LIMA management system

Whitepaper

Confidential - Group 2000 Proprietary

Document Id: **100-WPR-0030-1v1E**

Issue Date: **04 May, 2010**

Disclaimer of Warranties and Limitation of Liabilities

Group 2000 Nederland B.V. has taken due care in preparing this document. However, nothing contained herein modifies or alters in any way the standard terms and conditions of the Group 2000 Nederland B.V. purchase, lease, or license agreement by which the product was acquired, nor increases in any way Group 2000's liability to the customer. In no event shall Group 2000 Nederland B.V. be liable for incidental or consequential damages because of information contained in this accompanying document or any related materials.

All trademarks are acknowledged.

Non-disclosure notice

This document is disclosed for the use by personnel only and may contain information which is privileged, confidential, proprietary, or exempt from disclosure under a mutual Non-Disclosure Agreement. If you are not the intended recipient, you are strictly prohibited from disclosing, distributing, copying, or in any way using the information contained in this document. If you have received this document in error, please destroy and delete any copies you may have received.

Group 2000 Nederland B.V.
Van der Hoopweg 1
7602 PJ Almelo
P.O. Box 333
7600 AH Almelo
The Netherlands
Tel:	+31 - 546 - 482400
Fax	+31 - 546 - 482401

Group 2000 Nederland B.V. is a division of GROUP 2000 AG Switzerland.

Copyright Group 2000 Nederland B.V., 2010. All rights reserved.

Glossary

Abbreviations	
AF	Administration Function
AJAX	Asynchronous JavaScript Technology and XML
AO	Authorized Organization
BL	Business Logic
BLL	Business Logic Layer
CC	Contents of Communication
CDMA	Code Division Multiple Access
CEO	Chief Executive Officer
CMTS	Cable Modem Termination System
CSP	Communication Service Provider
DHCP	Dynamic Host Configuration Protocol
DL	Distribution Logic
DLL	Distribution Logic Layer
DR	Data Retention
ETSI	European Telecommunications Standardization Institute
EU	European Union
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GSN	GPRS Support Node
GUI	Graphical User Interface
GWF	Group2000 Web Framework
GWT™	Google Web Toolkit™
HI1	Handover Interface Port 1 (for LI Administrative Information)
HI2	Handover Interface Port 2 (for LI Intercept Related Information)
HI3	Handover Interface Port 3 (for LI Content of Communication)
HI-A	Handover Interface Port A (for RD disclosure management)
HI-B	Handover Interface Port B (for disclosed RD)
HLR	Home Location Register
HTTPS	Secure HyperText Transfer Protocol
IDR	Interception Detail Record
IMEI	International Mobile station Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IRI	Intercept Related Information
ISP	Internet Service Provider

Abbreviations	
LDAP	Lightweight Directory Access Protocol
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIMA	Lawful Interception Mediation Architecture
MAC	Media Access Control
MF2	Mediation Function 2
MF3	Mediation Function 3
MS	LIMA Management System
MSC	Mobile Switching Centre
NE	Network Element
OMMI	Open Mediator Management Interface
PP	Provisioning Plan
PS	Packet Switched
PSTN	Public Switched Telephony Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RD	Retained Data
RMI	Remote Method Invocation
SBC	Session Border Controller
SCA	Group2000 Service Component Architecture
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
SSO	Single Sign-On
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identification
UTC	Universal Time Coordinated
VoIP	Voice over Internet Protocol
WCDMA	Wideband CDMA
WSDL	Web Services Description Language
XML	eXtensible Markup Language

Copyright Group 2000 Nederland B.V., 2010. All rights reserved.

Table of contents

Copyright Group 2000 Nederland B.V., 2010. All rights reserved.

1 Introduction

LIMA is Group 2000's Lawful Interception Mediator Architecture. It is a flexible architecture for solutions that manage, intercept and mediate traffic for lawful interception and data retention purposes. Due to its modular architecture LIMA solutions can be integrated into any network environment. LIMA solutions are available for PSTN, GSM, GPRS, UMTS, WCDMA, IP, VoIP and Email traffic.

The LIMA product line consists of the following components:

- LIMA Management System

  Automated warrant handling and network provisioning
  Automated disclosure request handling
  Configuration of infrastructure for LI and DR

- LIMA Mediator

  Conversion of intercepted traffic into the required handover protocols

- LIMA Monitor

  Monitoring solutions for passive interception of traffic

- LIMA Store

  Historical database for retaining data

The LIMA Management System is the central component in a LIMA lawful interception solution. It provides a secure web-based interface via which authorized personnel can manage and oversee the lawful interception warrants and data retention disclosure requests. The LIMA Management System also plays a vital role in the provisioning of all systems that are involved in intercepting traffic.

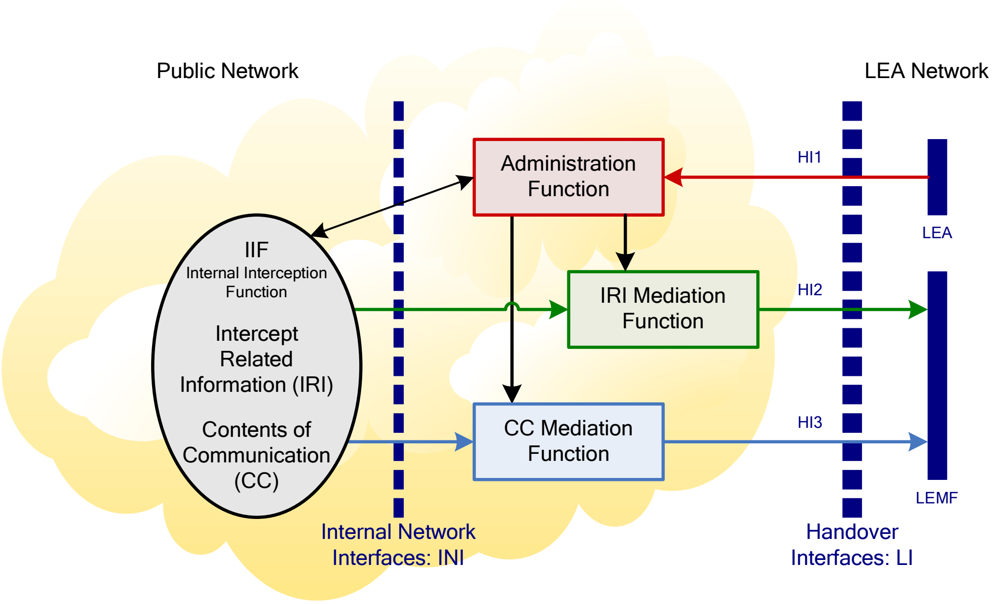
Based on a modular framework, the LIMA Management system can be extended with additional modules for reporting and network management, which aid in the daily tasks of managing interception measures and ensuring that they are functioning correctly.

