Huawei Carrier Grade Platform (CGP) Version 1 Release 5 Customization 1 Security Target

Version:	2.0
Last Update:	2014-11-20
Author:	Huawei Technologies Co., Ltd.

Table of Contents

List of Tables

List of Figures

1 Introduction

This Security Target is for the evaluation of Huawei's Carrier Grade Platform (CGP) Version 1 Release 5 Customization 1.

1.1 Security Target Identification

Title:	Huawei Carrier Grade Platform (CGP) Version 1 Release 5 Customization 1 Security Target
Version:	2.0
Date:	2014-11-20
Sponsor:	Huawei Technologies Co., Ltd.
Developer:	Huawei Technologies Co., Ltd.
Keywords:	CGP, core network, network device management

1.2 Target of Evaluation (TOE) Identification

Title:	Huawei Carrier Grade Platform (CGP) software
Version:	Version 1 Release 5 (Unique version identifier: CGP V100R005C01) This evaluation includes the following patch: • V100R005C01SPC506
Sponsor:	Huawei Technologies Co., Ltd.
Developer:	Huawei Technologies Co., Ltd.
Keywords:	Authentication, Role-based access control, Lawful Interception (LI) support, Communications security, Auditing, Security function management.

1.3 Target of Evaluation (TOE) Overview

The TOE is Huawei's Carrier Grade Platform, a software for the management of (cellular) core network devices, such as Home Location Registers, Mobile Softswitch Centers, Service GPRS Support Nodes, or Call Session Control Functions. It is commonly used as a component throughout a number of Huawei networking products to offer management functionality for these products.

The central (server) side of CGP runs within a physical Operation and Management Unit (OMU) on top of a Linux operating system. OMUs are boards (blades) that get inserted into network device cabinets (racks) which also contain application-specific boards, resulting in a product offering. Remote clients (a GUI, called LMT client) are available for management access to the server.

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

- Authentication. Operators using the GUI client to access the TOE in order to execute device management functions are identified by individual user names and authenticated by passwords.
- Role-based access control. CGP implements role-based access control, limiting access to different management functionality to different roles as defined in administrator-defined access control associations.
- Communications security. CGP offers SSL/TLS channels for FTP, and SOAP access to the OMU, as well as the encryption of X1/X2 channels for LIG communication. This includes the possibility to restrict remote sessions to the CGP server to specific client IP addresses.
- Auditing. Audit records are created for security-relevant events related to the use of CGP.
- Security function management. The TOE offers management functionality for its security functionality.

The operational environment of the TOE comprises, on the server side, an operating system that runs within the OMU board hardware and hosts both the TOE and a relational database (which is part of the operational environment as well) used by the TOE to store configuration and audit data.

The LMT client part of the TOE runs on top of a Windows operating system.

The remaining parts of the assembly products, where the TOE is located, are part of the operational environment.

1.4 TOE Description

1.4.1 Architectural overview

The TOE is Huawei's Carrier Grade Platform – in particular the software that provides the Operation Administration and Maintenance (OAM) functionality for core network devices to their users. As depicted in Figure 1, the TOE is implemented based on a client/server architecture – the server functionality is located in the network device itself, while a client GUI – commonly referred to as Local Maintenance Terminal (LMT) – can be run on PCs for remote management of the device.

