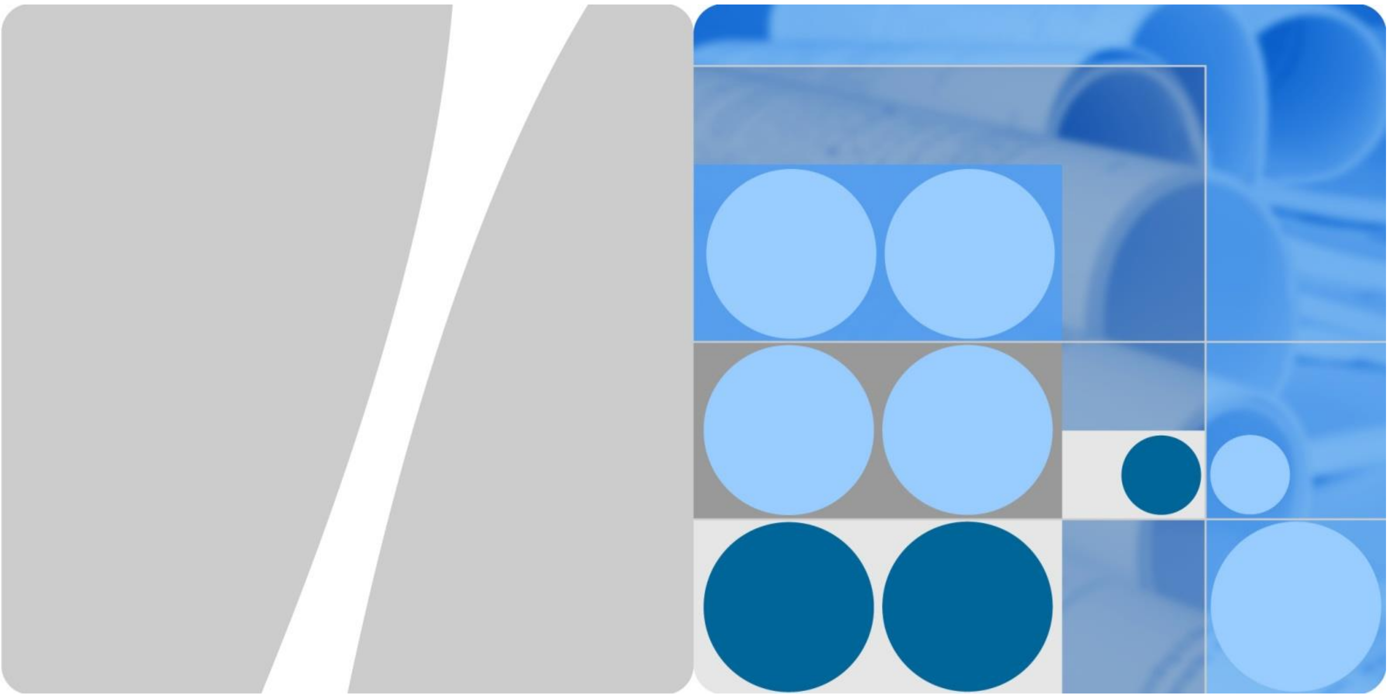

Security Target for Huawei USN9810 V900R012

Version 1.5

Date 2014-02-17

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Contents

Revision Record

Date	Revision Version	Change Description	Author
2013-3-6	0.1	Initial template	Yao Junning
2013-3-13	1.0	First version	Guoyong;Yao Junning
2013-05-31	1.1	Second version	Jason Chen
2013-08-01	1.2	Third version	Jason Chen
2013-09-20	1.3	Update of physical scope	Guoyong;Yao Junning
2013-11-15	1.4	Update according to EOR	Guoyong;Yao Junning
2014-02-17	1.5	Update Conformance claim	Guoyong;Yao Junning

1 Introduction

This section contains the ST reference, TOE reference, TOE overview and TOE description of Huawei USN9810 V900R012.

1.1 ST reference

Title: Huawei USN9810 Version 900 Release 12 Security Target

Version: 1.5

Publication date: 2014-02-17

1.2 TOE reference

The TOE is identified as below:

TOE name: Huawei USN9810

TOE version: V900R012C00SPC300

Developer: Huawei Technologies Co., Ltd.

TOE release date: 2013-6-16

1.3 TOE overview

1.3.1 TOE usage and major security features

The mobile network has developed from the 2G global system for mobile communications (GSM), the 2.5G general packet radio service (GPRS), and the 3G universal mobile telecommunications system (UMTS) to the enhanced 3G (E3G) long term evolution (LTE). Mobile networks cover wide areas, achieve high-speed wireless data transmission, and allow access to the Internet.

