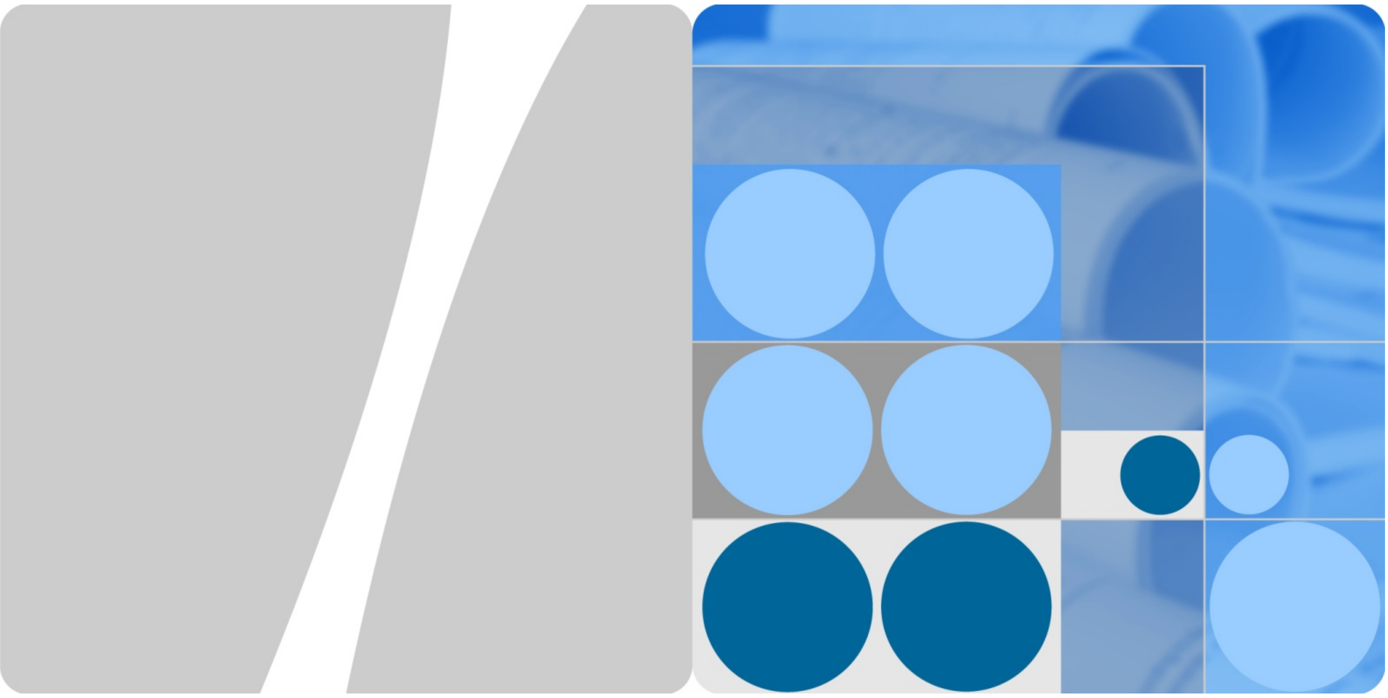

Security Target for Huawei UGW9811 V900R010

Version	1.5
Date	2013-11-07

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	Fist version	Chen Xiaoli;Yao Junning
2013-07-25	1.1	Change according to EOR	Jason Chen;Yao Junning
2013-08-26	1.2	Change according to EOR and developer comment	Shirley Chen;Yao Junning
2013-09-09	1.3	Change according to EOR	Shirley Chen; Yao Junning
2013-09-18	1.4	Update assurance component and guidance list	Shirley Chen; Yao Junning
2013-11-07	1.5	Update TOE version	Shirley Chen; Yao Junning

1 Introduction

1.1 ST reference

This ST is uniquely identified as below,

Title: Huawei UGW9811 Version 900 Release 10 Security Target

Version: V1.5

Publication date: 2013-11-07

1.2 TOE reference

The TOE is identified as below,

TOE name: Huawei UGW9811

TOE version: V900R010ENGC00SPC200

Developer: Huawei Technologies Co., Ltd.

TOE release date: 2013-7-10

1.3 TOE overview

In this section, the usage and its major security features are summarised, TOE type and major non-TOE hardware/software required by the TOE are summarised.

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 UGW9811, a unified packet gateway independently developed by Huawei, can be used in GPRS, UMTS, and EPC networks. The UGW9811 can function as a gateway GPRS support node (GGSN), serving gateway (S-GW), PDN gateway (P-GW), or any combination of these three roles, and can be managed individually. The TOE and its environment are shown in Figure 1.