This whitepaper describes the unique features of the LIMA Management System, First the general features are described. In subsequent sections, specific features of the user interface, the business logic and the real-time provisioning are detailed.

1.1 LI Model

The LIMA Management System implements the ETSI-defined Administration Function’s role. The LIMA Mediator implements the Mediation Functions for IRI (MF2) and CC (MF3) as needed.

The ETSI model defines an Internal Interception Function as part of Network Elements. Many types of Network Element have some support of LI. In the case that LI support inside a Network Element is missing, external monitoring equipment can be installed as an “external” Interception Function. There are several types of LIMA Monitor systems are available, like for DHCP, RADIUS, IP layer 3 and Deep Packet Inspection.

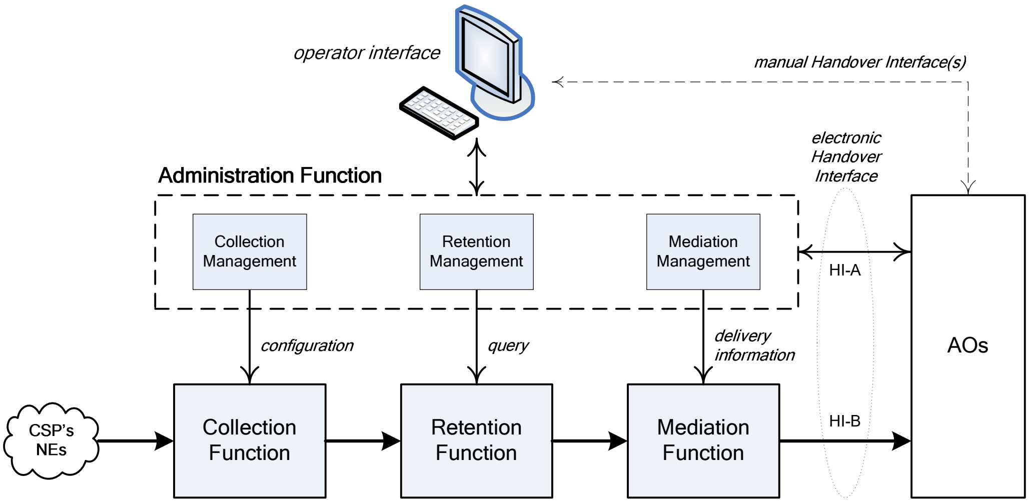


1.2 DR Model

The LIMA support for Data Retention follows the modular LIMA approach, which gives CSPs the option to implement a part or whole of the DR solution in-house. For example, A CSP might want to use its existing database-capacity for the storage of retained data. The following functional modules are distinguished:

- Collection Function
  collects and prepares the information
- Retention Function
  retains the information for the specified period in a retrievable way
- Mediation Function
  receives electronic disclosure requests and hands-over the retrieved information according to local legislation
- Administration Function
  manages the DR process in the organization

The following figure illustrates these four main functionalities.



More information on the LIMA DR solution is available in a separate whitepaper[i].

2 The LIMA Management System

The LIMA Management System is designed with a number of key requirements in mind:

- Separation of concerns

  Organizational: flexible user-roles and separation for multiple organizations (LEAs) that use a single LIMA Management System.

  Technically: the responsibilities like business logic, presentation aspects and communication must be functionally separated. This enables easier extendibility and maintenance.

- Data consistency, integrity & security

  The data-model must be able to accommodate complex and dynamic dependencies in an elegant way. Sensitive information must be stored encrypted.

- Generic model for distributed control

  The provisioning of interceptions must be flexible so that a per-site control plane instance can be used. Multiple components of the same type (switches, LIMA Mediators) must be handled to allow load-balancing.

- Easily extensible

  New business-logic rules (Provisioning Plans, Network Element support) and new modules implementing additional features must be supported. Plug-in support is available to realize this, see sections 2.8, 4.5 and 5.3 also.

- Insight

  Tracking interception measure status in the network, diagnostics, status overviews (passive and active), history of a warrant, and mediation events via IDR logging.

- Helpful exception handling and logging

  Target masking in log, leveled logging.

2.1 Frameworks

The LIMA Management System is based on the Group2000 Service Component Architecture (SCA) framework that provides generic functionality required for telecom-grade services, like logging, alarming, reporting, persistency, security, scheduling, property management, inter process communication mechanisms, connection pooling mechanisms and business process definition in such a way that new services can easily be developed and plugged-in into a product. The dynamic behavior of the business can easily be extended and configured based on the SCA framework. The SCA framework uses OSGI and can run on JBOSS, WEBLOGIC, etc.

The Group2000 Web Framework (GWF) has been developed to provide a generic approach for common GUI tasks like presenting data to the user, to allow the user to enter and submit data, to invoke commands to initiate application functions, and to monitor statuses. The LIMA Management System uses the GWF framework to offer a GUI to manage Lawful Interception; see section 3.2 also.

Copyright Group 2000 Nederland B.V., 2010. All rights reserved.

2.2 Warrant / Interception Management

The concept of an interception has many aspects. First, there is the identification, the requested service, and the specification of the target and the LEMFs. This information is received with the legal warrant, although parts of this information might be delivered before or after the definition of the interception itself e.g., in case an electronic HI1 interface is used.

The Management System will also add its own information to the Interception. At least an Interception Type has to be specified as this translates to choosing the correct Provisioning Plan. Other optional information like contacts or free-format remarks are supported also.

Different Provisioning Plans are available as a plug-in, making it possible to attune the application to the local situation. When adding, viewing or modifying an Interception, the selected Provisioning Plan will determine which data and parameters will have to be entered by the user.

The following functions are supported:

- Manage Interceptions (List, Add, Delete, View, Modify, Copy)

  When creating a new warrant, the LEA, the warrant identifier, the validity period and the Interception Type can be selected. Based on this input, subsequent pages with interception details are presented for specifying the target, the LEMFs, and comments.

- View aggregated Interception status
- View Interception status on provisioned NE’s

  In the interception overviews, two statuses are shown for each interception: the administrative status that indicates the desired state based on the validity period, and the overall operational state. By zooming in on an interception, the underlying interception measures are shown also with their states. The Provisioning Plan that is used for this Interception Type determines which interception measures are used. Also a manually operated administrative “paused” status is available, allowing the user to temporarily remove an active interception from the Network Elements, e.g. if requested by the LEA.

- Stop / start an Interception temporarily
- Cancel an Interception immediately
- Initiate a Delivery test for an Interception (depending on the handover standards used)
- Check Integrity of an Interception

  In case of persisting problems with provisioning Network Elements, an interception can remain in an unprovisioned state when all automatic retries have failed. In this situation, a resubmit command is available in the GUI to retry the provisioning process for this interception on demand.