The USN9810, a unified service node independently developed by Huawei, can be used in GPRS, UMTS, and EPC networks. The USN9810 provides the functions of the serving GPRS support node (SGSN) and mobility management entity (MME) and can be used as a separate SGSN, separate MME, or combined SGSN/MME. The USN9810 can also be used as a single network element (NE) to manage other USN 9810s. The TOE and its environment are depicted in Figure 1.

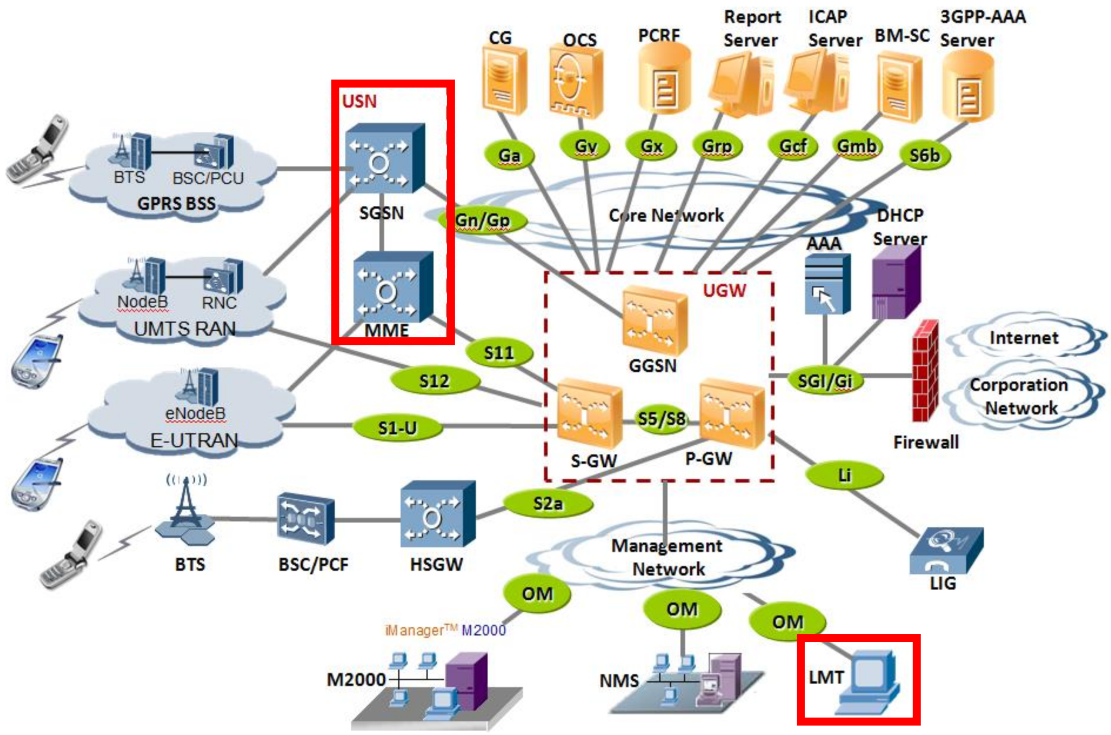

Figure 1 TOE and its environment

MS: mobile station	OCS: Online Charging system
BSS: base station subsystem	PCRF: Policy and Charging Rules Function
BTS: base transceiver station	Report Server: used to record and summarize service data reported by UGW9811
BSC: base station controller	ICAP server: Internet Content Adaptation Protocol Server
RNC: radio network controller	BM-SC: Broadcast Multicast Service Center
UTRAN: UMTS terrestrial radio access network	3GPP-AAA: authentication, authorization, and accounting for 3GPP network
E-UTRAN: Evolved UMTS Terrestrial Radio Access Network	AAA: authentication, authorization, and accounting for PDN
eNodeB: Enhanced NodeB	LIG: Lawful Intercept Gateway
SGSN: serving GPRS Support Node	LMT: Local Management Terminal
MME: Mobility Management Entity	M2000: Huawei iManager Element Management System
CG: charging gateway	NMS: Network Management System
HSGW: High Rate Packet Data Serving Gateway	

The networks other than the Maintenance network are categorized as the telecommunication service network.

- **Usage**

The USN9810 is a core device on the system architecture evolution (SAE) network. It provides the functions of a Mobility Management Entity (MME). As part of a 2G/3G core network it is also able to provide the functions of a Serving GPRS Support Node (SGSN).

The MME supports the following functions:

1) Security procedures: End-user authentication as well as initiation and negotiation of ciphering and integrity protection algorithms.
2) • Terminal-to-network session handling: All the signaling procedures used to set up packet data context and negotiate associated parameters like QoS.
3) • Idle terminal location management: The tracking area update process used to enable the network to join terminals for incoming sessions.