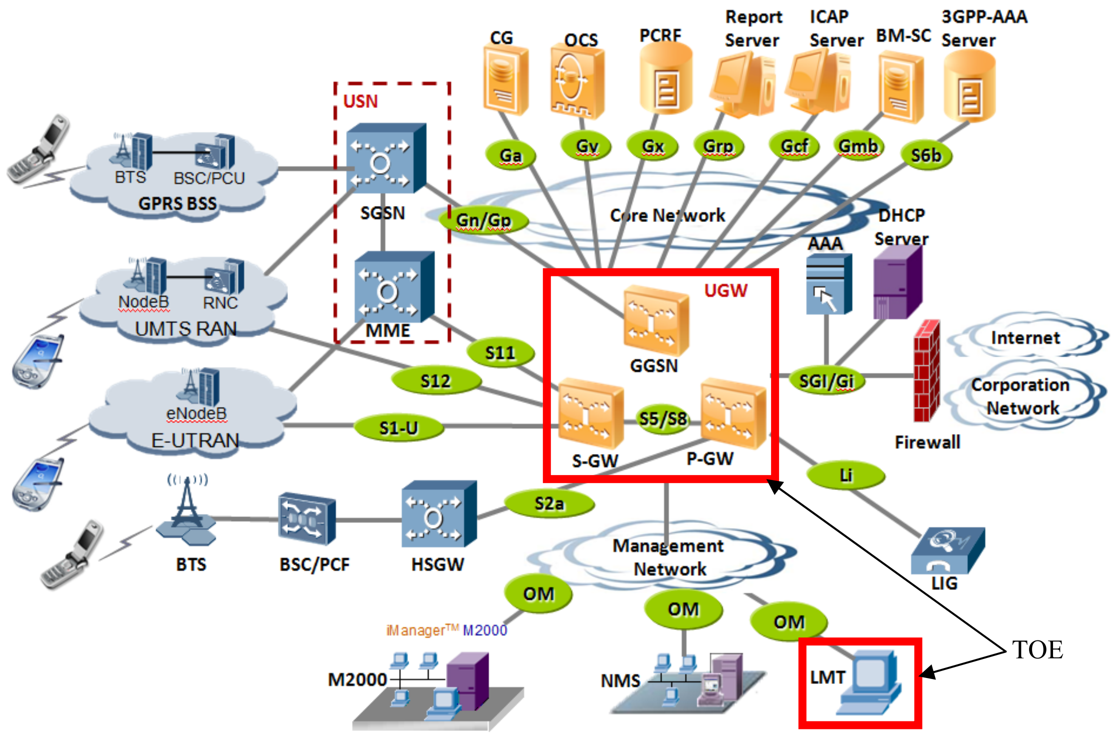

Figure 1 TOE and its environment

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: Boradcast 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**

In the telecommunication service network, the UGW9811 provides the following functions when acted as GGSN/S-GW/P-GW:

1. Acting as an interface between mobile stations (MSs) and external PDNs: The UGW9811 acts as a gateway for MSs to access an external packet data network (PDN). The UGW9811 acts as GGSN which exchanges routing information between MSs and PDN. The UGW9811 serves as a router for all IP addresses of MSs in the GPRS/UMTS/EPC network.

2. Session management: The UGW9811 acts as GGSN which sets up communication between MSs and external PDNs.

3. Mobility management: The UGW9811 acts as a serving-gateway, support Local mobility anchor point for inter-eNodeB handover.

4. Data receiving and processing: The UGW9811 acts as GGSN which receives data from MSs and routes the data to an external PDN. It also receives data from the external PDN, and selects a path in the GPRS/UMTS network to forward the data according to the destination address. Then, it sends the data to the SGSN.

5. Abundant charging functions: The UGW9811 provides the functions of normal charging, hot billing, content-based charging, and online charging.

6. Service awareness: Service awareness (SA) is an application layer-based traffic inspection and control technique. The SA technique has wide applications in areas such as flow-based charging (FBC), bandwidth control, service report, security protection.

- **TOE major security features**

The major security features implemented by the UGW9811 and subject to evaluation are:

Authentication

The authentication feature enables the UGW9811 to identify and authenticate MS users and check the validity of service requests initiated by the MS users to ensure that only valid users can access network services.

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.

Access Control

The TOE offers the management of network devices.

Role-based access control: The TOE implements role-based access control, limiting access to different management functionality to different roles as defined in administrator-defined access control associations. The TOE allows the definition of User Groups, as well as Command Groups in order to define roles that can be assigned to users.

The TOE can limit the user access to the TOE device or application using the ACL (Access Control List) feature by matching information contained in the headers of connection-oriented or connectionless IP packets against ACL rules specified.

The TOE can limit the session establishment in the mobile network using the blacklist/whitelist feature by matching the resource of the session establishment request against the blacklist/whitelist specified.

Communications security

The TOE provides communication security by implementing Secure Sockets Layer (SSL), and Internet Protocol Security (IPsec).

The TOE offers SSL encryption for the communication between the LMT client and the TOE or between the M2000 (Huawei network management system) and the TOE.

Except the OM interface, the IPsec is used in the interface between the TOE and other non-OM network elements such as Gn/Gp/S11 interfaces.

Auditing

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

The TOE classify the audit record into four categories according to the management scope and action: Operation logs, Security logs, System logs and Diagnosis logs.

