



# LIMA Lawful Intercept

Product Description  
proven. complete. modular.

Reference 160-WPR | Version 11.5.1

Confidential | Group 2000 Proprietary | Issue date 28-08-2023

## Document Revisions

Date	Version	Description
25-09-2019	7v0	Updated version for LIMA LI 7.0
10-08-2020	8v0	Updated version for LIMA LI 8.0
17-08-2020	8v0.1	Minor updates
21-08-2020	8v0.2	Minor updates
01-09-2020	8v0.3	Added S8 Home Routing support
01-10-2020	8v0.4	Minor updates
01-02-2021	8v0.5	Minor updates and AD/LDAP support
01-07-2021	10v0	Updated for LIMA LI 10.0 release
01-05-2022	10v1	Minor updates
15-08-2022	11v0	Updated for LIMA LI 11.0 release
05-01-2023	11v0.1	Updated with LIMA MS performance figures
10-05-2023	11v5	Updated for LIMA LI 11.5 release
28-08-2023	11v5.1	Updated HPF Mediator performance for Gen10plus h/w

## References

### External Documents

Ref.	Document Description	Document Reference
[E1]	LIMA Lawful Intercept 5G - Product Description	LIMA Lawful Intercept 5G - Product Description - 8v0.2

## Table of contents

Table of contents .....	3
1 Introduction .....	7
1.1 LIMA Lawful Intercept .....	7
1.2 LIMA MS Key requirements .....	8
2 The LIMA Management System .....	10
2.1 General features LIMA Management System.....	10
2.1.1 GUI.....	10
2.1.1.1 Wizards .....	10
2.1.1.2 Search and sorting.....	10
2.1.1.3 Lockout function .....	11
2.1.2 User Management .....	11
2.1.2.1 Accounts .....	11
2.1.2.2 Directory Service Support .....	11
2.1.2.3 Two-Factor authentication (2FA) .....	12
2.1.2.4 Roles .....	12
2.1.2.5 Privileges.....	12
2.1.3 Internationalization .....	13
2.1.3.1 Language .....	13
2.1.3.2 Time .....	13
2.1.3.3 Configuration.....	13
2.2 LIMA Warrant Management.....	14
2.2.1 Warrant Management Introduction .....	14
2.2.1.1 Import a Warrant (activation or modification request).....	14
2.2.1.2 Manually create or modify a warrant.....	15
2.2.2 Import warrant functionality (e-Warrants) .....	15
2.2.3 Manual creation and modification of warrants .....	16
2.2.4 General warrant management functionality .....	17
2.2.5 Warrant Management Configuration.....	17
2.3 LIMA Interception Management.....	18
2.3.1 Supported Interception Management Functions .....	19
2.3.1.1 Basic functions .....	19
2.3.1.2 Special functions .....	20
2.3.1.3 Interception tracking option.....	21
2.4 Electronic HI-1 interface.....	21

2.5	Network Element Management.....	22
2.5.1	Basic Functions.....	22
2.5.2	Special functions .....	23
2.6	Configuration and maintenance usage .....	23
2.6.1	Interception types.....	23
2.6.1.1	Basic Functions.....	24
2.6.2	LEA Management .....	25
2.6.3	LEMF Management .....	25
2.6.4	Contact Management (optional).....	26
2.6.5	System Administration .....	26
2.7	Billing and Invoicing Module .....	27
2.8	Reporting.....	27
2.8.1	Report scheduling and dispatching.....	28
2.9	Archiving .....	29
2.10	LIMA Management System non-functional aspects .....	30
2.10.1	Platform.....	30
2.10.1.1	Hardware platform.....	30
2.10.1.2	Operating System .....	30
2.10.1.3	Virtual deployment .....	30
2.10.2	Logging and Alarming.....	30
2.10.2.1	Interception Detail Record (IDR) Logging.....	31
2.10.2.2	NE-event logging.....	31
2.10.2.2.1	Alarms .....	31
2.10.2.2.2	Status Events .....	31
2.10.2.2.3	E-mail Notifications .....	31
2.10.3	Security .....	32
2.10.3.1	Access Control.....	32
2.10.3.2	Cryptographic policies.....	32
2.10.3.3	Data at Rest .....	32
2.10.3.4	Data in Transit.....	32
2.10.3.5	Hardening.....	32
2.10.3.6	Auditing .....	32
2.10.4	Performance.....	33
2.10.5	High Availability .....	33
2.10.6	Backup .....	33
3	LIMA Mediator.....	34

3.1	Introduction .....	34
3.2	LIMA Mediator architecture .....	34
3.2.1	Input Adapters .....	35
3.2.2	Output Adapters .....	36
3.2.3	Buffering .....	36
3.3	LIMA Mediator non-functional aspects .....	36
3.3.1	Platform .....	36
3.3.1.1	Hardware platform .....	36
3.3.1.2	Operating System .....	37
3.3.1.3	Virtual deployment .....	37
3.3.2	Management .....	37
3.3.2.1	Alarming .....	37
3.3.2.2	Logging and Statistics .....	37
3.3.3	Security .....	38
3.3.3.1	Cryptographic policies .....	38
3.3.3.2	Data at Rest .....	38
3.3.3.3	Data in Transit .....	38
3.3.3.4	Hardening .....	38
3.3.4	Performance .....	39
4	LIMA LMISF .....	40
4.1	LIMA LMISF solution architecture .....	40
4.2	LIMA LMISF non-functional aspects .....	41
4.2.1	Platform .....	41
4.2.1.1	Hardware platform .....	41
4.2.1.2	Operating System .....	41
4.2.1.3	Virtual deployment .....	42
4.2.2	Security .....	42
4.2.2.1	Cryptographic policies .....	42
4.2.2.2	Data at Rest .....	42
4.2.2.3	Data in Transit .....	42
4.2.2.4	Hardening .....	42
5	LIMA Monitors .....	43
5.1	Introduction .....	43
5.2	LIMA Monitors (Filters) .....	43
5.2.1	LIMA VoIP monitors .....	43
5.2.1.1	LIMA SIP monitor .....	43