The functions of the SGSN include:

1) Routing and forwarding data packets from/to all mobile users in its own SGSN area Encryption and authentication.
2) Session management: The Session Management enables the USN9810 to establish connections between mobile stations (MSs) and the gateway GPRS support node (GGSN) and to manage the Packet Data Protocol (PDP) contexts of the MSs. Session management comprises procedures such as PDP context activation, modification, deactivation, and preservation.
3) Mobility management: The Mobility Management (MM) is used to control the access of MSs to general packet radio service (GPRS) and universal mobile telecommunications system (UMTS) networks and to track the current locations of them, such as the routing areas (RAs) and SGSNs where the MSs reside. This function involves such procedures as attach, detach, and routing area update (RAU). These procedures allow the location information of a moving MS to be updated in a timely manner.
4) Bill generation and export for collecting usage information of radio resources.

- **TOE major security features**

The major security features implemented by the USN9810 and subject to evaluation are:

Authentication

The TOE can authenticate administrative users (referred as “users” hereafter) by user name and password. The TOE is able to enforce password policies as well as “lockout” policies to deter password guessing attacks. Further, it is possible to limit login of specific users to specific time frames and to define expiry dates for accounts and passwords.

Authorization

The TOE offers the management of network devices. The TOE implements access control that allows limitation of access both in terms of operations that a user is authorized to perform and in terms of objects that a user can perform these operations on. The TOE allows the definition of User Groups, as well as Command Groups and Managed Object Groups, in order to define roles that can be assigned to users.

Access control

The TOE support access control function on IP protocol, the TOE can protect valid IP address which is connecting. When the TOE connects to network for the first time, the user must configure the valid IPs, then the function that it can refuse invalid IP address connection is effective.

The TOE support VLAN and VRF function, it can benefit for network separation. VLAN and VRF function can separate the network to several virtual networks on one router, so customers can use the VLAN and VRF to separate the network to protect security environment.

- **Communications security**

The TOE provides communication security by implementing Secure Sockets Layer (SSL) and Transport Layer Security (TLS) for communication between the LMT client and the TOE or between the M2000 (Huawei network management system) and the TOE.

The TOE is also able to restrict session establishment to administrator-specified IP source addresses in LMT client requests.

- **Auditing**

The TOE generates and stores audit records for security-relevant management actions. The audit data can be queried by the authorized user.

The TOE classifies the audit record into four categories according to the management scope and action: Operation logs, Security logs, System logs and Application software operation logs.

- **Security function management**

The following means are provided by the TOE for the management of security functionality:

- User and group management
- Access control management (by means of defining command groups, managed object groups, and association of users with particular managed elements , managed objects, and commands) enabling/disabling of SSL for communications security.

1.3.2 TOE type

The TOE is a Service and Network Controller and its local management graphical user interface (GUI)

1.3.3 Non-TOE hardware/software/firmware required by the TOE

The server part of the TOE requires:

Name	Version
Database	PROTON Database based on postgreSQL, postgresql 8.3.20).

The management LMT GUI requires:

- A PC suitable to run the OS (see below)
- Microsoft Windows XP SP3 or later

1.4 TOE Description

1.4.1 Physical scope

The hardware components of TOE include cabinets, sub racks, boards, and power supply system. The TOE consists of 11 types of boards:

Name	version	Description
OMU	CN21UPBA2/ CN22UPBA6	The operation & maintenance unit (OMU) performs the operations and maintenance of the system.
USI	USIA7	• Serving as the interface board of the UPB, the USIA7 provides various external interfaces, including: • Six gigabit Ethernet interfaces (10/100/1000M auto-sensing) to other network devices • Standard VGA interface to the KVMS • USB interface to the keyboard and mouse • Hot swapping
ECU	CN21UPBA3/ CN22UPBA3	The enhanced control plane unit (ECU) performs the service processing and charging functions related to the control plane.
EPU	MSPB0	The Enhanced Packet forward Unit (EPU) board processes the services related to the user plane.
ETI	ETIA0/SSIA0/ SSIA2	Functioning as the rear board of the enhanced control plane unit (ECU), the E1/T1 interface board (ETI) is generally used together with matching subboards.
PFI	PFIA0	Packet Forward Interface (PFI) as the rear board of the broadband interface processing board and the rear board of the EPU board.
SWU	SWUA1/SWUB1	The SWU is a switch unit. It consists of an exchange carrier board and a time division multiplexing (TDM) daughter board. The SWU supports layer-2 network switching, TDM narrowband switching, device management, configuration restoration and hot swap.
TSI	SWIA0/SWIB0	The Time Slave Interface (TSI) board is used in the extended subrack supporting cascading between subracks and provides the clock receive function.
TMI	SWIA1/SWIB1	The Time Master Interface (TMI) board is used in the extended subrack supporting cascading between subracks and provides

		the clock receive function.
SMM	SMMD/SMME	The SMM board is used to manage all hardware in the OSTA 2.0 subrack including the subrack, boards of all types, fan tray to implement the device management, event management, asset management, power management, remote maintenance, configuration restoration, and power saving control.
SDM	SDM	The SDM (Shelf Data Module) stores the subrack asset information, such as subrack name, bar code, vendor, and delivery date.