Security function management

The following means are provided by the TOE for 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/IPsec 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 the following:

- At least two L3 switches to connect to the maintenance network and the telecommunication service network separately
- AAA servers for the 3GPP network and the PDN network to perform MS user authentication
- Firewalls between the server part of the TOE and the various PDN networks

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 five types of boards:

Name	version	Description
SRU/MPU	V900R10C00	Switch and Route Processing Unit/Main Processing Unit, which is the core circuit board for system management. The SRU/MPU collects routing information and generates routing tables. The SRU/MPU serves as the operation and maintenance agent of the system.
SFU	V900R10C00	Switching Fabric Unit, which performs the data exchange function. The SFU switches service data in the entire system and works in 3+1 backup mode to share service data load.
SPU	V900R10C00	Service Processing Unit, which performs the service processing function. The SPU processes all UGW9811 services, including GTP access, charging, and policy

		enforcement.
LPU	V900R10C00	Line Processing Unit, which provides physical interfaces that connect the UGW9811 to NEs or external networks.

The TOE comes with the following software:

Name	Version
UGW9811	V900R010ENGC00SPC200
LMT GUI	V900R010C00

The TOE comes with the following guidance:

Name	Version
HUAWEI UGW9811 Unified Gateway V900R010C00 Product Documentation 06(GGSN&S-GW&P-GW)	V900R010C00, 2013/06/08
UGW9811 NPE Solution Documentation	V900R009C01, 2011/12/15
Common Criteria Security Evaluation – Certified Configuration	V1.2, 2013/11/07

1.4.2 Logical scope of the TOE

See section 1.3.1 “TOE major security features”

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 (instead of ALC_CMC.3), and no other packages

3 Security Problem Definition

3.1 Assets

All data from and to the interfaces available on the TOE is categorized into user data and TSF data.

User Data: The TOE provides the packet service for the mobile user. The user data includes the user data packet of the user to access PDN network and the information of the user such as user identity and user location.

TSF data: The TSF data includes the following type:

1) Audit records.

2) Configuration parameters for the security features such as audit, authentication and authorization, access control, communication etc.

3) Network traffic destined to the TOE processed by security feature and functions.

4) Routing and other network forwarding-related tables, including the following security attributes,

- Network layer routing tables
- Link layer address resolution tables
- BGP, OSPF databases.

5) Management User account data, including the following security attributes

- Management User identities
- Locally managed passwords
- Locally managed access levels

3.2 Threat Agents

The Assets are threatened by the following threat agents:

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

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

TA.ROGUE_SYSTEM: A SGSN/MME/S-GW seeking to connect to the server part of the TOE while there is no resource or they are not allowed to

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

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

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

3.3 Threats

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

T.UNAUTHORIZED_MS: TA.ROGUE_MS_USER tries to access the telecommunication service network/PDN that he/she is not authorized to

T.UNAUTHORIZED: TA.ROGUE_USER tries to access the TOE management function that he/she is not authorized to

T.AUTHORIZED: TA.ROGUE_USER performs actions on the TOE that he/she is allowed to but not desired and these actions cannot be traced back to that specific user

T.UNKNOWN_USER: TA.NETWORK_T or TA.NETWORK_M gains unauthorized access to the TOE and is able to perform actions on the TOE

T.NETWORK_M: TA.NETWORK_M is able to modify/read external network traffic originating from / designated for the TOE and thereby:

- Perform actions on the TOE
- Gain unauthorized knowledge about the traffic between the LMT and the server

T.NETWORK_T: TA.NETWORK_T is able to modify/read external network traffic originating from designated for the TOE and thereby gain unauthorized knowledge about the traffic between the server and LIG, SGSN, MME, RNC, eNodeB, PGW, SGW, PCRF, OCS, 3GPP-AAA server, AAA server, DHCP server, Report server, CHR server, BM-SC, HSGW, ICAP server

T.UnwantedTraffic: TA.NETWORK_T, TA.ROGUE_MS_USER or TA.ROGUE_SYSTEM sends unwanted network traffic to the TOE which consumes the TOE's processing capacity for incoming network traffic, thus fails to process traffic expected to be processed. This may further causes the TOE fails to respond to system control and security management operations.

T.PHYSICAL: TA.PHYSICAL gains physical access to the TOE (either LMT or UGW9811 Server) and is able to perform actions on the TOE.

3.4 Organizational Security Policies

P.ISOLATION: The user must provide security domain isolation of the networks. Different security policies should be deployed for different security domains. In addition, the isolation of the management/control/end-user planes should be designed, in such a way that events on one Security Plane are kept totally isolated from the other Security Planes.

3.5 Assumptions

A. NetworkSegregation: It is assumed that the network interfaces that allow access to the TOE's user interfaces are in a management network that is separate from the application (or, public) networks that the network device hosting the TOE serves.

4 Security Objectives

4.1 Security Objectives for the TOE

O.IDAUTH: The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.

O.IDAUTHMS: The TOE shall support MS user authentication, allowing the TOE to accept/reject the non-3GPP MS users based on the response of the 3GPP AAA servers, and accept/reject MS users accessing PDN networks based on the response of the PDN AAA servers.