- Query Network Element for an Interception
- View administrative history for an Interception (audit log)
- View operational history for an Interception (IDR log)
- Assign LEA to an Interception (optional)
- User access may be restricted based on assigned LEA

2.2.1 Provisioning Plans

When an interception has to be provisioned in the network, *interception measures* have to be put in place on various Network Elements. Each kind of network has its own pattern of interception measures. The Provisioning Plan determines how and when the interceptions are put in place in the network by creating dedicated interception measures for all Network Elements involved.

Provisioning Plan code executes inside the distribution layer, which is introduced in section 5.

Provisioning Plans can be reused in situations where identical behavior is needed. For example, an ISP that offers its services in multiple countries via the same infrastructure can use the same behavior for the implementation of LI in these countries.

2.2.2 Interception Types

The LIMA Management System offers the possibility of defining various Interception Types. Examples of Interception Types are VoIP interceptions based on a phone number, DHCP interceptions based on MAC, static IP interceptions, PSTN interceptions, email interceptions, keyword-based interceptions, etc. The same physical LIMA Management System can handle various types of interceptions in parallel.

Each Interception Type is linked to a number of Network Elements. By doing so, the LIMA Management System's internal scheduling and the Provisioning Plan mechanism will automatically provision the correct systems when interceptions need to be activated or deactivated.

An Interception Type is also linked to a *Provisioning Plan*. In this way, the Interception Type provides the set of Network Elements, while the Provisioning Plan defines the behavior for the provisioning of interceptions in the network.

By separating the provisioning behavior from the selection of Network Elements, two or more Interception Types can be defined that use the same behavior. For example, an ISP that offers its services in multiple countries via the same infrastructure can define an Interception Type per country, while still using the same Provisioning Plan.

A LEA can be assigned to an Interception Type. User access may be restricted based on assigned LEA.

2.3 Network Element Management

Network Elements are typical network equipment and other LI components like (other) Management System instances. A more meaningful categorization is to distinguish the function of a Network Element in terms of the LI ETSI model. In this model we distinguish the following functions:

- Administration Function (AF)

  This is the LIMA Management System. In case of multiple hierarchical Management Systems (see section 4.4), lower-level AFs can be present also.

- Mediation Function

  A LIMA Mediator.

- Interception Function (IF)

  A LIMA Monitor or foreign network equipment that supports intercepting IRI or CC. For example, a Cisco CMTS contains an internal IF.

Network Element management is available to configure the connection parameters for individual Network Elements. Plug-ins are available for different Network Element types making it possible to attune the application to the local situation. When adding, viewing or modifying a Network Element, the selected Network Element type will determine which data and parameters will have to be entered by the user.

The following functions are supported:

- Manage Network Elements (List, Add, Delete, View, Modify, Copy)

  Network Elements can be created, modified and deleted to reflect the evolving network. All relevant information of a Network Element needs to be specified only once. When –for example– the access information changes, this change will automatically be applied for all interceptions that relate to the Network Element.

- View Network Element status

  A Network Element has two statuses: the administrative status that determines if the Network Element should participate in the provisioning of interceptions (maintenance mode), and the operational status that indicates connectivity and the correctness of the interception measures on that Network Element.

- Export and import Network Element data
- Test connection to a Network Element
- Invoke Integrity Check on Network Element

  Although an automatic integrity-check is performed when the connection to a Network Element is established, and periodic integrity-checks can be configured, an integrity-check can be executed on demand also. See section 5.4 for a detailed description of the integrity-check feature.

- List Interceptions on a Network Element
- Suspend / resume a Network Element
- View administrative history for a selected Network Element (audit log)
- View operational history for a selected LIMA Network Element (IDR log)

2.4 LEA and LEMF Management

A warrant is issued by a LEA, and specifies the LEMF equipment to which the intercepted information has to be sent. The LIMA Management System allows to specify predefined LEAs and LEMFs in the GUI.

LEAs are applied throughout the management system to identify associated LEMFs, Interceptions and Provisioning Interfaces. LEA management is optional.

The real advantage of predefined LEAs lies in the user access restrictions that can be set-up. A user of the LIMA Management System can be restricted to certain LEAs only. This enables to have dedicated groups of operators for different LEAs. The following functions are supported:

- Manage LEAs (List, Add, Delete, View, Modify)
- View associated Interceptions and LEMFs
- User access may be restricted to selected LEAs

Predefined LEMFs avoid errors due to typos and increase the efficiency by removing the need to specify the handover interface details (IP-addresses, telephone numbers, encryption-keys) of LEMFs in each warrant. Plug-ins are available for different handover protocol types making it possible to attune the application to the local situation. The following functions are supported:

- Manage LEMFs (List, Add, Delete, View, Modify, Copy)
- Export and import LEMF data
- View Administrative history for a selected LEMF (audit log)
- List associated interceptions for a LEMF
- Test connection to a LEMF
- Assign a LEA to a LEMF
- User access may be restricted based on assigned LEA

2.5 AO Management

The Authorized Organization (AO) is the DR-equivalent of the LEA and LEMF of the LI domain. The AO is defined as the origin and destination of disclosure requests. The LIMA Management System offers managing AOs in a similar way as the management of LEAs and LEMFs:

- Manage AOs (List, Add, Delete, View, Modify)
- Export and import AO data
- View Administrative history for a selected AO (audit log)
- View associated disclosure requests
- Test electronic handover interface connection to an AO
- User access may be restricted to selected AOs

2.6 Retention Component Management

The LIMA Collection Function, LIMA Retention Function and LIMA Mediation Function (for DR) support can be managed by the LIMA Management System. This allows for enhanced automation of frequently used tasks:

- Administration of the collection, storage, retrieval and hand-over modules
- View real-time information (connectivity / reachability, attention flags)
- View statistical information (disk usage, job-statistics, data-statistics)

2.7 Disclosure Request Management

The Disclosure Request is comparable to the Interception. The following functions are supported:

- Manage Disclosure Requests (List, Add, Delete, View, Modify)

  When creating a new disclosure request, the AO, the request-identifier, the QoS parameters (priority, deadline) and Disclosure Request Template can be selected. Based on this input, subsequent pages with disclosure request details are presented for specifying filter parameters, AOs, and comments.
- View Disclosure Request status
- Cancel scheduled Disclosure Requests (if not executed yet)
- Initiate a delivery test for a Disclosure Request (AO connectivity)
- View administrative history for a Disclosure Request (audit log)
- View operational history for a Disclosure Request (IDR log)
- User access may be restricted based on assigned AO

A request for retained data can be issued from two controlled entities: the management GUI and the electronic handover interface "A" (HI-A). Complete disclosure requests received via an electronic HI-A interface can be executed directly, or after review by CSP personnel. This a a choice.