The TOE comes with the following software:

Name	Version
USN9810	V900R012C00SPC300
OS	SUSE Linux Enterprise Server 10 SP2

The TOE comes with the following guidance:

Name	Version
USN9810 Product Documentation	V900R012C00, 2013/08/05
Common Criteria Security Evaluation – Certified Configuration	V1.2, 2013-11-12

1.4.2 Logical scope

The logical scope can be found in section 1.3

2 Conformance claims

This ST and the TOE conform to the version of CC as below:

Part 1: Introduction and general model Version 3.1 Revision 4

Part 2: Security functional components Version 3.1 Revision 4

Part 3: Security assurance components Version 3.1 Revision 4

This ST conforms to CC Part 2 conformant

This ST conforms to CC Part 3 conformant

This ST conforms to no Protection Profile

This ST confirms to EAL 3 augmented with ALC_CMC.4, and no other packages

3 Security Problem Definition

3.1 Assets

The classification of the different data types is given in the following:

- **User Plane Data**: USN9810 supplies GPRS, UMTS, LTE business, in USN9810 there are transfer data by User Equipment, and SMS data.
  - IP packets transmitted by user equipment.
  - SMS transmitted by user equipment.
  - Location information transmitted by user equipment.
- **Control Plane Data**: USN9810 stores the connection information about connecting devices.
  - Session information of the network device。
  - Configuration information of the network device。
- **Management Plane Data**: TSF data is information used by the TSF in making TOE Security Policy decisions:
  - audit records
  - configuration parameters (for auditing, authentication, access control, communications security, etc.)
  - Command Group definitions
  - Manage Authority and Operate Authority definitions
  - Source IP addresses in remote client session establishment requests
  - the security attributes given below for the objects they belong to:

Users:

a) passwords

b) unsuccessful authentication attempt since last successful authentication attempt counter

c) User Group membership

d) account expiration date

e) password expiration date

f) login start and end time

Managed Objects:

a) Managed Object Group membership

3.2 Threat Agents

The Assets are threatened by the following threat agents:

TA.ROGUE_USER: A user seeking to act outside his/her authorization

TA.ROGUE_SYSTEM: A device seeking to connect to the server part of the TOE while there is no resource or they are not allowed to

TA.NETWORK: An attacker who can access the management network/telecommunication network that the TOE is connected to

TA.PHYSICAL: An attacker with physical access to the TOE

3.3 Threats

T.AccountabilityLoss: TA.ROGUE_USER performs undesirable actions that he is allowed to perform, or attempts to perform actions he is not allowed to, and this cannot be traced back to TA.ROGUE_USER.

T.Eavesdrop: TA.NETWORK is able to intercept, and potentially modify or re-use, information assets that are exchanged between the TOE client (LMT) and the TOE server part (OMU).

T.UnauthenticatedAccess: TA.ROGUE_USER or TA.ROGUE_SYSTEM gains access to the TOE.

T.UnauthorizedAccess: TA.ROGUE_USER gains access to commands or information he is not authorized to access.

3.4 Assumptions

A.PhysicalProtection: It is assumed that the server part of the TOE and the workstation that is hosting the client part of the TOE are protected against unauthorized physical access.

A.TrustworthyUsers: It is assumed that the organization responsible for the TOE and its operational environment has measures in place to establish trust into and train users of the TOE commensurate with the extent of authorization that these users are given on the TOE. (For example, super users and users that are assigned similar privileges are assumed to be fully trustworthy and capable of operating the TOE in a secure manner abiding by the guidance provided to them.)

A.TrustworthyConfigurations: It is assumed that the customer`s configurations of connections to other trusted devices are correct.

A.Support: It is assumed the operational environment provides reliable time stamps for the generation of audit records and a database to store the audit records.

A.TrustedNetwork: It is assumed that the Telecommunication Service networks are trusted.

A.TrustedSystems: It is assumed that the systems in the Telecommunication Service networks and the EMS are trusted.

4 Security Objectives

4.1 Security Objectives for the TOE

O.Authentication: The TOE shall authenticate management users of its user interfaces.

O.Authorization: The TOE must implement an access control mechanism to differentiate between different authorities for TOE users.

O.AccessControl: The TOE shall refuse access by invalid devices or users.

O.Communication: The TOE shall implement logical protection measures for network communication between the server part of the TOE and the client part of the TOE.