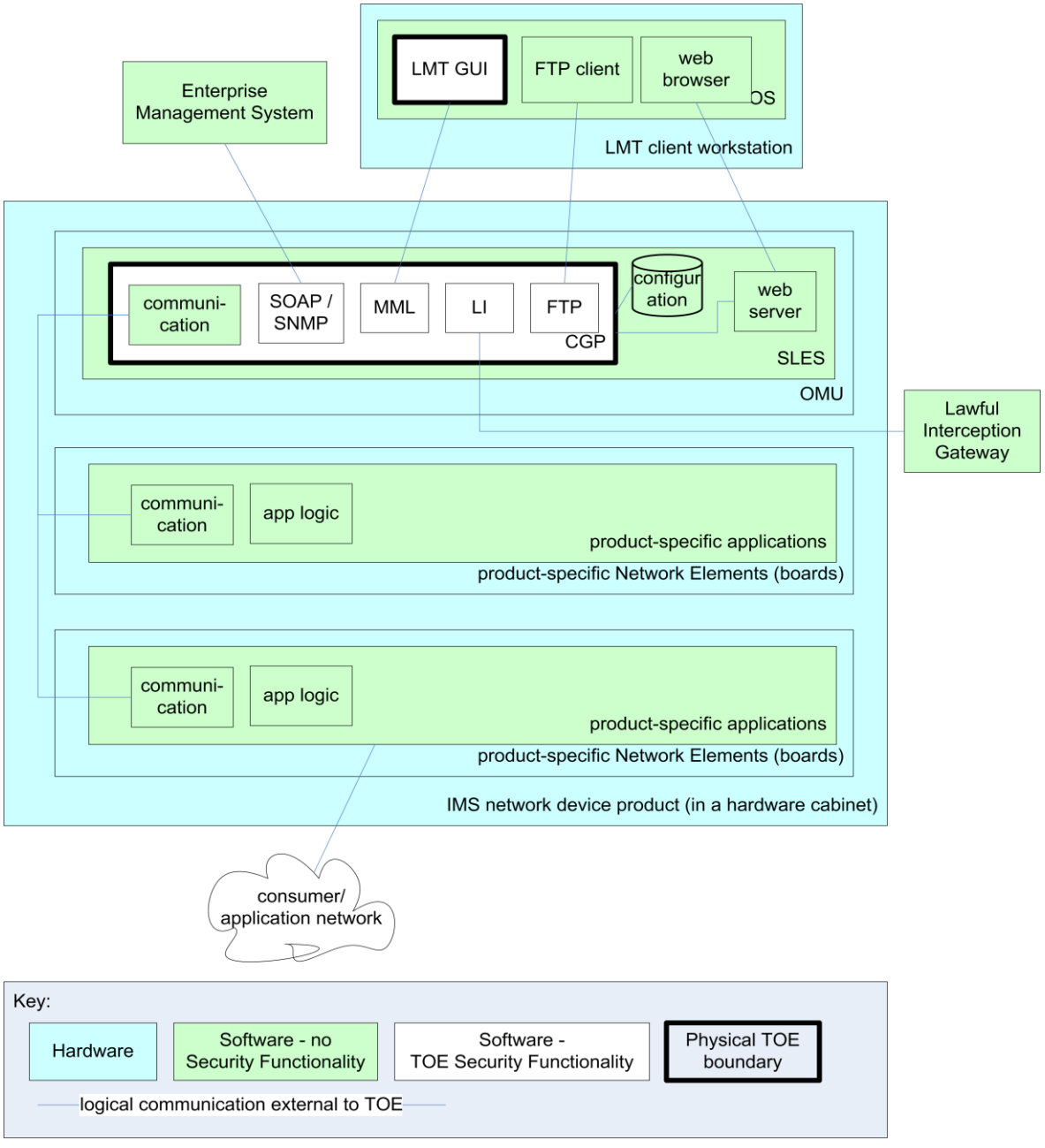

Figure 1: TOE architecture and boundaries

Physically, the server part of the TOE is located on an OMU board, a type of Universal Process Blade that is located within the network device. The TOE server communicates product-internally with application-specific boards (Network Elements) of the product in order to provide management and maintenance functionality for the device.

Remote communication between LMT client and the OMU of a device is based on TCP/IP, it using the proprietary link between the LMT client software and the OMU.

Also, a SOAP interface is available for communication with the operational environment (namely Huawei's Enterprise Management System, a separate product offering), as well as an SNMPv3 interface.

Via these interfaces, the OMU offers management functionality for the network device. To be more precise, the LMT GUI implements security function management.

The TOE supports Lawful Interception (LI) technology. CGP offers the management of LI functionality via X1/X2 channels. In particular, this includes the configuration of communication parameters that instruct CGP how to interoperate with a Lawful Interception Gateway (LIG) in the operational environment for exchanging control messages and alerts.

The TOE stores configuration data, such as user attributes and access control associations, as well as audit records, in a configuration database in the operational environment.

1.4.2 Physical scope

As depicted in Figure 1, the TOE is software only. It is used in a number of Huawei's core network devices that are comprised of elements compatible with the Advanced Telecommunications Computing Architecture (ATCA). Within these networking devices, the OMU board hosting the server part of the TOE is a common board that is paired with different combinations of application-specific boards (network elements). The server part of the TOE is the actual Carrier Grade Platform software running on the OMU that implements the generic device management capabilities for these products. For the guidance of TOE, the registered personnel can download the guidance from Huawei's website: http://support.huawei.com.

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

The server part of the TOE depends on the following hard- and software in its operational environment:

- the cabinet (rack and subrack) housing the OMU and application-specific boards, comprising an actual network device product assembly
- the physical OMU board providing processing resources and physical interfaces
- the operating system running on the OMU, SuSE Linux Enterprise Server 10
- a database product used to store configuration and other maintenance data, PROTON Database based on postgreSQL

The client part of the TOE is comprised of the LMT client, running on a designated LMT workstation. The web browser needed to access the web-based WebUI provided by the server is part of the operational environment.

