TOE. The SSL, SNMPv3, SSH and HTTPS connection is used for message channel. The key used for cipher the communication between the NEs and U2000 are generated following the SSL, SNMPv3, SSH and HTTPS protocol (FTP_ITC.1.NE).
- SNMPv3 connections between the server and The OSS of SNMP clients (FTP_ITC.1.OSS)
- SSL connections between the server and the OSS of CORBR and XML clients (FTP_ITC.1.OSS)
- SSH connections between the server and the OSS of SSH clients (FTP_ITC.1.OSS)
- The TOE also provides a secure channel for the the communication to NEs performed performance data bulk collection and backup,update software.(FTP_ITC.1.NE)

6.1.6 User session management

The TOE also offers the user session 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 30 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_SSL.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

  i. user account create, delete, modify

  ii. change user password

  iii. grant access right to user account

c) user group(role) management

  i. user group create, delete, modify

  ii. grant access right to user group

d) security policy management

  i. modify password policy

  ii. modify user account policy

e) user session management

  i. Kick out individual user session

f) ACL management

  i. ACL create, delete, modify

  ii. Specify ACL for individual user account

g) Operation set and Device set management

h) SSL connection management

i) 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 U2000 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，FAU_STG.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, FMT_MSA.3, 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
OM	Operation and Maintenance
NE	Network Element
OSS	Operations Support System

7.2 Terminology

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.

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.

Operator See User.

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

7.3 References

[CC] Common Criteria for Information Technology Security Evaluation. Part 1-3. September 2012. Version 3.1 Revision 4.

[CEM] Common Methodology for Information Technology Security Evaluation. September 2012. Version 3.1 Revision 4.