O.Audit: The TOE shall be able to generate audit records for security-relevant events.

4.2 Security Objectives for the Operational Environment

OE.Administration: Those responsible for the operation of the TOE and its operational environment must ensure that only authorized users have access to the management plane, and in particular to the part of the TOE and its data that is running in management plane. This includes ensuring that audit records stored in the database in the operational environment are protected against unauthorized access, and that cryptographic keys and certificates are properly managed to support the communications security mechanisms implemented by the TOE.

This also includes the restriction of physical access to the server part of the TOE and the workstation hosting the client, making the TOE unavailable to access from the consumer/application networks served by the network device, and ensure that devices and networks the TOE assumes to be trusted are indeed trustworthy.

OE.Support: Those responsible for the operation of the TOE and its operational environment must ensure that the operational environment provides reliable time stamps for the generation of audit records and a database to store these records.

OE.Users: Those responsible for the operation of the TOE and its operational environment must be trustworthy, and trained such that they are capable of securely managing the TOE and following the provided guidance.

OE.Devices: Those responsible for the operation of the TOE must ensure that the configuration of connections to trusted devices in the TOE environment is correct.

4.3 Security Objectives Rationale

The following rationale provides justification that all threats are countered and all security objectives for the TOE are necessary.

Threat	Rationale for security objectives
T.AccountabilityLoss	The threat that records of security-relevant actions are not created properly is countered by a requirement to generate audit records for such events (O.Audit). The generation of audit records is supported by the operating system providing reliable time stamps to the TOE (OE.Support).
T.Eavesdrop	The threat of eavesdropping is countered by requiring communications security for network communication between clients and the TOE (O.Communication).
T.UnauthenticatedAccess	The threat of unauthenticated access to the TOE or its data is countered by requiring the TOE to implement an authentication mechanism (O.Authentication, O.AccessControl).
T.UnauthorizedAccess	The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism (O.Authorization).

Table 1: Coverage and sufficiency analysis for threats

The following rationale provides justification that all assumptions are upheld and all security objectives for the TOE are necessary.

Assumption	Rationale for security objectives
A.PhysicalProtection	The assumption that the TOE will be protected against unauthorized physical access is expressed by a corresponding requirement in OE.Administration.
A.TrustworthyUsers	The assumption that users are trained and trustworthy is expressed by a corresponding requirement in OE.Users.
A.TrustworthyConfigurations	The assumption that connections to trusted devices are configured correctly is expressed by a corresponding requirement in OE.Devices
A.Support	Assumptions on support for the TOE’s security functionality provided by the operational environment are addressed in OE.Support.
A.TrustedNetwork	The assumption that the Telecommunication Service networks are trusted is expressed by a corresponding requirement in OE.Administration.
A.TrustedSystems	The assumptions that systems in the Telecommunication Service networks are trusted is expressed by a corresponding requirement in

	OE.Administration.

Table 2: Coverage and sufficiency analysis for assumptions

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 TOE Security Functional Requirements

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) **The following auditable events:**

i. user activity

1. login, logout

2. operation (MML command) requests

ii. user management

1. locking, unlocking (manual or automatic)

2. add, delete, modify

3. group membership change

4. password change

5. management authority change

6. operation authority change

7. online user query

8. session termination

iii. user group management

1. add, delete, modify

2. **management authority change**
3. **operation authority change**

iv. **command group management**

1. **add, delete, modify**

v. **authentication policy modification**

vi. **workstation management**

1. **modification of access list**

vii. **log management**

1. **log policy modification**

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, **interface (if applicable), workstation IP (if applicable), Managed Element ID (if applicable), and MML command name (if applicable).**

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 authorized per FDP_ACF.1** 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.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply **querying** of audit data based on **date and time range, user ID, terminal, Managed Element ID, interface, and/or result.**

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **CGP access control policy** on **users as subjects, Managed Elements and Managed Objects of Managed Elements as objects, and commands and queries issued by the subjects targeting the objects.**

FDP_ACF.1 Security attribute based access control

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

a) **users and their following security attributes:**

i. **User Group membership**

ii. **ME authorizations**

b) **Managed Elements and their following security attributes:**

i. **Command Groups**

c) **Managed Objects and their following security attributes:**

i. **Managed Object 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:

a) **the user, or a User Group that the user is a member of, has been granted ME authorization for the Managed Element targeted by the request, and**

b) **the user, or a User Group that the user is a member of, is associated with a Command Group of the Managed Element targeted that contains the requested command, and**

c) **the user, or a User Group that the user is a member of, is associated with a Managed Object Group for the Managed Object targeted; and if a configuration change is requested, the requested parameter is within the range authorized by the Managed Object Group definition**