The client part of the TOE depends on the following hard- and software in its operational environment:

- the workstation providing the processing resources and physical interfaces for the LMT client, or a web browser for access to the WebUI
- Windows 2000/XP/Vista as operating system

The TOE is distributed as a component of a larger product assembly, and the guidance that is part of the TOE is integrated into the product manuals of the individual product.

The product assemblies supported by this evaluation of CGP are:

- Huawei ENS, offering the Domain Name System (DNS) and Telephone Number Mapping (ENUM) in IMS networks
- Huawei CCF, a Charging Gateway for IMS networks, offering an interface for offline charging
- Huawei UGC3200, offering Media Gateway Control Function (MGCF) in IMS networks and Gateway Mobile Switching Center (GMSC) in mobile networks
- Huawei SPG2800, a universal service provisioning gateway, offering the universal northbound service provisioning interface for the IMS components
- Huawei MRP6600, a multimedia resource function processor, is used to carry multimedia resources and supports multimedia services

- Huawei SAE-HSS9820, offering Home subscriber server (HSS) in the evolved packet core (EPC) network and Home location register (HLR) in mobile networks
- Huawei UPCC, a Unified Policy and Charging Controller(UPCC) for IMS networks

The LMT client is shipped with the respective network device.

Please note that the application-specific functionality offered by these product assemblies is not subject to this evaluation. The TOE is only concerned with the provision of operational and maintenance functionality that is common to these products.

1.4.4 Summary of Security Features

1.4.4.1 Authentication

The TOE authenticates its users via individual user names and passwords. 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.

The TOE entertains two user domains: LI user domain and service user domain.

LI user domain includes two roles: LI user super user, and administrator-defined roles of LI user.

Service user domain includes two roles: service user super user, and administrator-defined roles of service user.

LI users differentiate between service users, i.e. the operators responsible for the day-to-day operation of the TOE, and LI users who can access the TOE in order to configure lawful interception functionality to be executed by network elements.

By means of implementing a separate user ID space described above, the TOE ensures that the realms of service and LI management are kept completely separate – service users do not know about the existence of and cannot interfere with the operations of LI users, and vice versa.

1.4.4.2 Access control

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.

The TOE differentiates between service users and LI users by implementing a separate access control functionality for two user domains.

1.4.4.3 Communications security

The TOE offers SSL/TLS encryption for communication between the LMT client and the OMU, and for communication between the operational environment and the TOE via SOAP.

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

CGP implements encryption for the FTPS protocol that allows users to access the FTP server hosted by CGP.

The TOE also implements encryption of the communication between its Lawful Interception module and a Lawful Interception Gateway in the operational environment, commonly referred to as the X1 / X2 interfaces.

1.4.4.4 Auditing

The TOE records and reviews audit data, which is stored in the database and it can be queried using TOE-provided tools (i.e., via the LMT client).

The TOE differentiates between service users and LI users, service users can use the LMT client to review the audit records available in the database for everything except LI-related actions. LI users can review only audit records related to LI functionality and actions initiated by LI users.

1.4.4.5 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)
- Supporting of SSL for communications security.
- Enabling and disabling of the LI feature.

1.4.5 Logical Scope

1.4.5.1 Evaluated configuration

The evaluated configuration of CGP is based on the physical and logical scope and security functions described above. In addition, the following configuration specifics are applicable to the TOE:

- CGP supports standby configurations between two OMUs for the same product. This functionality has not been evaluated.
- CGP supports LI user security management, during the evaluation **SET TTSEC** command must be executed to enable the LI user security function.
- CGP supports DES encryption for various communication channels, such as the channel between CGP and a Lawful Interception Gateway, for legacy reasons. This evaluation does not cover the use of the DES algorithm for LI feature.
- CGP supports DES for encryption of configuration data. During the evaluation CGP must be configured so that AES is used instead of DES for LI feature.
- CGP supports COMMON communication between LMT clients and the OMU. This evaluation does not cover the use of the COMMON communication. During the evaluation CGP must be configured so that SSL communication mode is used instead of COMMON communication mode.
- CGP supports DES communication between the operational environment (EMS server) and the OMU in SNMP interface. During the evaluation CGP must be configured so that the parameters **SNMP Protocol version** as **SNMPv3**, and **Private protocol** as **DES (CBC-DES)**.
- CGP supports security policy, during the evaluation security policy data must be configured and parameters value should be:
    - Password policy = Enable
    - Change password upon first login = Enable
    - Password expiration warning period(day), customized account default as 5 and build-in account default as 20
    - Minimum password length = 8
    - Character set, enable all character sets.
    - Enforce password history = 5
    - Enforce password days = 10
    - Minimum password age, customized account default as 5 and build-in account is not available.
    - Account lockout policy = Enable
    - Number of login attempts before lockout = 5
    - Count reset interval(minute) = 10
    - Lockout duration(minute) = 30
    - Unused account lockout period(day), customized account default as 30 and build-in account is not available.
    - Repeated login rejection policy = Enable
- CGP supports session establishment management. During the evaluation the parameters value of **Account validity period, Password validity period**, **Start login time**, and **End login time** must be specified when adding the new user through the **ADD USER** command.