When a disclosure request has been executed, the results might need to be sent to an AO. Also manual delivery actions can be used like faxing, burning a CD-ROM, etc. Manual delivery is supported as follows:

- File output is the most elementary method of disclosing information. A (comma-)separated file can be read and viewed by many software packages.

- Reports are useful for relatively small disclosures that may be faxed. To generate reports the LIMA reporting module is available.

2.7.1 Query Template

The layout of the retained data-store and the queries that can be executed against it, are closely related. The data-store layout is defined by configuration conform specific needs. There is no need for any GUI support here.

Query Templates are comparable to the LI Provisioning Plans. The Query Templates define parameterized queries on the data-store. Since these queries depend on the data-store layout, they are defined by configuration.

2.7.2 Disclosure Request Template Management

The Disclosure Request Template is comparable to the LI Interception Type. It governs the relation between allowable queries (depending on AO, and user permissions) and the underlying Query Template that implements the request.

2.7.3 Proof of Disclosure

IDR logs are maintained on Disclosure Requests, giving information on the kind of request and the amount of output. According to the EU Directive, the result-set of a disclosure request must not be stored. Some organizations feel the need to have a formal proof of the hand-over of the disclosed information. This depends on the capabilities of the handover specification.

2.8 Modularity

The LIMA Management System supports additional modules that can be plugged in.

In addition to the standard modules for warrant, disclosure-request, Network Element, LEA, LEMF and AO management, a number of optional modules are available. These can be used to add specific functionality to the system, like an electronic HI1 interface according to national legislation, billing and invoicing features and a reporting and statistics module. See section 4.5 also.

Also specific features can be implemented on request, like interfaces to subscription databases like an HLR, for additional efficiency.

2.9 Investigation

The LIMA Management System offers extensive support to help identify the cause of any problems encountered during provisioning activities. Also a full account of the activities performed is available.

2.9.1 Logging

The administrative (audit log) and operational (IDR log) logging is accessible. The presented lists provide filter options, including a per-interception filter. Where applicable, it is possible to zoom in on record details. Access to the logs is a dedicated security privilege.

2.9.1.1 Audit Logging

Each activity in the GUI of the LIMA Management System is logged. By inspecting this log, authorized personnel can investigate what happened to a warrant, or what actions a specific user has performed.

2.9.1.2 IDR Logging

The Interception Detail Record log is maintained by component of the LIMA architecture. These logs provide detailed information of the provisioning of interceptions and the mediation activities, as well as traffic statistics (Monitor, Mediator, RD-store) and connectivity problems that might occur (Network Elements, LEMFs).

The IDR logs do not contain target-information.

The various IDR logs can be centrally stored on the LIMA Management System if desired. Access to the IDR log – which can be filtered on a specific interception – via the LIMA Management System GUI is a dedicated security privilege.

2.9.2 Fault Tracking

2.9.2.1 Alarming

All LIMA components generate SNMP alarms in case of problems. Besides connection-oriented alarms, also resource-usage and configuration-failure alarms are generated. These alarms are sent to an existing network management center if desired, but the Lima Management System is able to receive and display SNMP traps in the GUI also.

2.9.2.2 Received Status Events

When the status of a Network Element or an interception changes, a notification is sent from the Distribution Logic (see section 5) to the business logic of the LIMA Management System. In this way, the actual operational state is shown in the GUI.

2.9.2.3 Sending Notifications

The business logic of the LIMA Management System supports actions to be taken on certain state-changes , like issuing HI1 notifications over an electronic HI1 interface, or sending an email to a specific mailbox to trigger attention, or comply with a workflow process.

2.9.3 Statistics and Reporting

Via dedicated modules, various statistics can be maintained on the usage and performance of the LIMA Management System.

The Reporting function allows the user to generate pre-defined Management Reports. Reports may, for example, comprise overviews of administered Interceptions, Network Elements with active Interceptions, but may also comprise overviews of Interception deliveries (based on IDR logging). Management Reports may have one or more parameters to be entered at runtime to customize the generated report, like the reporting period, or a specific LEA. The following functions are supported:

- Manage Report templates (List, Add, Delete)
- Generate Management Reports
- Store generated Reports

3 Presentation Logic

The LIMA Management System GUI is designed to manage interceptions and the LI- and DR-infrastructure. The following features are realized:

- Clear interface towards the user

  After logging into the application, the user is provided with a status overview displaying key data about the status of the managed interceptions, Network Elements and retained-data disclosure requests.

  Frequently-used tasks can be started via the menu and buttons in the side-panel.

- Security

  Access rights on users and user groups

  Access rights on LEAs

  Integration with company directory server

- Customizability

  Multilingual

  Out-of-the-box cross-browser support

  Support of extension modules / plug-ins without the need to change the core product

- Real-time presentation of statuses

  Interceptions

  Network Elements

3.1 Feature Outline

The LIMA MS Web GUI consists of a tabular interface providing access to the functions described in more detail in section 2. Multiple pages may be opened simultaneously allowing the user to easily switch between different types of information.

Where useful, wizards are available to enter data (e.g. adding interceptions). Input-fields that offer a selection of choices, will be limited to valid choices only. Default values will be pre-entered by the application where useful. It is possible to enter most required data in input and edit pages by using the keyboard only.

Plug-in support provides the possibility to attune the application capabilities to the Network Element types and Interception Types. Provisioning Plans are realized as plug-ins. Plug-ins may be added to or updated in an existing LIMA Management System.

Many individual tasks, pages and fields can be configured with respect to accessibility (user role based), optional or mandatory, read-write access and input format (e.g. date, time and numeric format, field length, value restrictions). The GUI configuration will be customized at installation time.

Localization of the GUI interface and of online help texts will be available for selected left-to-right languages. See section **Error! Reference source not found.** also. The LIMA Management System internally uses UTC timestamps in all circumstances. In this way, correct local time can be presented for all users, even when the system is deployed in more than one time zone. The user selects his local time-zone at login.

Lists are presented with a search-filter and sorting capability. Both a ‘simple search’ where the filter option is based on (a part of) a single string or value in relevant text-columns, as well as ‘advanced search’ where multiple selection criteria can specified are possible. Furthermore, users may temporarily adjust the sorting order, and move and hide columns. Item lists will support paging, meaning that only a limited set of data is retrieved and displayed on the screen. The list size is configurable at installation time.

Lists of managed items support an ‘auto-update’ feature: when a user adds or removes an item, this will be reflected in lists of that item for other users also. Also statuses of Interceptions and Network Elements and notifications will be updated automatically.