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

a) **If the user is a service user and is the super user requesting a service operation, access is granted without performing the checks in FDP_ACF.1.2 a).**

FDP_ACF.1.4 ~~(refined away)~~

FIA_AFL.1 **Authentication failure handling**

FIA_AFL.1.1 The TSF shall detect when ***an administrator configurable positive integer within*** **1 and 5** unsuccessful authentication attempts occur related to **login event since the last successful authentication of the indicated user identity and before the counter for these attempts is reset after an administrator configurable time frame either between 1 and 60 minutes or "never", and only if the user is not the super user.**

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***surpassed***, the TSF shall **lockout the account for an administrator configurable duration either between 1 and 1440 minutes or "indefinitely".**

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) **password**

c) **unsuccessful authentication attempt since last successful authentication attempt counter**

d) **User Group membership**

e) **ME authorizations**

f) **account expiration date**

g) **password expiration date**

h) **login start and end time.**

FIA_SOS.1 **Verification of secrets**

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

a) **if enabled, an administrator configurable minimum length between 6 and 32 characters, and**

b) **if enabled, an administrator configurable combination of the following:**

i. **at least one lower-case alphanumerical character,**

ii. **at least one upper-case alphanumerical character,**

iii. **at least one numerical character,**

iv. **at least one special character.**

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.

FMT_MSA.1 **Management of security attributes**

FMT_MSA.1.1 The TSF shall enforce the **CGP access control policy** to restrict the ability to ***query, modify*** the security attributes **identified in FDP_ACF.1 and FIA_ATD.1** to **administrator-defined roles, service user super users**.

FMT_MSA.3/a **Static attribute initialization**

FMT_MSA.3.1 The TSF shall enforce the **CGP access control policy** to provide ***permissive*** default values for security attributes (Managed Object Group membership) that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **administrator-defined roles, service user super users** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/b **Static attribute initialization**

FMT_MSA.3.1 The TSF shall enforce the **CGP access control policy** to provide ***restrictive*** default values for security attributes (User Group membership) that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **administrator-defined roles, service user super users** 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) **configuration of authentication failure handling policy**

b) **configuration of password policy**

c) **user management (creation, deletion, modification of lockout status or password, User Group membership)**

d) **definition of Managed Object Groups and Command Groups**

e) **definition of IP addresses and address ranges that will be accepted as source addresses in client session establishment requests**

FMT_SMR.1 **Security roles**

FMT_SMR.1.1 The TSF shall maintain the roles

a) **service user**

b) **service user super user**

c) **administrator-defined roles, i.e. defined by association of service users with User Groups, Command Groups, and Managed Object Groups.**

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

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~~ (the server part and the GUI client part of the TOE).

FTA_TSE.1 TOE session establishment

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

a) **account expiration date**

b) **password expiration date**

c) **login start and end time**

d) **source IP address.**

FTP_ITC.1/EMS Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ (the EMS) that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit (the EMS) to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **performing EMS related functionalities**

5.3 Security Assurance Requirements

The development and the evaluation of the TOE shall be done in accordance to the following security assurance requirements:

EAL3 augmented by ALC_CMC.4

5.4 Security Requirements Rationale

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

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

Security Objective	Rationale for security objectives
O.Authentication	User authentication is implemented by FIA_UAU.2/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 for all of these is provided in FMT_SMF.1.
O.Authorization	The requirement for authorization is spelled out in FDP_ACC.1, and the access control policies are modeled in FDP_ACF.1. Unique user IDs are necessary for access control provisioning (FIA_UID.2), and user-related attributes are spelled out in FIA_ATD.1. Access control is based on the definition of roles (FMT_SMR.1), and management functionality for the definition of access control policies is provided (FMT_MSA.1, FMT_MSA.3a, FMT_MSA.3b, FMT_SMF.1).
O.AccessControl	The requirement for access control is spelled out in FTA_TSE.1, where logins can be refused based on network attributes like IP address, VRF route and VLAN id.
O.Communication	Communications security is implemented by the establishment of a secure communications channel between TOE parts in FPT_ITT.1 and between TOE and EMS in FPT_ITC.1. Management functionality to enable these mechanisms is provided in FMT_SMF.1.
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 authentication mechanism (FIA_UID.2). Since the TOE generates audit records in a binary format, tools are provisioned to read and search these records (FAU_SAR.1, FAU_SAR.3). Management functionality for the audit mechanism is spelled out in FMT_SMF.1.

Table 3: Security requirements rationale

5.5 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~~analysed here again.

The following table demonstrates that all dependencies of the SFRs have been successfully addressed:

Security Functional Requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	Met in environment by OE.Support
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	None	
FIA_SOS.1	None	
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	None	
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 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	
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_ITT.1	None	
FTA_TSE.1	None	
FTP_ITC.1/EMS	None	

6 TOE Summary Specification

6.1.1 Authentication

The TOE authenticates the users of its user interfaces based on individual user IDs and passwords. User IDs are unique within the TOE and stored together with associated passwords and other (security) attributes in the TOE's configuration database.