- CGP supports workstation management. During the evaluation workstation access control function must be enabled through the **SET WS** command.
- CGP supports network time protocol, during the evaluation the parameter values of **Authentication flag** must be configured as **Yes**, and other parameters value should match with the NTP server side when adding the NTP server data through the **ADD NTPSVR** command.

2 CC Conformance Claim

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

This ST is EAL3-conformant as defined in [CC] Part 3.

No conformance to a Protection Profile is claimed.

3 TOE Security Environment

3.1 Assets

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

- **User data**: User Data is information stored in TOE resources that can be operated upon by users in accordance with the TSP and upon which the TSF places no special meaning. In this category falls all data that is not listed under TSF data since according to the CC, all data is either user or TSF data. For example, user data includes performance data collected from Managed Elements that the TOE makes available to users upon request.
- **TSF data**: TSF data is information used by the TSF in making TSP 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
    - AES keys for encryption of X1/X2 communication channels
    - the **security attributes** given below for the objects they belong to:
        - for users:
            - passwords
            - unsuccessful authentication attempt since last successful authentication attempt counter
            - User Group membership
            - account expiration date
            - password expiration date
            - login start and end time
        - for Managed Objects:
            - Managed Object Group membership

3.2 Threats

The assumed security threats are listed below.

The **information assets** to be protected comprise the information stored, processed or generated by the TOE. This information contains configuration data for the network device that the TOE is a part of, TSF data (such as user account information and passwords, audit records, etc.) and other information that the TOE facilitates access to (such as performance data of the individual elements in the product).

The **threat agents** can be categorized as either:

1. A user (not a user of the TOE) who gets access to data communicated over unprotected networks (“remote attacker”). This person has no access to the TOE interfaces and no access to the system the TOE is integrated into.
2. A user (not a user of the TOE) who gains access to the TOE.
3. An authorized user of the TOE who has been granted authority to access certain information and perform certain actions.

In the first and second cases, the users are assumed to be potentially hostile with a clear motivation to get access to the data.

In the third case, all authorized users of the TOE are entrusted with performing certain administrative or management activities with regard to the managed device. Consequently, organizational means are expected to be in place to establish a certain amount of trust into these users. However,

accidental or casual attempts to perform actions or access data outside of their authorization are expected.

3.2.1 Threats

T.AccountabilityLoss	Records of security-relevant actions of users for forensic and accountability purpose are not created properly.
T.Eavesdrop	An eavesdropper (remote attacker) in the management network that is served by the TOE is able to intercept, and potentially modify or re-use, information assets that are exchanged between TOE (LMT) client and the TOE server part (OMU).
T.UnauthenticatedAccess	A user who is not a user of the TOE gains access to the TOE.
T.UnauthorizedAccess	A user of the TOE authorized to perform certain actions and access certain information gains access to commands or information he is not authorized to access.

3.3 Assumptions

3.3.1 Environment of use of the TOE

3.3.1.1 Physical

A.PhysicalProtection	It is assumed that the TOE and its operational environment (in particular, the network device that the TOE is a component of, but also the workstation that is hosting the client part of the TOE) are protected against unauthorized physical access.

3.3.1.2 Personnel

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 belong to administrators group are assumed to be fully trustworthy and capable of operating the TOE in a secure manner abiding by the guidance provided to them. Note that the users who do not belong to administrators group or unauthorized, are untrustworthy and not eligible for this assumption.)

3.3.1.3 Connectivity

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. This includes the assumption that the operational environment implements measures that ensure that the source IP address in remote client session establishment requests has not been tampered with, and that no bogus OMU servers exist in the management network.
A.Support	The operational environment must provide the following supporting mechanisms to the TOE: • Reliable time stamps for the generation of audit records. • The database that stores the data of TOE must be protected and available.

4 Security Objectives

4.1 Objectives for the TOE

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

O.Communication The TOE must implement logical protection measures for network communication between the server part of the TOE and both clients that are part of the TOE and that are part of the operational environment.

O.Authentication The TOE must authenticate users of its user interfaces.

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

4.2 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 OMU, and in particular to the part of the TOE and its data that is running on the OMU. This includes ensuring that audit records stored 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 network device that contains the OMU to authorized personnel, and making the OMU unavailable to access from the consumer/application networks served by the network device.

The TOE must be operated in its evaluated configuration as specified in this ST and the guidance that is part of the TOE.