O.Resource: The TOE shall provide functionalities and management configuration to prevent traffic overload.

O.Connect: The TOE shall provide functionality to limit other devices (e.g., MS, SGSN/MME/S-GW) from connecting to it

O.Audit: The TOE shall provide functionality to generate audit records for security-relevant administrator actions.

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.

O.Communication: The TOE must implement logical protection measures for network communication between the server and LMT part of the TOE, and the server part of the TOE and various devices in the telecommunication network[1].

4.2 Security Objectives for the Operational Environment

The following security objectives, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

OE.PHYSEC： The operator shall ensure the TOE is protected against unauthorized physical access.

OE.Person: Personnel working as authorized administrators shall be carefully selected for trustworthyness and trained for proper operation of the TOE.

OE.TrustedSystems: The operator shall correctly configure the TOE such that only trusted devices can connect to the TOE

OE.NetworkElements： The operator shall provide:

[1] See T.Network_T

- At least two L3 switches to separate the management network and the telecommunication service network
- 3GPP-AAA server to authenticate the non-3GPP MS user to use the 3GPP network
- PDN AAA server to authenticate the MS user to the PDN network
- Firewall between the server part of the TOE and the PDN networks

OE.NetworkSegregation：The operational environment shall provide segregation by deploying the Ethernet interface on MPU/SRU in TOE into a local sub-network, compared to the interfaces on LPU in TOE serving the application (or public) network.

OE.NetworkSecurity：The operational environment shall provide network security. Different security policies should be deployed for different security domains. In addition, the isolation of the management/control/end-user planes should be designed, in such a way that events on one Security Plane are kept totally isolated from the other Security Planes.

4.3 Security Objectives rationale

The tracing shows how the security objectives trace back to the threats, OSPs and assumptions as described in the security problem definition. The security objectives rationale also demonstrates that all the given threats, OSPs and assumption are addressed.

Threat / OSPs/Assumption	**Objectives**
T.UNAUTHORIZED_MS	The threat of unauthorized access to access the telecommunication service network or the PDN is countered by a requirement that the TOE will authenticate the MS user (O.IDAUTHMS) according to the 3GPP AAA server for the non-3GPP user or the PDN AAA server for users who want to access the PDN. These servers are provided by the operational environment (OE.NetworkElements).
T.UNAUTHORIZED	The threat of unauthorized access to the management function of the TOE or related data is countered by requiring the TOE to implement an authentication and authorization functionality (O.IDAUTH, O.Authorization) In addition, OE.Person ensures that only users that are carefully selected and properly trusted can gain access to certain roles.
T.AUTHORIZED	The threat of users may perform undesired action is countered by OE.Person, which ensures that only users that are carefully selected and properly trusted can gain access to certain roles. Should this prove insufficient, O.Audit will ensure that the actions of the user can be traced back to him.
T.UNKNOWN_USER	The threat that TA.NETWORK_M may gain unauthorized access to the TOE and perform actions on the TOE is countered by requiring the TOE implements authentication mechanism (O.IDAUTH). The threat that TA.NETWORK_T may gain

	unauthorized access to the TOE is countered by providing functionality to limit other devices to connect to the TOE (O.Connect) and the operator shall configure the TOE correctly to only allow trusted systems in the telecommunication network to connect to the TOE (OE.TrustedSystems).
T.NETWORK_M	This threat is countered by providing the SSL to protect the communication between the TOE and the LMT (O.Communication)
T.NETWORK_T	This threat is countered by providing the IPSec to protect the communication between the TOE and the other devices in the telecommunication service network (O.Communication)
T.UnwantedTraffic	This threat is countered by requiring the TOE to prevent internal collapse due to traffic overload (O.Resource) and providing functionality to limit other devices to connect to the TOE (O.Connect), and to request the operator to correctly configure the TOE such that only trusted system can connect to the TOE (OE.TrustedSystems)
T.PHYSICAL	This threat is countered by requiring the operational environment to provide adequate physical security to the TOE (OE.PHYSEC)
P.ISOLATION	This policy is expressed by a corresponding requirement in OE.NetworkSecurity. The devices needed to provide network separation and policy (L3 switches, firewalls) are fulfilled by OE.NetworkElements.
A.NetworkSegregation	The assumption is expressed by a corresponding requirement in OE.NetworkSegregation. The devices needed to provide network segregation is fultilled by OE.NetworkElements.

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.
- ***Italicized and bold text*** indicates the completion of a selection.
- Iteration/N indicates an element of the iteration, where N is the iteration number/character/name.

5.2 TOE Security Functional Requirements

5.2.1 Security Audit (FAU)

FAU_GEN.1 Security 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 requests

ii. user management

1. add, delete, modify

2. password change

3. operation authority change

4. online user query

5. session termination

iii. authentication policy modification

iv. system management

1. reset to factory settings

v. 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), User ID (if applicable), CLI command name (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/a The TSF shall provide the ability to apply **selection** of audit data based on **log level, slot-id for the system log.**

FAU_SAR.3.1/b The TSF shall provide the ability to apply **querying** of audit data based on **date and time range, user ID for the operator log and security log**.