Authorized administrators are able to configure a system-wide password policy that is then enforced by the TOE. Besides the minimum length of the password, which can be set to be between 6 and 32 characters, administrators have the option to enforce the use of specific characters (numeric, alphanumeric low or capital, and special characters).

The TOE also offers the enforcement of permanent or timer-based account lockouts: administrators can specify after how many consecutively failed authentication attempts an account will be permanently or temporarily locked, and whether the counter for failed attempts will be reset automatically after a certain amount of minutes.

If applicable, i.e., if an administrator has specified values for these parameters for a specific user, the TOE will deny authentication of the user if the number of "account valid days" configured for the user has been exceeded, if the password has not been changed within the timeframe specified in the "password valid days" configuration for the user, or if the user tries to authenticate in a timeframe that lies outside of the "login start time" and "login end time" specified for the user.

Authentication based on user name and password is enforced prior to any other interaction with the TOE for all external interfaces of the TOE, namely the MML interface (typically accessed via the LMT GUI by users), as well as the SOAP interface used by remote service users.

(FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UID.2, FTA_TSE.1)

6.1.2 Authorisation

The TOE controls which operations users can perform on Managed Elements.

Managed Elements (MEs) are logical representations of product units that can be managed using the TOE. For example, the TOE itself (CGP) is a ME. The individual network elements that the product is comprised of, such as a ~~signaling~~signalling unit, are Managed Elements. The racks and subracks holding the network and management elements are Managed Elements. Etc. MEs are identified by a unique, vendor-specified ID within the product.

Each Managed Element contains one or more Managed Objects (MOs) that are associated with a number of tables in the configuration database that specify parameters for these objects (for example, IP addresses for the network ports that an ME might have).

Access control is enforced three-fold:

Managed Element authorization: operators can be authorized to see a Managed Element (for example, when listing the available MEs in a system)

Operation authorization: operators can be authorized to perform specific commands on a Managed Element (for example, DSP COMM to display the status of communication links of a ME)

Managed Object authorization; operators can be authorized to modify objects of (configuration data for) a Managed Element (for example, SET ALMLVL to set the severity of specific alarms that can be generated on an ME)

In order to implement role-based access control, users can be grouped into User Groups.

Users and User Groups can be given ME authorization (also referred to as "Manage Authority" or "ME rights") for specific Managed Elements. This merely represents the fact that users are authorized to know about the existence of the ME (the ME will show up in lists, etc.) – additional authorization to perform any specific management commands on the ME (and their objects) are then assigned in separate steps.

The Operation authorization specifies the MML commands a user can execute on a specific ME, such as "LST ME" to list all Managed Elements present (in fact, all MEs the user has "Manage Authority" for) and "ADD USER" to add a new user. This authorization is implemented by means of Command Groups:

Authorized administrators can define Command Groups for Managed Elements, containing a subset of the available MML commands. Users or User Groups can be assigned to these Command Groups, which grants them the right to execute the specified commands on the specified ME. Managed Elements come with pre-defined Command Groups, such as "Alarm Management Command Group" and "Performance Query Command Group". These can be modified or deleted by authorized administrators, who can also create additional Command Groups to reflect operational needs.

Lastly, the TOE allows authorized administrators to specify Managed Object Groups (MOGs), which define for a specific Managed Element the Managed Objects of the ME that a user is authorized to manage, and potential configuration limits that define limits for configuration parameters for these objects. By default, the TOE comes pre-configured with a Managed Object Group called "PUBLIC", and all Managed Elements and their objects (without configuration limits) are part of this group. Newly created users are automatically assigned the PUBLIC MOG, which means that – unless further granularity is desired and administrators either change members of the PUBLIC MOG or dis-associate the PUBLIC MOG from a user – access control can be abstracted to the management of ME authorization and Operation authorization.

As a result, authorized administrators who add new users to the system must specify which MEs these users are allowed to see (ME authorization) and which Command Groups for these MEs the users belong to (with "none" and "all" being valid assignments), and can specify which Managed Object Groups they belong to if the default PUBLIC assignment is not desired.

Command Groups and MOGs can also be assigned to User Groups instead of individual users.

A few service users in the TOE are associated with special roles:

a) A service level super user exists who is not subject to any access control on the service user level. While the user name for this user can be changed, the exemption of the user from access control enforcement cannot.

b) An EMS and a NMS user exist for EMS and NMS systems connecting to the TOE. These systems provide network management functionality to their users and, by default and when enabled, are authorized to perform a subset of commands on all MEs without limitations. In other words: They have ME authorization for all MEs, Operation authorization for a specific set of commands, and are associated with the PUBLIC MOG.