OE.Support Those responsible for the operation of the TOE and its operational environment must ensure that the operational environment provides the following supporting mechanisms to the TOE:

- Reliable time stamps for the generation of audit records.
- The database that stores the data of TOE must be protected and available.

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. Note that the users who do not belong to administrators group or unauthorized, are untrustworthy and not eligible for this environmental objective.

4.3 Security Objectives Rationale

4.3.1 Coverage

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

Objective	Threat / Policy
O.Audit	T.AccountabilityLoss
O.Communication	T.Eavesdrop
O.Authentication	T.UnauthenticatedAccess

O.Authorization	T.UnauthorizedAccess

Table 1: Mapping Objectives to Threats and Policies

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

Environmental Objective	Threat / Assumption / Policy
OE.Administration	A.NetworkSegregation A.PhysicalProtection
OE.Support	A.Support
OE.Users	A.TrustworthyUsers

Table 2: Mapping Objectives for the Environment to Threats, Assumptions and Policies

4.3.2 Sufficiency

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

Threat	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 on the OMU 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 for its users (O.Authentication).
T.UnauthorizedAccess	The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism (O.Authorization).

Table 3: Sufficiency analysis for threats

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

Assumption	Rationale for security objectives
A.NetworkSegregation	The assumption that the TOE is not accessible via the application networks hosted by the networking device is addressed by requiring just this in OE.Administration.
A.PhysicalProtection	The assumption that the TOE will be protected against unauthorized physical access is expressed by a corresponding requirement in OE.Administration.
A.Support	Assumptions on support for the TOE's security functionality provided by the operational environment are addressed in OE.Support.
A.TrustworthyUsers	The assumption that users are trained and trustworthy is expressed by a

	corresponding requirement in OE.Users.

Table 4: Sufficiency analysis for assumptions

5 Extended Components Definition

No extended components have been defined for this ST.

6 Security Requirements

6.1 TOE Security Functional Requirements

The following table shows the Security functional requirements for the TOE, and the operations performed on the components according to CC part 2: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.). Typographical distinctions are used throughout this chapter in the reproduction of the SFRs to further identify these operations: assignments and selections are formatted in **bold**, refinements in ***bold and italics***, and iterations by appending an alphabetic counter (a, b, c, …) to the component identifier.

Security Functional Class	Security Functional Requirement	Component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
Security Audit (FAU)	FAU_GEN.1 Audit data generation	FAU_GEN.1	CC Part 2	No	No	Yes	Yes
	FAU_GEN.2 User identity association	FAU_GEN.2	CC Part 2	No	No	No	No
	FAU_SAR.1 Audit review	FAU_SAR.1	CC Part 2	No	No	Yes	No
	FAU_SAR.3 Selectable audit review	FAU_SAR.3	CC Part 2	No	No	Yes	No
	FAU_STG.3 Action in case of possible audit data loss	FAU_STG.3	CC Part 2	No	Yes	Yes	No
Cryptographic Support (FCS)	FCS_COP.1: Cryptographic operation	FCS_COP.1a	CC Part 2	Yes	No	Yes	No
	FCS_COP.1: Cryptographic operation	FCS_COP.1b	CC Part 2	Yes	No	Yes	No
User Data Protection (FDP)	FDP_ACC.1: Subset access control	FDP_ACC.1	CC Part 2	No	No	Yes	No
	FDP_ACF.1: Security attribute based access control	FDP_ACF.1	CC Part 2	No	No	Yes	No
Identification and Authentication (FIA)	FIA_AFL.1: Authentication failure handling	FIA_AFL.1	CC Part 2	No	Yes	Yes	Yes
	FIA_ATD.1: User attribute definition	FIA_ATD.1	CC Part 2	No	No	Yes	No
	FIA_SOS.1: Verification of secrets	FIA_SOS.1	CC Part 2	No	No	Yes	No
	FIA_UAU.2: User authentication before any action	FIA_UAU.2	CC Part 2	No	No	No	No
	FIA_UID.2: User identification before any action	FIA_UID.2	CC Part 2	No	No	No	No
Security Management (FMT)	FMT_MSA.1: Management of security attributes	FMT_MSA.1	CC Part 2	No	No	Yes	Yes
	FMT_MSA.3: Static attribute initialization	FMT_MSA.3a	CC Part 2	Yes	Yes	Yes	Yes
	FMT_MSA.3: Static attribute initialization	FMT_MSA.3b	CC Part 2	Yes	Yes	Yes	Yes
	FMT_SMF.1: Specification of Management Functions	FMT_SMF.1	CC Part 2	No	No	Yes	No
	FMT_SMR.1: Security roles	FMT_SMR.1	CC Part 2	No	No	Yes	No
Protection of the TSF (FPT)	FPT_ITT.1: Basic internal TSF data transfer protection	FPT_ITT.1	CC Part 2	No	No	No	Yes
TOE Access (FTA)	FTA_TSE.1: TOE session establishment	FTA_TSE.1	CC Part 2	No	No	Yes	No