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to ***prevent*** unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall **delete the oldest files** if the audit trail exceeds **the size of store device**.

5.2.2 User Data Protection (FDP)

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **access control policy** on **users as subjects, and commands issued by the subjects targeting the objects.**

FDP_ACF.1 Security attribute based access control

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

a) users and their following security attributes: user level

b) commands and their following security attributes: Command Groups

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **the user has been granted authorization for the commands targeted by the request, and**

- **the user is associated with a Command Group that contains the requested command**

FDP_ACF.1.3 (Refined away)

FDP_ACF.1.4 (Refined away)

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 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" for the LMT 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" for the LMT user.**

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 level

c) password

d) unsuccessful authentication attempt since last successful authentication attempt counter

e) login start and end time.

f) account expiration date for LMT user

g) **password expiration date for LMT user**

FIA_SOS.1 Verification of secrets

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

a) A user name consists of a maximum of 32 letters and numerals and must start with a letter. The user name is case insensitive.

b) **A password is a 6- to 32-character string that contains letters and numerals. The letters are case sensitive. The password must adhere to the password policy.**

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.

FIA_UAU.2/MS User authentication before any action

FIA_UAU.2.1 The TSF shall require each (MS) user to be successfully authenticated (by the 3GPP-AAA server or PDN AAA server) before allowing any other TSF-mediated actions on behalf of that user.

Application note: the 3GPP-AAA server authenticates the MS users form the non-3GPP network (such as CDMA-2000 network), and the PDN AAA server authenticates the MS users who want to access the PDN

FIA_UID.2/MS User identification before any action

FIA_UID.2.1 The TSF shall require each (MS) user to be successfully identified (by the 3GPP-AAA server or PDN AAA server) before allowing any other TSF-mediated actions on behalf of that user.

Application note: the 3GPP-AAA server identifies the MS users form the non-3GPP network (such as CDMA-2000 network), and the PDN AAA server identifies the MS users who want to access the PDN

5.2.4 Security Management (FMT)

FMT_MSA.1 Management of security attributes

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

FMT_MSA.3 Static attribute initialization

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

FMT_MSA.3.2 The TSF shall allow the **nobody** 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, encryption policy**

b) **user management**

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

d) **IP-Based ACL policy**

e) **APN-specific packet filtering based on ACL**

f) **SGSN/MME/S-GW blacklist and whitelist**

g) **IPSEC configuration**

h) **SSL configuration**

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles:

a) **Admin user**

b) **administrator-defined roles**

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.

FPT_STM.1 Reliable time stamps

FPT_STM.1 The TSF shall be able to provide reliable time stamps.

5.2.6 Resource utilization (FRU)

FRU_PRS.1 Limited priority of service

FRU_PRS.1.1 The TSF shall assign a priority (used as configured bandwidth) to each ~~subject~~ (ME user) in the TSF.

FRU_PRS.1.2 The TSF shall ensure that each access to **bandwidth** shall be mediated on the basis of the ~~subjects~~ (ME users) assigned priority.

FRU_RSA.1 Maximum quotas

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: **bandwidth** that (ME users) can use ***simultaneously***.

5.2.7 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 (TSF).

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of **16** sessions per (TSF).

FTA_SSL.1 TSF-initiated session locking

FTA_SSL.1.1 The TSF shall lock an interactive session after **a time interval which can be configured** 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 the 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) authentication

b) source IP address

c) account expiration date

d) password expiration date

e) login start and end time

f) VRF network

g) **VLAN network**

FTA_TSE.1/NE TOE session establishment

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

a) IP-based ACL

b) VRF network

c) VLAN network

FTA_TSE.1/MS TOE session establishment

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

a) **Access Point Name**

b) **The SGSN/MME/S-GW on blacklist**

c) **The SGSN/MME/S-GW not on white list**

d) **Source IP address**

e) **VRF network**

f) **IP-based ACL**

5.2.8 Trusted Path/Channels (FTP)

FTP_ITC.1/M2000 Inter-TSF trusted channel

FTP_ITC.1.1 The ~~TSF~~ (server part of the TOE) shall provide a communication channel between itself ~~and another trusted IT product~~ (M2000) 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~~ (server part of the TOE) shall permit (M2000) to initiate communication via the trusted channel.

FTP_ITC.1.3 The ~~TSF~~ (server part of the TOE) shall initiate communication via the trusted channel for **performing M2000 related actions**.

FTP_ITC.1/LI Inter-TSF trusted channel

FTP_ITC.1.1 The ~~TSF~~ (server part of the TOE) shall provide a communication channel between itself and ~~another trusted IT product~~ (the LIG) 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~~ (server part of the TOE) shall permit (the LIG) to initiate communication via the trusted channel.

FTP_ITC.1.3 The ~~TSF~~ (server part of the TOE) shall initiate communication via the trusted channel for **performing LIG related actions**.