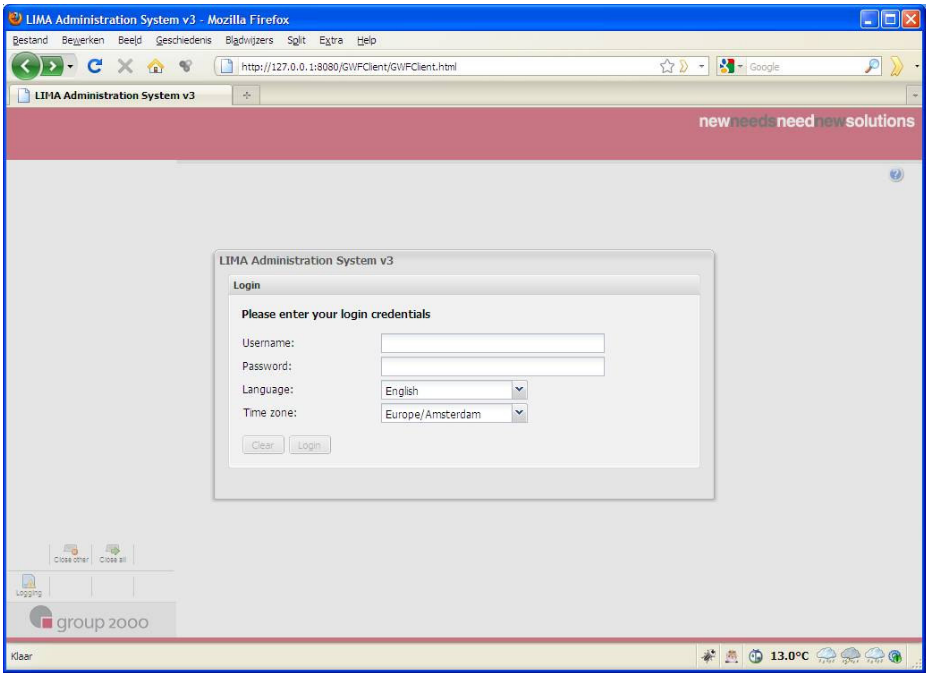
The GUI has a screen lockout function that blanks the application window. The lockout period is configurable and the user will have to re-authenticate in order to continue the session. Previously opened pages and entered data will still be available, even if not saved yet. The user session will void after a configurable period.

The various functional items that can be managed or reported by the LIMA Management System are described in more detail in section 42.

In the following section, a few typical screens are shown[ii].

3.1.1 Screen Impression

The following picture shows the log-in screen. The language and local time zone can be selected.



LIMA Administration System v3 - Mozilla Firefox

http://127.0.0.1:8080/GWFClient/GWFClient.html

LIMA Administration System v3

Login

Please enter your login credentials

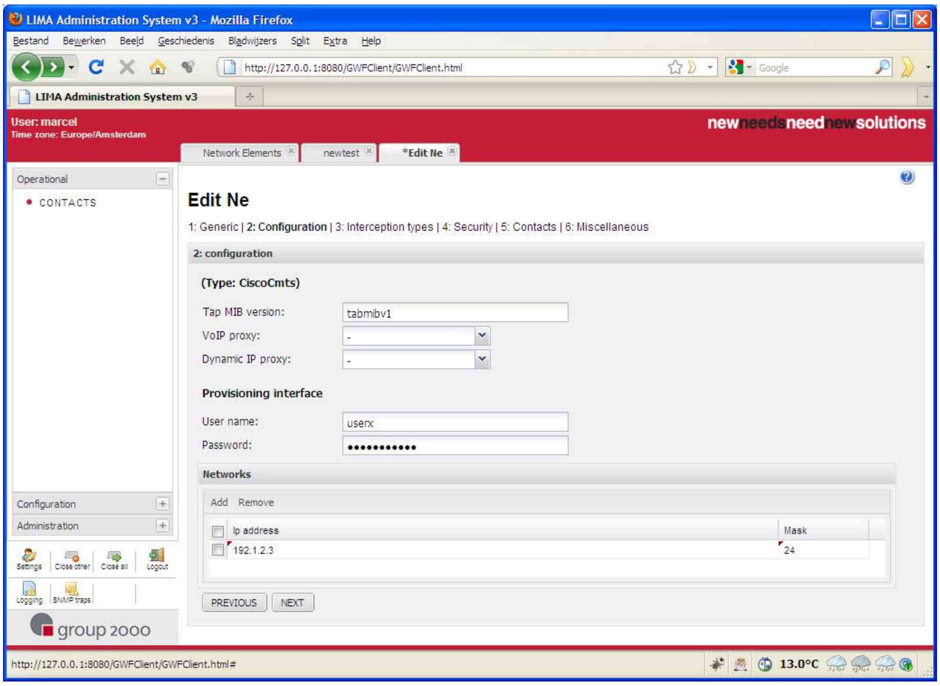
Username:

Password:

Language: English

Time zone: Europe/Amsterdam

The following screen shows the tab-pages visible in the red banner. Tab-pages can be closed at will. The tab shown offers the possibility to modify the parameters of a Network Element: “Edit NE”. Below this title, multiple wizards pages are shown, numbered 1 to 6. The number of wizard pages and their content depend on the information that is entered in the proceeding wizard pages. In this way, specific parameters can be realized per Network Element type if needed.



User: marcel
Time zone: Europe/Amsterdam

Edit Ne

1: Generic | 2: Configuration | 3: Interception types | 4: Security | 5: Contacts | 6: Miscellaneous

2: configuration

(Type: CiscoCmts)

Tap MIB version: tabmibv1
VoIP proxy: -
Dynamic IP proxy: -

Provisioning interface

User name: userx
Password: ●●●●●●●●●●●

Networks

Add Remove

	Ip address	Mask
□	192.1.2.3	24

PREVIOUS NEXT

3.2 Web Technology

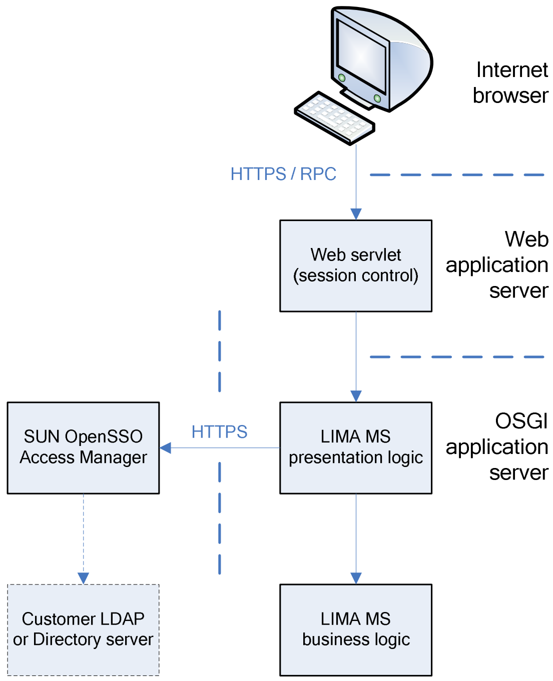
The GUI consists of a client web application which is dynamically configured by the GUI logic running on the server. The client application connects through the Web servlet with the GUI logic residing on the LIMA Management System server. Access control is implemented using SUN OpenSSO server, see section 3.3 also.