Security Functional Class	Security Functional Requirement	Component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
Trusted Path/Channels (FTP)	FTP_TRP.1: Trusted path	FTP_TRP.1	CC Part 2	No	Yes	Yes	Yes

Table 5: Security Functional Requirements of the TOE

6.1.1 Security Audit (FAU)

6.1.1.1 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. system management

1. LI function enabled, disabled

viii. log management

1. log policy modification

ix. LI information management

1. modification of configuration settings

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).**

6.1.1.2 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.

6.1.1.3 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.

6.1.1.4 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**.

6.1.1.5 FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall **delete the oldest audit records every hour** if the audit trail exceeds **200,000 entries**.

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_COP.1a Cryptographic operation

FCS_COP.1.1a The TSF shall perform **symmetric de- and encryption** in accordance with a specified cryptographic algorithm **AES (ECB mode)** and cryptographic key sizes **128 bits** that meet the following: **None**.

6.1.2.2 FCS_COP.1b Cryptographic operation

FCS_COP.1.1b The TSF shall perform **symmetric de- and encryption** in accordance with a specified cryptographic algorithm **DES (CBC-DES)** and cryptographic key sizes **56 bits** that meet the following: **None**.

6.1.3 User Data Protection (FDP)

6.1.3.1 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**.

6.1.3.2 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 type (service user or LI user)

ii. User Group membership

iii. 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) If the user is a service user, the request is granted if:

i. 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

ii. 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

iii. 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

b) If the user is an LI user, the request is granted if:

i. the user has been granted ME authorization for the Managed Element targeted by the request, and

ii. the user is member of a User Group that is authorized to perform the requested command or query

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

a) Service users cannot

i. perform LI operations

ii. disable the TOE's LI feature

b) LI users cannot

i. perform service operations

ii. enable the TOE's LI feature

6.1.4 Identification and Authentication (FIA)

6.1.4.1 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"**.

6.1.4.2 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 type (service user or LI user)**
- **c) password**
- **d) unsuccessful authentication attempt since last successful authentication attempt counter**
- **e) User Group membership**
- **f) ME authorizations**
- **g) account expiration date**
- **h) password expiration date**
- **i) login start and end time.**

6.1.4.3 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**.

6.1.4.4 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.

6.1.4.5 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.

6.1.5 Security Management (FMT)

6.1.5.1 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**.

6.1.5.2 FMT_MSA.3a Static attribute initialization

FMT_MSA.3.1a The TSF shall enforce the **CGP access control policy** to provide **permissive** default values for security attributes ***Managed Object Group membership(all service users are associated with the "PUBLIC" MOG by default)*** that are used to enforce the SFP.

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

6.1.5.3 FMT_MSA.3b Static attribute initialization

FMT_MSA.3.1b 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.3.2b The TSF shall allow **administrator-defined roles, service user super users** to specify alternative initial values to override the default values when an object or information is created.

6.1.5.4 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) configuration of Account lockout policy (if enabled, an administrator configurable Lockout duration as 30 minutes and Unused account lockout period as 30 days by default)

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

e) definition of Managed Object Groups and Command Groups

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

g) enabling/disabling of the TOE's LI feature.

6.1.5.5 FMT_SMR.1 Security roles

FMT_SMR.1.1 **Th**e TSF shall maintain the roles

a) administrator-defined roles of service user (assigned privileges to perform service management commands, and defined by service administrator through User Groups, Command Groups, and Managed Object Groups)

b) service user super user (assigned privileges to control all client resources, creates other users, grants rights to other users, and executes all the operations provided by the OMU)

c) LI user super user (assigned privileges to perform all LI data configuration and LI user management)

d) administrator-defined roles of LI user (assigned privileges to perform LI data configuration and LI user management, and defined by LI administrator through User Groups)

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

6.1.6 Protection of the TSF (FPT)

6.1.6.1 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.

6.1.7 TOE access (FTA)

6.1.7.1 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.

6.1.8 Trusted Path/Channels (FTP)

6.1.8.1 FTP_TRP.1 Trusted path

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

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for **initial user authentication, remote management**.