FTP_ITC.1/NE Inter-TSF trusted channel

FTP_ITC.1.1 The ~~TSF~~ (server part of the TOE) shall provide a communication channel between itself and another trusted IT product[2] 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~~ (server part of the TOE) shall permit ***another trusted IT product*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The ~~TSF~~ (server part of the TOE) shall initiate communication via the trusted channel for **performing another trusted IT product related functions**.

[2] See T.Network_T

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.

This level has been chosen because it is commensurate with the threat environment that is experienced by typical consumers of the TOE.

5.4 Rationale for the Security Requirements

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 Objectives	Security Functional Requirements
O.IDAUTH	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). The TOE prevents a user having too many sessions (FTA_MCS.1) and locks session when they are inactive for a configured period of time (FTA_SSL.1). Management functionality for all of these is provided in FMT_SMF.1.
O.IDAUTHMS	MS user authentication is implemented by FIA_UAU.2/MS and FIA_UID.2/MS.
O.Resource	The requirement for assigning a priority (used as configured bandwidth) is spelled out in FRU_PRS.1, enforcing the maximum quotas for bandwidth and limited the bandwidth (used by the MS) is spelled out in FRU_RSA.1
O.Connect	The requirement for limiting other device to access the TOE is spell out in FTA_TSE.1, where connection can be refused based on security attributes like authentication, IP address, account expiration date, and so on. FTA_TSE.1/NE: where connection can be refused based on IP address FTA_TSE.1/MS: where connection can be refused based on Access Point Name (APN)

Security Objectives	Security Functional Requirements
	Management functionality of configuring who is allowed to connect is spell out 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). The loss of audit log is protected (FAU_STG.1, FAU_STG.3). The time stamp required is provided by the TOE (FPT_STM.1). Management functionality for the audit mechanism is spelled out in FMT_SMF.1.
O.Authorization	The requirement for authorization is spelled out in FDP_ACC.1, and the access control policies are modelled in FDP_ACF.1. Unique user IDs and user authentication are necessary for access control provisioning (FIA_UID.2, FIA_UAU.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.3, FMT_MSA.3, FMT_SMF.1).
O.Communication	The requirement to provide secure connection between the LMT and the server part of the TOE is spell out in FPT_ITT.1. The requirements to provide secure communication between the server part of the TOE and other devices (M2000, LIG, devices in the telecommunication networks) are spell out in FTP_ITC.1/M2000, FTP_ITC.1/LI, and FTP_ITC.1/NE. Management functionality to enable these mechanisms is provided in FMT_SMF.1

5.5 Dependencies

SFR	Dependencies
FAU_GEN.1	FPT_STM.1: met
FAU_GEN.2	FAU_GEN1: met FIA_UID.2: met by FIA_UID.2
FAU_SAR.1	FAU_GEN.1: met

SFR	Dependencies
FAU_SAR.3	FAU_SAR.3: met
FAU_STG.1	FAU_GEN.1: met
FAU_STG.3	FAU_STG.1: met
FPT_STM.1	-
FDP_ACC.1	FDP_ACF.1: met
FDP_ACF.1	FDP_ACC.1: met FMT_MSA.3: met
FIA_AFL.1	FIA_UAU.1: met by FIA_UAU.2
FIA_ATD.1	-
FIA_SOS.1	-
FIA_UAU.2	FIA_UID.1: met by FIA_UID.2
FIA_UID.2	-
FIA_UAU.2/MS	FIA_UID.1: met by FIA_UID.2/MS
FIA_UID.2/MS	-
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]: met by FDP_ACC.1 FMT_SMR.1: met FMT_SMF.1: met
FMT_MSA.3	FMT_MSA.1: met FMT_SMR.1: met
FMT_SMF.1	-
FMT_SMR.1	FIA_UID.1: met by FIA_UID.2
FPT_ITT.1	-
FRU_PRS.1	-

SFR	Dependencies
FRU_RSA.1	-
FTA_MCS.1	FIA_UID.1: met by FIA_UID.2
FTA_SSL.3	-
FTA_TSE.1	-
FTA_TSE.1/NE	-
FTA_TSE.1/MS	-
FTP_ITC.1/M2000	-
FTP_ITC.1/LI	-
FTP_ITC.1/NE	-

6 TOE Summary Specification

6.1 Authentication

The TOE provides Point-to-Point Protocol (PPP) security verification by the Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) modes for MS users authentication

The TOE authenticates the users 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 memory. A user must enter the correct user name and password to log in to the UGW9811, which prevents unauthorized access to the UGW9811.

A user name consists of a maximum of 32 letters and numerals and must start with a letter. The user name is case insensitive.

The 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).

To meet the requirements for assigning rights to different users and prevent unauthorized access and operations, the users are categorized into different levels by role and are assigned the corresponding operation rights.

A user group defines a set of rights for different user type. A command group is a set of commands. A user group can be authorized rights via command groups, an user group may include more than one command groups. Commands are classified into command groups, and then the command groups are assigned to users with different authorities, realizing authority management.