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

6.1.3 Access control

The ACL function in TOE can restrict IP addresses. Customers must use the ACL function to configure the valid IP address.

All planes supply the ACL function, which supports black-list mode and white-list mode:

In black-list mode: customers can configure refused IP addresses.

In white-list mode: customers can configure the permitted IP addresses.

Both of modes can be used at the same time, customers can therefore use both modes to satisfy requirements as needed..

(FTA_TSE.1)

6.1.4 Communications security

The TOE provides communications security for network connections. This includes connections via the following interfaces:

MML connections between LMT clients and the OMU (using SSL/TLS)

SOAP connections between the operational environment (EMS server) and the OMU (using SSL/TLS)

The SSL/TLS cipher suites supported for SSL connections are:

Cipher suite	**TLS 1.0**	**TLS 1.1**	**SSL 3.0**
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA			X
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA			X
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA			X
SSL_RSA_WITH_3DES_EDE_CBC_SHA			X
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	X	X	
TLS_DH_anon_WITH_AES_128_CBC_SHA	X	X	
TLS_DH_anon_WITH_AES_256_CBC_SHA	X	X	
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	X	X	
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	X	X	
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	X	X	
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	X	X	
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	X	X	
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	X	X	
TLS_RSA_WITH_3DES_EDE_CBC_SHA	X	X	
TLS_RSA_WITH_AES_128_CBC_SHA	X	X	
TLS_RSA_WITH_AES_256_CBC_SHA	X	X	

Also, the TOE will deny session establishment requests from LMT clients whose IP source address is not part of an administrator-defined list of IP addresses and subnets (referred to as “workstations”). Separate lists for service users exist.

(FPT_ITT.1, FTA_TSE.1, FTP_ITC.1/EMS)

6.1.5 Auditing

The TOE generates audit records for security-relevant events. (Please refer to FAU_GEN.1 for a list of event types, and the type of information recorded.) Where appropriate, the data recorded with each audit record includes the unique user ID associated with a subject during authentication.

The auditing functionality of the TOE cannot be started or stopped independently from the operational TOE. However, the TOE generates audit records for the start and shutdown of CGP, and of its individual subsystems.

Out of the audit logs that the TOE generates, the following comprise the logs relevant for the security functionality modelled in this ST:

a) an operation log, containing the audit records for particular MML operations performed by service users

b) a security log, containing audit records for security-related events, such as user login and management

Service users can use the LMT client to review the audit records available in the database for everything. The client offers search functionality based on time intervals, user IDs, interface, workstation IP, result, ME ID, and command name (in case of MML commands).

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

6.1.6 Security function management

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:

a) User management, including User Group memberships, passwords, account lockout, validity periods for an account and/or password, etc.

b) Access control management, including the definition of Managed Object Groups, Command Groups, and the association of users and User Groups with Managed Elements, Managed Object Groups, and Command Groups in Manage Authority and Operate Authority relationships.

c) Enabling/disabling of SSL for the communication between LMT clients and the OMU.

d) Defining IP addresses and address ranges for clients that are allowed to connect to the OMU server.

(FMT_SMF.1)

A Acronyms and Abbreviations

A	
ATCA	advanced telecommunications computing architecture
ATM	asynchronous transfer mode
B	
BG	border gateway
BSC	base station controller
BSS	base station subsystem
BTS	base transceiver station
C	
CG	charging gateway
CDR	charging data record
CGP	carrier grade platform
CS	circuit switched
D	
DNS	domain name server
E	
EIR	equipment identity register
G	
GGSN	Gateway GPRS support node
GPRS	General Packet Radio Service
GSM	Global System Mobile
GTP	GPRS Tunnel Protocol

H	
HA	home agent
HLR	home location register
I	
IP	Internet Protocol
ICMP	Internet control message protocol
IPv4	Internet Protocol version 4
ISDN	integrated services digital network
M	
MME	mobility management entity
MS	mobile station
O	
OMU	operation and maintenance unit
OS	operating system
P	
PDP	Packet Data Protocol
PDU	Packet Data Unit
P-GW	PDN gateway
P-TMSI	packet temporary mobile subscriber identity
Q	
QoS	quality of service
R	
RADIUS	remote authentication dial-in user service
RAN	radio access network
RNC	radio network controller

S

SGSN	serving GPRS support node
S-GW	serving gateway
SS7	signaling system No.7
SSH	secure shell
SMS	short message service
SOL	serial over LAN

T

TCP	Transmission Control Protocol

U

UDP	User Datagram Protocol
UE	user equipment
UMTS	Universal Mobile Telecommunications System

W

WAP	wireless access protocol