6.2 Security Functional Requirements Rationale

6.2.1 Coverage

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

Security Functional Requirements	Objectives
FAU_GEN.1	O.Audit
FAU_GEN.2	O.Audit
FAU_SAR.1	O.Audit
FAU_SAR.3	O.Audit
FAU_STG.3	O.Audit
FCS_COP.1a	O.Communication
FCS_COP.1b	O.Communication
FDP_ACC.1	O.Authorization
FDP_ACF.1	O.Authorization
FIA_AFL.1	O.Authentication
FIA_ATD.1	O.Authentication O.Authorization
FIA_SOS.1	O.Authentication
FIA_UAU.2	O.Authentication
FIA_UID.2	O.Audit

Security Functional Requirements	Objectives
	O.Authentication O.Authorization
FMT_MSA.1	O.Authorization
FMT_MSA.3a	O.Authorization
FMT_MSA.3b	O.Authorization
FMT_SMF.1	O.Audit O.Authentication O.Authorization O.Communication
FMT_SMR.1	O.Authorization
FPT_ITT.1	O.Communication
FTA_TSE.1	O.Authentication
FTP_TRP.1	O.Communication

Table 6: Mapping SFRs to objectives

6.2.2 Sufficiency

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

Security objectives	Rationale
O.Audit	The generation of audit records is implemented by FAU_GEN.1. Audit records are supposed to include user identities (FAU_GEN.2) where applicable, which are supplied by the 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). Functionality to delete oldest audit records is provided if the amount of records in the database becomes too large (FAU_STG.3). Management functionality for the audit mechanism is spelled out in FMT_SMF.1.
O.Communication	Communications security is implemented by the establishment of a secure communications channel between TOE parts in FPT_ITT.1, and a trusted path for remote users in FTP_TRP.1. FCS_COP.1a addresses the AES encryption of X1/X2 channels, and FCS_COP.1b addresses the DES encryption of SNMPv3 interface. Management functionality to enable these mechanisms is provided in FMT_SMF.1.
O.Authentication	User authentication is implemented by FIA_UAU.2 and supported by individual user identifies in FIA_UID.2. The necessary user attributes (passwords) are spelled out in FIA_ATD.1. The authentication mechanism supports authentication failure handling (FIA_AFL.1), restrictions as to the validity of accounts for logon (FTA_TSE.1), and a password policy (FIA_SOS.1). Management functionality is provided in FMT_SMF.1.
O.Authorization	The requirement for access control 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).

Table 7: SFR sufficiency analysis

6.2.3 Security Requirements Dependency Rationale

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

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

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

Security Functional Requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	Not resolved. Time stamps are provided to the TOE by the operational environment. This is spelled out in A.Support / OE.Support.
FAU_GEN.2	FIA_UID.1	FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.3	FAU_STG.1	Not resolved. Audit records are stored in (and protected by) the operational environment.
FCS_COP.1a	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Not resolved. Keys are configured manually by administrators and stored in the configuration database. They may be deleted or replaced in the database, i.e. key destruction is addressed in the operational environment.
FCS_COP.1b	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Not resolved. Keys are configured manually by administrators and stored in the configuration database. They may be deleted or replaced in the database, i.e. key destruction is addressed in the operational environment.
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.3a	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_MSA.3b	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_TRP.1	None	

Table 8: Dependencies between TOE Security Functional Requirements

6.3 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 components as specified in [CC] Part 3. No operations are applied to the assurance components.

6.4 Security Assurance Requirements Rationale

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

7 TOE Summary Specification

7.1 TOE Security Functionality

7.1.1 Authentication

The TOE differentiates between service users and Lawful Interception (LI) users, as further described in section 7.1.2. The authentication mechanism for both types of users is the same, but user and policy management for the two realms is separated as described below.

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.

In order to avoid collisions in the name space for service users and Lawful Interception (LI) users (see also section 7.1.2), LI user IDs are always preceded by "tt\".

For services users, 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).

A separate policy with the same configuration options can be specified for LI users.

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. Separate policies with the same configuration options exist for both service users and LI users.

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 service and LI users), the LI interface used by a Lawful Interception Gateway, 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)

7.1.2 Access control

Access control is enforced on two levels:

On a high level, the TOE differentiates between service users and lawful interception (LI) users. Service users do not have any access to LI functionality or configuration data, and vice versa. Depending on the type of user, the corresponding access control mechanism below applies.

The LI functionality of the TOE can be en- and disabled. If the LI functionality is disabled, only authorized administrators from the service user population can enable it. If the LI functionality is enabled, only authorized administrators from the LI user population can disable it.

The operations of LI users and service users are completely separated in the TOE on a logical basis. As far as security functionality is concerned, the management functionality available to both service and LI users is widely the same: user populations can be managed the same for both user types, password policies and account lockout policies can be defined separately for LI users and service users, and audit record are created in both "realms" and then made available to authorized users of the respective realm: service users can review records related to service operations (such as, actions initiated by service users for the configuration of network elements) but not related to LI operations (such as, definition of interception targets), and vice versa.

LI users cannot logon to the TOE if the LI functionality is disabled.