Commands are classified into command groups and command groups are assigned to users with different rights. One command belongs to only one specific command group. The system provides eight predefined command groups. The commands contained in these command groups cannot be modified. This means that a command group to which a command belongs cannot be changed, and rights can be assigned only by specifying command groups.

The TOE supports max attempts due to authentication failure within certain period of time. This function is achieved by providing counts on authentication failure.

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.

When a session is inactive for a configured period of time, the TOE will lock this session and the user needs to re-enter his password to unlock the session.

(FDP_ACC.1, FDP_ACF.1, FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UID.2, FIA_UAU.2/MS, FIA_UID.2/MS, FTA_SSL.1, FMT_SMR.1, FMT_MSA.1, FMT_MSA.3)

6.2 Access Control

The access control feature enables carriers to manage user authorities to ensure that only authorized users are allowed to operate the UGW9811 within the authorization range, such as adding, modifying, or deleting users, logging in or logging out users, and assigning rights to users.

The access control feature is implemented in the three planes: management plane, control plane and end-user plane.

In the management plane, the TOE can enforce the account locking function for the LMT user access control.

In the control plane, the access control feature includes:

- Different access control policies for subscribers. These control policies have different priorities, which ensure that subscribers with a higher priority level have priority access to network resources.
- Supports to control the subscriber capacity and the bandwidth. When the number of subscribers or the bandwidth usage reaches the maximum limit, the TOE does not allow new subscribers to access.
- Supports to deny the session establishment request from the blacklisted SGSNs, MMEs, and S-GWs,APN.

In the end-user plane, the TOE supports:

- Bandwidth management to restrict the maximum bandwidth for the specific service(eg, P2P) of the subscriber group.
- IP-based ACL, Blacklist and Whitelist, APN-specific Packet Filtering Based on ACLs
- Anti-spoofing function to check the uplink and downlink user-plane traffic and discards packets from spoofed source IP addresses.
- VRF (Virtual routing and forwarding) and the VLAN(virtual local area network) functions to separate the different network from each other to ensure network security.

6.2.1 Account Locking

The UGW9811 supports a maximum of 16 actives sessions for the LMT login.

For LMT login, when a user is absent, the account can be locked to prevent unauthorized access to the system.

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.

Support limiting access by IP address. This function is achieved by comparing IP address of requesting session with configured value stored in memory.

6.2.2 SGSN/MME/S-GW Blacklist and Whitelist

The UGW9811 supports adding specific IP address ranges of serving GPRS support nodes (SGSNs), mobility management entities (MMEs), and serving gateways (S-GWs) to whitelists or blacklists. The UGW9811 grants access to whitelisted SGSNs, MMEs, and S-GWs and rejects access to blacklisted ones.

By specifying the SGSNs, MMEs, and S-GWs on which subscribers can be activated, carriers can restrict the service usage by or roaming behaviors of subscribers.

The TOE supports to deny the MS session establishment request from the blacklisted SGSNs, MMEs, and S-GWs.

6.2.3 IP-based ACL

The TOE supports IP-based Access Control List (ACL) to filter traffic destined to TOE to prevent internal traffic overload and service interruption.

The TOE also uses the ACL to identify flows and perform flow control to prevent the CPU and related services from being attacked

1) Support enabling ACLs by associating ACLs to whitelist, blacklist, user-defined-flow. This function is achieved by interpreting ACL configurations then storing interpreted value in memory.

2) Support screening, filtering traffic destined to CPU. This function is achieved by downloading ACL configurations into hardware.

3) Support rate limiting traffic based on screened traffic. This function is achieved by downloading configuration of rate into hardware.

The TOE can use the ACL to deny the network's data packet based on some criteria defined in the ACL such as destination ip address, destination port number, ip protocol.

The TOE can flexibly set the ACL rules for the user-defined flows to prevent unidentified attacks in the network. In addition, you can specify the characteristics of the attack data flows and set rules for filtering the data flows of these characteristics.

Besides the above IP-based ACL function for the received IP data packets, the TOE supports the APN-specific packet filtering Based on ACLs. With this function, the UGW9811 checks the uplink and downlink traffic at the user-plane of an access point name (APN) based on an ACL packet filtering policy. The UGW9811 forwards or discards packets that match specific ACL rules. This feature enables the UGW9811 to prevent unauthorized access of UEs or servers on the PDN, therefore protecting the network and subscribers from malicious attacks.

The TOE can use the APN based on ACL to deny the user's data packet based on some criteria defined in the ACL such as destination IP address, destination port number, IP protocol.

(FIA_AFL.1, FTA_MCS.1, FTA_TSE.1, FTA_TSE.1/NE, FTA_TSE.1/MS. FRU_PRS.1, FRU_RSA.1)

6.3 Communication security

The LMT log in the UGW9811 can use the SSL.

The TOE provides a trusted communication channel between the TOW and the SGSNs, MMEs, and S-GWs which are defined in the whitelist.

The TOE provides a trusted communication channel between the TOW and the LIG.