The user interface is accessible by every system that supports a standard browser like Internet Explorer, FireFox, Safari or Opera.

The presentation logic dynamically creates the browser pages, checks user authorization, handles the user requests and passes the user requests and submitted data to the business logic. The dynamic creation of browser pages enables limiting access to certain information, as well as the use of plug-ins without the need for changing the existing code base.

The business logic processes the received user requests and submitted data. It passes commands to the distribution and framework logic and persists the data in the LIMA Management System’s database. It retrieves status information and passes this to the presentation logic which notifies the user. Additionally, it provides the presentation logic with rules for the presentation of fields, options and command buttons, depending on user access rights, available options, plug-ins and user entered selections. See section 4 for a description of the business logic.

The following figure illustrates the components:


Internet browser
HTTPS / RPC
Web servlet (session control)
Web application server
HTTPS
SUN OpenSSO Access Manager
LIMA MS presentation logic
OSGI application server
Customer LDAP or Directory server
LIMA MS business logic

3.2.1 Web Toolkit

Any web interface must deal with cross browser compatibility, since each browser renders a webpage slightly different. Dealing with this browser-specific behavior becomes increasingly difficult when the complexity of a web application increases. A solution to this challenge is to use a specific web toolkit.

The LIMA Management System uses the Google Web Toolkit[iii] (GWT™) to render pages and implement the AJAX communication between client and browser. The toolkit enables the development of high-performance web applications without the developer having to be an expert in browser quirks, XMLHttpRequest, and JavaScript. GWT™ is used by many products at Google, and is used by thousands of developers around the world.

3.2.2 Localization

The LIMA MS supports language packs that are independent of the presentation services. Language packs can be installed and updated without impact on the installed code-base.

Localization of the GUI interface and of online help texts is available for selected left-to-right languages. The customer default language will be configurable at installation time; users will be able to select their own preferred language at login. The default system language is English.

Localization of Administrative and Operational log information is planned as a future enhancement; initially all log information will be in English.

3.3 Security

Access control is implemented using SUN OpenSSO. This application is intended for managing users, user groups and policies and provides secure user authentication and role-based access management. The application may store user and user group information locally but alternatively connect to an existing LDAP or Directory server for user authentication and retrieving user roles.

3.3.1 Access control

Users log in using their user name and password. SUN OpenSSO may limit simultaneous logins for the same user, guard subsequent failing login attempts etc. It also provides a user interface to manage the users' password and personal data.

Each connected GUI client session is treated independently, even within the same browser and/or using the same login credentials. User passwords are never provided to the GUI client nor stored on the GUI server.

The connections between client and server and between server and the access manager consist of secure HTTPS connections.

3.3.2 User Rights

All provided functions are associated with pre-defined user roles making it possible to attune the displayed information to the specific roles of individual users. Such functions may consist of entire pages, privileges to modify data, data lists, list columns or individual data fields and buttons.

The following user roles are predefined:

- Operator – managing Interceptions
- Analyst – analyzing Interception provisioning, Network Element provisioning, Integrity checking, etc.
- System administrator – manages LEAs, LEMFs, Network Elements, Provisioning Plans, Provisioning Interfaces, Contacts, Schedulers, Invoice charges
- User repository administrator – manages users, user groups and policies, user access configuration and session management
- Security – generic audit log access, access log

In addition to functional user roles, it will be possible to associate users to LEAs and Network Elements making it possible to limit user access to data which is related to that LEA or Network Element only.

4 Business Logic

The business logic layer of the LIMA Management System is responsible for the realization of the interceptions, and for the timely provisioning of interceptions in the network. This starts with storing the interception details in a database, as well as in executing completeness- and correctness-validations.

Furthermore, the business logic is responsible for the implementation of electronic HI1 interfaces where needed.

4.1 Persistency

The business logic layer acts as a data abstraction layer. All data, like interceptions and Network Elements are stored in a relational database. All sensitive information such as target identities and Network Element access-passwords, are encrypted by the business logic layer before being stored. The standard mechanisms for database backup and replication can be used without disclosing any sensitive information.

The Business Logic Layer uses the persistency services of the SCA framework (see section 2.1). The LIMA Mediator, LIMA Monitor and Provisioning Modules do not store information as their internal information is volatile for security reasons.

4.2 Real-time Interception Scheduling

The LIMA Management System has a scheduler that provisions Network Elements at the time they need to start intercepting and removes the interception when the warrant is not valid anymore (Warrant Start and Warrant End times). As an extra precaution, the warrant start- and end-date are also sent to the LIMA Mediator. The Mediators will check the validity of the warrant independently from the Management System. If an interception is still provisioned on the LIMA Mediator while the warrant is not valid any more, it will drop any intercepted traffic received, without delivering it to the LEMF. Such situations could occur when the network connection between the LIMA Management System and the LIMA Mediator is unavailable at the time the interception needs to be removed.

The provisioning of interceptions is handled by the Distribution Logic Layer, see section 5.

4.3 Disclosure Request Scheduling

The disclosure request execution service takes care of the scheduling and execution of disclosure requests for retained data.

First, the request is converted into the appropriate query-syntax. In case of errors, this will be indicated directly. When multiple disclosure requests are executed, the order of execution is important in order to be able to fulfill QoS requirements. The DR scheduler takes request-priorities and disclosure-deadlines into account.