7.1.2.1 Access control – service users

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 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 OMU user (if the ME in question is the OMU itself). 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 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 can not.

- 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)

7.1.2.2 Access control – LI users

The access control mechanism for LI users works as follows:

- Three pre-defined User Groups (Administrators, Operators, Users) exist. They define the commands that a LI user can execute. (For example, only members of the Administrators group can manage other LI users.)
- ME authorizations are implemented in the same fashion as for service users. LI users can be authorized to perform the operations granted by their User Group association on specific MEs.

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

- A hard-coded user tt/Admin exists who is a member of the Administrator Group, and thus, can perform all management commands that are available to LI users.
- A LIG user exists that is used to authenticate the LI Gateway in the operational environment that can be used to set up and monitor lawful interception activities.

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

7.1.3 Communications security

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

- MML connections between LMT clients and the OMU (using SSLv3/TLS 1.0/TLS 1.1)
- SOAP connections between the operational environment (EMS server) and the OMU (using SSLv3/TLS 1.0/TLS 1.1)
- FTPS between the operational environment and the OMU (using SSLv3/TLS 1.0/TLS 1.1)
- XI / X2 interface between the LIG in the operational environment and the OMU (using AES)
- SNMP connections between the operational environment (EMS server) and the OMU (using DES)

For communication between the TOE's LI module and a Lawful Interception Gateway in the operational environment via so called X1 (control instructions) and X2 (event notification) channels, the TOE implements AES encryption as defined in FCS_COP.1a:

The TOE and the LIG agree on a randomly generated AES session key that is exchanged in an AES-encrypted message using a FixKey, a static key configured by administrators via the LMT interface and stored in the TOE's configuration database.

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 and LI users exist.

For communication between the TOE's SNMP module and EMS server in the operational environment via SNMPv3 protocol, the TOE implements DES encryption as defined in FCS_COP.1b:

The TOE and the EMS server use the DES algorithm to encrypt and decrypt SNMP messages obey the SNMPv3 protocol with the same private key which must be configured on both sides before communicating.

(FCS_COP.1a, FCS_COP.1b, FPT_ITT.1, FTA_TSE.1, FTP_TRP.1)

7.1.4 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 to comprise the logs relevant for the security functionality modeled in this ST:

- an operation log, containing the audit records for particular MML operations performed by service users
- a security log, containing audit records for security-related events, such as user login and management

These logs are stored in the operational environment, i.e. in the database that is used by CGP to store configuration and other data. The TOE will delete the oldest records from the database if the audit records stored exceed 200,000 entries, in order to keep the database from overflowing.

Service users can use the LMT client to review the audit records available in the database for everything except LI-related actions. LI users can review only audit records related to LI functionality and actions initiated by LI users. 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, FAU_STG.3)

7.1.5 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:

- User management, including User Group memberships, passwords, account lockout, validity periods for an account and/or password, etc.
- 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.
- Supporting of SSL for the communication between LMT clients and the OMU.
- Defining IP addresses and address ranges for clients that are allowed to connect to the OMU server.
- Configuration of a FixKey (static key) stored in the TOE's configuration database and used for the negotiation of session keys for LI traffic encryption.
- Enabling and disabling of the LI feature.

All of these management options are typically available both via the LMT GUI and the MML CLI.

(FMT_SMF.1)

8 Abbreviations, Terminology and References

8.1 Abbreviations

CC	Common Criteria
CGP	Carrier Grade Platform
CLI	Command Line Interface
GUI	Graphical User Interface
ID	Identifier
IMS	IP Multimedia Subsystem
LI	Lawful Interception
LMT	Local Maintenance Terminal
ME	Managed Element
MML	Man Machine Interface
MOG	Managed Object Group
NE	Network Element
OAM	Operation Administration and Maintenance
OMU	Operation and Management Unit
PP	Protection Profile
RDBMS	Relational Database Management System
SFR	Security Functional Requirement
SLES	SuSE Linux Enterprise Server
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

8.2 Terminology

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

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

LI User: A user in the Lawful Interception realm of the TOE. Those users are managed separately from Service Users of the TOE.

Managed Element
Operational unit of a product. For example, a signaling or switching unit.

Managed Element authorization
Authorization to access/see a Managed Element. See section 7.1.2.

Managed Object Objects of a Managed Element that can be configured or queried. (E.g., a network interface.)

Managed Object authorization
Authorization to modify objects of a Managed Element. See section 7.1.2.

Operator See User.

Operation authorization
Authorization to perform a specific command on a Managed Element. See section 7.1.2.

Service User: A user in the service realm of the TOE. Those users are responsible for the operational management of the TOE and the products managed by the TOE from the carrier perspective. They are managed separately from the Lawful Interception (LI) Users of the TOE.

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

8.3 References

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

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