When using maintenance terminals to perform OM operations for the UGW9811, carriers can use SSL to ensure the security of data transmission and maintenance interfaces on the UGW9811.

SSL：

SSL provides the following security services:

- Identity authentication

  Identity authentication means checking whether the individual in communication is an expected object. SSL authenticates servers and clients based on digital certificates to check whether the servers and clients are authorized. Both clients and servers have their own identifiers, which are numbered with the public key. To verify that a user is authorized, SSL requires digital authentication during data exchange in the handshake stage.

- Connection privacy

  Connection privacy means that data is encrypted before transmission to prevent data from being hacked by malicious users. SSL enables confidentiality by using encryption algorithms. Common encryption algorithms are DES, 3DES, RC2, and RC4.

- Data integrity

> Data integrity means that any modification to data during transmission can be detected. SSL establishes a secure channel between the client and the server and uses message digest algorithms to ensure data integrity so that all the data processed by SSL can reach the destination without being modified. Common message digest algorithms are message digest 5 (MD5) and secure hashing algorithm-1 (SHA-1).

The UGW9811 supports SSL versions SSLv3, TLS1.0, and TLS1.1.

IPsec

The UGW9811 supports IPsec. IPsec provides two security protocols to ensure the privacy, integrity, authenticity, and anti-replay of data packets during transmission: Authentication Header (AH) and Encapsulating Security Payload (ESP). Internet Key Exchange (IKE) can automatically negotiate key exchange, and establish and maintain security associations (SAs) to simplify the use and management of IPsec.

(FTP_ITT.1, FTP_ITC.1/M2000, FTP_ITC/LI, FTP_ITC.1/NE)

6.4 Auditing

The logs of the TOE include:

1) Operation logs: Operation logs record the information about operations performed by the user, such as the task name, user name, client IP address, and operation time. An administrator can query for and save users' logs based on specified parameters.

2) Security logs: Security logs record all security events, including user login events, user authentication events, and management events.

3) System logs: System logs record system information, including the black box information, process status, and OS operating error. System logs are used to locate and analyse faults.

4) Diagnostic logs: Application software operation logs (DEBUG_LOG) record the operation log information about the OMU software and NE software. The operation log information includes error information and operation information. Application software operation logs are used to commission the application software and locate faults.

The TOE can provide auditing ability by receiving all types of logs and processing them according to user’s configuration:

The TOE generates audit records for security-relevant events (for example, Operation logs, Security logs, System logs, Application software operation logs). Attempt to access regardless success or failure is logged, along with user id, source IP address, timestamp etc.

For system log，Support classification based on severity level. This function is achieved where logging messages are encoded with severity level and output to log buffer. Support enabling, disabling log output. This function is achieved by interpreting enable/disable commands and storing results in memory. Log output is performed based on this result.

Where appropriate, the data recorded with each audit record includes the unique user ID associated with a subject during authentication. (for example, Operation logs, Security logs)

Audit review

Users can query for operation logs and security logs only after an administrator assigns related rights to the users. By regularly checking logs, an administrator can trace and audit operators' behaviours, find attack behaviours in time, and take measures, such as changing the password and locking the account.

Review functionality is provided via the command line interface, which allows administrators to inspect the audit log.

The TOE supports the authorized users to query for operation logs and security logs based on the query criteria such as operator, start time and end time.

For system log：

1) Support log output screening, based on severity level, regular expression. This function is performed by providing filtering on output.

2) Support querying log buffer. This function is achieved by performing querying operation with conditions input.

3) Support redirecting logs to various output channels: monitor, log buffer, trap buffer, log file. This function is achieved by interpreting commands and storing results in memory or in log files in CF card. Log channel for output is selected prior to execution of redirecting.

Audit Storage

These logs are stored on the hard disk of the SRU/MPU board of the TOE. Only users which have G_6 and G_7 can access these logs files

Each type of log file defines the maximum number of audit records supported to be stored. If the audit record number of the log file exceeds the maximum number threshold, the latest audit record will be dropped. If the storage capacity reached the threshold, the latest log will overwrite the earliest log.

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

6.5 Time

The TOE supports its own clock, to support logging and timed log-outs.

(FPT_STM.1, FTA_SSL.3)

6.6 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:

1) User management, including user name, password, User Group memberships, including the association of users and corresponding privileged functionalities. etc.

2) Access control management, including the blacklists.

3) Enabling/disabling and configuring of SSL.

4) Enabling/disabling and configuring of IPsec

5) Support configuration on session lock when no operation is performed on the user session within a given interval;

6) Support configuration on max attempts due to authentication failure within certain period of time;

7) Support configuration on limiting access by IP address;

8) Support configuration ACLs based on IP protocol number, source and/or destination IP address, source and/or destination port number if TCP/UDP;

9) Support configuration on APN-specific packet filtering Based on ACLs.

10) Support configuration on SGSN/MME/S-GW blacklist and whitelist.

Above functions are achieved by providing interpreting input commands and storing result of interpreting in memory. Some results like routes generated, ACLs will be downloaded into hardware to assist forwarding and other TSF functions.

(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