4.4 Hierarchical Management Systems

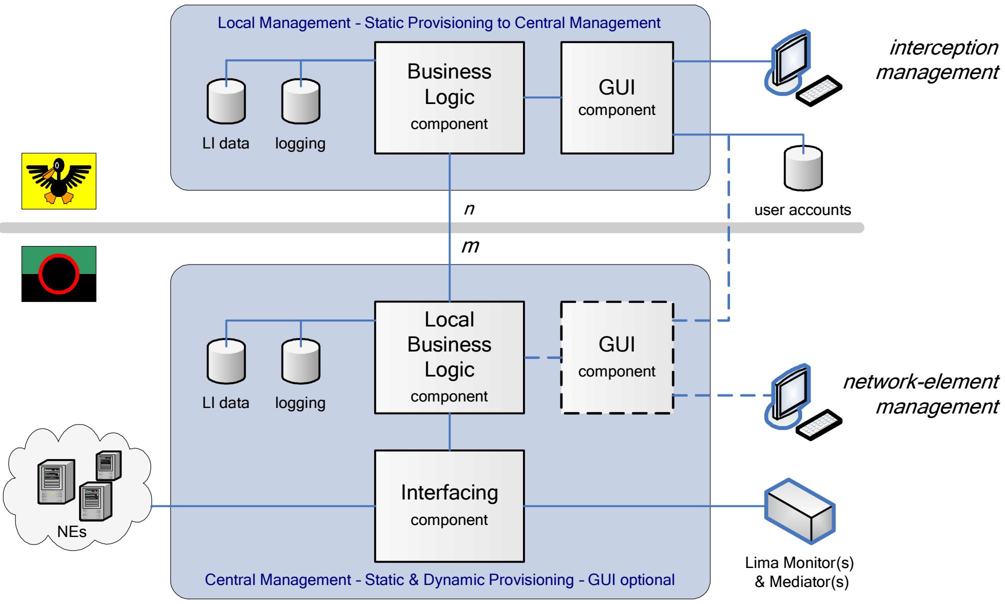
The LIMA Management System supports a hierarchical configuration where one LIMA MS provisions one or more other LIMA MSes in a Master / Slave configuration. A hierarchical configuration can, for example, be deployed whenever a single LI solution spans multiple networks or countries.

In these configurations, the detailed management tasks can be handled on a central LIMA MS that takes care of the interception of the target communication. The management of the interceptions can be implemented per-country or per-site.

Of course, the LIMA Management System provides full isolation between multiple master Management Systems. This is implemented by assigning a LEA to each master Management System. User rights can be assigned to these LEAs, see section 3.3 also.

The hierarchical layering of LIMA Management Systems is realized as a dedicated electronic HI1 interface.

The following figure illustrates a simple hierarchical layering. The top half shows a specific country-implementation that manages interceptions on a higher level. The bottom half shows the slave Management System that provisions the interceptions in the network.


Local Management - Static Provisioning to Central Management
Business Logic component
GUI component
LI data
logging
interception management
user accounts
n
m
Local Business Logic component
GUI component
LI data
logging
network-element management
NEs
Interfacing component
Lima Monitor(s) & Mediator(s)
Central Management - Static & Dynamic Provisioning - GUI optional

4.5 Optional Modules

The Business Logic Layer offers a set of (internal) interfaces that can be used to implement a variety of modules. The Presentation Logic Layer itself uses this interface to provide the LIMA Management System's GUI, and modules that extend the GUI can use the same interface.

4.5.1 Electronic HI-1 Interfaces

Some countries require an electronic HI1 interface. For example, in The Netherlands an electronic HI1 interface is mandatory to automate the warrant key management. The general mechanism, however, can also be used to issue and query warrants and to facilitate the exchange of alarms, informational messages and test call requests. These possibilities can be categorized as administrative and operational activities:

- Send status notifications

  To indicate the availability of Network Elements, for example to indicate planned maintenance.

  Also the activation and deactivation of an interception may be required to be signaled.

- Send alarms

  To indicate problems in the network that affect the LI service.

- Receive warrants or information belonging to warrants

  In some countries, the LEAs can issue warrants directly. In other countries, a part of the warrant details are provided only, like key-material for authentication on the HI2 and HI3 interfaces.

  Complete warrants received via an electronic HI1 interface can be configured to be executed directly, or after review by CSP personnel.

A LEA can be assigned to an electronic HI1 interface instance, allowing the LIMA Management System to restrict access to the interceptions.

Since electronic HI1 interfaces are implemented as plug-ins, multiple interfaces could be used in parallel if required.

4.5.2 Reporting

The reporting module is able to generate reports based on the information stored in the database. This information includes Interceptions, IDR logs, the audit log, Network Elements, and others.

Report templates can be created via available external tools. The templates can be uploaded and managed using the LIMA MS GUI. This approach gives the flexibility to create the reports required, based on these templates. The available reports can be created via the GUI on demand, as well as on a regular basis, in this case the report can be e-mailed if needed. The generated reports can also be opened via the GUI.

The following management report templates are available by default:

- Active Interceptions: reports the number of interceptions set per Mediator, and optionally failure events per Mediator.
- Delivery Attempts: reports on the handed-over information which is extracted from the events in the interceptions logs of the Mediators (packet switched, circuit switched). Information from the Mediator’s Input and Output Adapters will be included.
- Network Element Disruptions: reports on the received critical alarms. A distinction between automatic and manual restarts will be made.

4.5.3 Billing

Some countries allow CSPs to be partly reimbursed. In order to automate the process, a dedicated billing module is available.

Billing of various items can be selected, like the number of warrants, warrant modifications, number of intercepted calls, number of e-mails, amount of PS traffic, etc.

The billing module requires the reporting module.

5 Distribution Logic

There is a single entity that has the overall responsibility of realizing the interceptions in the network: the business logic layer (BLL) of the LIMA Management System. The BLL delegates much of these responsibilities to a lower level: the Provisioning Plans that execute in the Distribution Logic Layer. If needed, a Provisioning Plan can delegate a part of its responsibility to a lower level Provisioning Plan.

This set-up can be compared to a company where the CEO has the overall responsibility without knowing the details of shop floor. When the CEO wants to know these details, he orders his subordinates to report to him.

The hierarchical decomposition of responsibilities is essential in order to minimize well known software pitfalls:

- rigidity - inferior adaptability
- fragility - additions to one area cause a failure in another area
- immobility - no reuse
- viscosity - easier to create workarounds instead of solving a problem.

While the BLL has the overall responsibility, the Distribution Logic Layer (DLL) is the functional entity that realizes the responsibility of provisioning interceptions in the network.

5.1 Execution Environment

The Distribution Logic is an execution environment for the Provisioning Plans. The Provisioning Plans govern the provisioning of interceptions using the facilities of the DL execution environment.

The DL execution environment provides the following services:

- Connectivity to the BLL or a higher-level DL

  The DL receives configuration information, as well as commands for the management of the Network Elements and Interceptions.

- Connectivity to the Network Elements

  The LIMA components can be connected directly, while other Network Elements are connected through protocol converters called Provisioning Modules, see section 5.2.

- Hosting Provisioning Plans

  The Provisioning Plans determine how interceptions are provisioned in the network. Multiple Provisioning Plans can execute in a single DL. Network Elements can be used by all Provisioning Plans. See section 5.3.

- Interception replication (N-times-M provisioning)

  When a target is intercepted by more than one LEA, the interception measures for obtaining the IRI and CC from the Network Elements can be shared. In this way, valuable resources of the Network Elements are saved. The DL supports the Provisioning Plans when this style of provisioning can be used for a particular network.

- sureTap® integrity check

  The sureTap® feature checks the status of interception measures on a Network Element. The Provisioning Plans will correct detected deviations. See section 5.4.

Copyright Group 2000 Nederland B.V., 2010. All rights reserved.

5.2 Provisioning Modules

The LIMA Management System communicates with the Network Elements via an SSL-secured RMI connection, using commands for functions like adding and deleting interceptions and querying Network Elements for their list of interceptions. Alternatively, for backwards compatibility, the Open Mediator Management Interface (OMMI) protocol (XML over SSL) can be used also.

LIMA systems like the LIMA Mediator and LIMA Monitor natively support the secured RMI interface and can be controlled by the LIMA Management System directly. Third party Network Elements like SBC devices and VoIP soft switches, etc., have their own proprietary provisioning interface. Examples of protocols used there are SNMPv3, telnet, WSDL, and CORBA.

In order to control these third party Network Elements from the LIMA Management System, Provisioning Modules are used. These Provisioning Modules translate the native commands into the protocol-specific interaction required by a particular Network Element. In this way, the Provisioning Modules ensure that all Network Elements expose a uniform behavior towards the LIMA Management System.

Provisioning Modules are stand-alone processes that can be installed on any server that hosts LIMA components.

5.3 Provisioning Plan

5.3.1 Structure of Interception Measures

The Provisioning Plan decides what measures are required to implement the Interception in the network. This includes decisions about:

- Correlation

  An important aspect of provisioning is the correctness of identifiers and correlation information. Each interception includes information that allows other Network Elements to correlate the intercepted information to a warrant. Generation of intermediate identities for the IRI and CC information on the internal network interfaces is the responsibility of the Provisioning Plan.

- Interception replication (N-times-M provisioning)

  Some NEs allow interception of a target only once. Since multiple LEAs can require intercepting the same target, the LIMA architecture provides automatic provisioning rules that allow a single target to be intercepted multiple times on different criteria (like MSISDN, IMSI and IMEI).

- NE Multiplicity

  Are all NEs provisioned, or only a single NE? How is that single NE selected? For example, in a mobile network, all MSCs or GSNs are provisioned since a target may be serviced by any MSC or GSN. For fixed networks, a subscriber is typically serviced by a dedicated NE. This dedicated NE can be known, but in certain networks the NE servicing the subscriber is found by trying to provision all NEs, and only one of these provisioning actions NE will succeed.

- Multiple Target Identities

  For some Interception Types, multiple target identities exist at the same time. E.g., for voice interception, a SIP URI and an E.164 number might be specified. In this case, the use of several distinct access technologies causes the multiple identities. Another example might be the assignment of multiple IP(v6)-addresses.

Copyright Group 2000 Nederland B.V., 2010. All rights reserved.

- Timing

  Normally, the Mediator is provisioned first. However, in situations where a NE chooses its own correlation identifier, the Mediator must be provisioned afterwards since the correlation identifier that has to be used is not know beforehand.

5.3.2 Provisioning behavior

A very important categorization is that of static and dynamic target identities. For example, a telephone number can be regarded as a static target-identity (during the lifetime of an interception), while IP-addresses are often leased for a few hours, and have a dynamic nature therefore. These dynamic target identities require instant changes in the realized interception measures.

The interception measures for the LIMA Mediator and – for example – a DHCP monitor can be set when the warrant's start-time has been reached. The interception measures that intercept the target's traffic can only be rolled out when an IP-address assignment is observed. This style of provisioning interception measures is called *dynamic provisioning*.

The Provisioning Plan manages both the structure of the interception measures, as well as the dynamic behavior that is required to implement the interception correctly.

5.4 Integrity Check – sureTap®

When an interception is initially provisioned in the network, it is important to ensure the integrity of the provisioned information. Interceptions can be removed, added or altered on Network Elements for a number of reasons, including software upgrades, system restarts, etc. The intentional or unintentional interference of unauthorized personnel that has access to uncontrolled parts of the lawful interception solution must be considered as a risk in this case.

An integral part of the LIMA Management System is the *integrity check* mechanism, called sureTap®.

sureTap® works in three ways to maintain the integrity of the interception measures on the Network Elements:

- Whenever the connection to a Network Element is restored

  When the Distribution Logic layer (re-)connects to a Network Element, either directly, or via a Provisioning Module, the status of the interception measures on that Network Element are unknown. The Distribution Logic will automatically execute an integrity check on the Network Element first.

- On configurable intervals

  Since interception measures can be removed from Network Elements at any time, regular scheduled integrity checks can be defined.

- On demand

  Whenever there is any doubt, an integrity check on a particular Network Element can be initiated via the GUI.

  - *Check and fix interceptions on all Network Elements*
  - *Only check interceptions on all Network Elements*
  - *Check and fix interceptions on a single, specific Network Element*
  - *Only check interceptions on a single, specific Network Element*

The sureTap® integrity check acts on Network Elements, regardless of the Provisioning Plans that make use of the Network Element. The procedure is as follows.

- In case the NE supports retrieving all interception measures ('list-all' command), the returned list of interception measures is compared to the internal administration. Missing interception measures will be added, and interception measures with incorrect information will be updated by the Provisioning Plan that is associated with this interception measure. Any stray interception measures will be removed by the Distribution Logic itself since they do not belong to any Provisioning Plan.
- Some Network Elements do not support a 'list-all' command, The interception measures that should be present on the NE are queried one at a time. Missing interception measures will be added, and interception measures with incorrect information will be updated by the Provisioning Plan that is associated with this interception measure. Without a 'list-all' command, stray interception measures cannot be detected.

The outcome of an integrity check is logged in the IDR log of course. Any corrective actions are logged in the IDR log also.

The sureTap® integrity check mechanism will make sure that the interception measures of the legal warrant are carried out in the best possible way, avoiding interruption of the interception as much as possible.

6 Conclusion

The LIMA Management System provides:

- management of interceptions without detailed knowledge of the Network Elements involved,
- management of disclosure requests,
- configuration and management of the LI/DR infrastructure,
- a single extensible web-based GUI for LI and DR,
- access security based on users, user-groups and LEAs,
- audit logging and operational logging,
- the sureTap® interception integrity check,
- total flexibility in provisioning the Network Elements by using Provisioning Plans.

The LIMA Management System is able to fulfill all LI- and DR-related management tasks.

Copyright Group 2000 Nederland B.V., 2010. All rights reserved.

[i] Group2000 whitepaper “Data Retention – a Modular Approach”, document code 160-WPR-0029.

[ii] The final layout might differ from the screens shown in this document.

[iii] For more information on the Google Web Toolkit™, visit http://code.google.com/webtoolkit/.

Copyright Group 2000 Nederland B.V., 2010. All rights reserved.