5.2.1.2	LIMA RTP Monitor.....	44
5.2.2	LIMA Mail monitors .....	44
5.2.2.1	LIMA SMTP monitor.....	44
5.2.2.2	LIMA POP monitor .....	45
5.2.2.3	LIMA IMAP monitor .....	45
5.2.3	Passive IP monitors .....	45
5.2.3.1	LIMA Radius monitor .....	45
5.2.3.2	LIMA DHCP monitor .....	46
Glossary	47	
Disclaimer of Warranties and Limitation of Liabilities .....		48
Non-disclosure notice .....		48

# 1 Introduction

LIMA Lawful Intercept is Group 2000's proven industry-leading solution for Lawful Interception. Our LI solution can integrate in any fixed, cable and mobile network, with any vendor, and with all technologies. In many markets lawful interception is an obligatory requirement for telecom providers, which in most cases does not generate revenue. For that reason, we believe that the operational costs for having an LI solution should be minimized.

With our warrant management and workflow management features, we minimize the operational costs of the solution. These features simplify and automate the warrant management process. Another benefit of these features is that they reduce the risks of human errors.

To ensure that the complete end-to-end Lawful Interception chain from interception to Monitor Center is working as intended, our solution can be complemented with an automated end-to-end LI verification tool: LIMA Élite.

As full and active member of ETSI we can timely anticipate on changes to the handover standards and thus minimizing the impact to your solution when these changes happen. For these reasons, many operators world-wide chose for our LIMA LI solution. An LI solution, which is reliable, trustworthy, cost-effective and which relieves our customers from many LI related influences out of their control.

## 1.1 LIMA Lawful Intercept

LIMA Lawful Intercept is Group 2000's modular and scalable solution for Lawful Interception. The LIMA Lawful Intercept architecture embodies a flexible architecture for solutions that manage, intercept and mediate traffic for lawful interception. LIMA focuses on lawfully intercepting digital communications to support investigations.

Due to its modular architecture LIMA solutions can be integrated into any network environment. LIMA solutions are available for interception of all network types and services: fixed and mobile telephony, IP data, unified messaging, RCS, LTE, VoLTE and 5G for that matter. On the LEA delivery site, our LIMA Mediator support all commonly used protocols like:

- CALEA T1.678, J-STD-025B, ETSI TS 102 232-x, ETSI TS 133 108, ETSI TS 201 671, including various country specific implementations like ETSI-IP.nl, TR-TKÜV, etc.

Please note that a comprehensive product description concerning 5G, our LIMA Lawful Interception solution supporting interception of targets in both the EPC-anchored mode (NSA) and interception in the core-anchored mode (SA) can be found as an external document with reference: [E1]. LIMA Lawful Intercept 5G - Product Description - 8v0

The LIMA Lawful Interception product line consists of the following optional and licensed components:

- **LIMA Management System**
  - Automated warrant handling and workflow management
  - Automated interception handling and interception provisioning
  - Network Element (NE) management
  - Configuration of infrastructure for Lawful Interception
  - Billing and invoicing module
- **LIMA Mediator**

- Conversion of intercepted traffic into the required handover protocols
- **LIMA LMISF**
  - Component for VoLTE S8 Home Routing support
- **LIMA Monitors**
  - Monitoring solutions for passive interception of traffic
- **LIMA Élite**
  - End-to-end LI verification

The LIMA Management System (LIMA MS) is the central component in a LIMA Lawful Interception solution. It provides a secure web-based interface via which authorized users can manage and oversee the warrants and interceptions. LIMA MS also provisions all the network systems that are involved in intercepting traffic

Based on a modular framework, the LIMA MS can be extended with additional modules. These additional modules are described in other product descriptions. Within this document, the LIMA Lawful Interception solution is described.

## 1.2 LIMA MS Key requirements

The LIMA MS is designed with several key requirements in mind:

- **Separation of concerns**
  - Organizational: flexible user-roles and separation for multiple organizations (LEAs) that use a single LIMA MS.
  - 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 etc.) must be handled to allow load-balancing.
- **Scalable**

LIMA MS supports the creation of interceptions for multiple target types, multiple instances of the same target type, multiple services, multiple operators and multiple networks, in one go.
- **User friendly**

LIMA MS simplifies the warrant management process, interception creation and interception handling.



- **Easily extensible**  
New business-logic rules (Provisioning Plans, NE support) and new modules implementing additional features must be supported.
  
- **Insight**  
Insight is given via overviews and reports.

## 2 The LIMA Management System

### 2.1 General features LIMA Management System

#### 2.1.1 GUI

The LIMA MS is a modular web application that runs on a web server. The GUI of the LIMA MS is provided by the Group 2000 Web Framework which runs in the Service Component Architecture. 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 MS server. The user interface of the LIMA Management System is accessible by every system that supports a standard browser like Internet Explorer, Firefox and Google Chrome. We always strive to support the latest versions of these browsers.

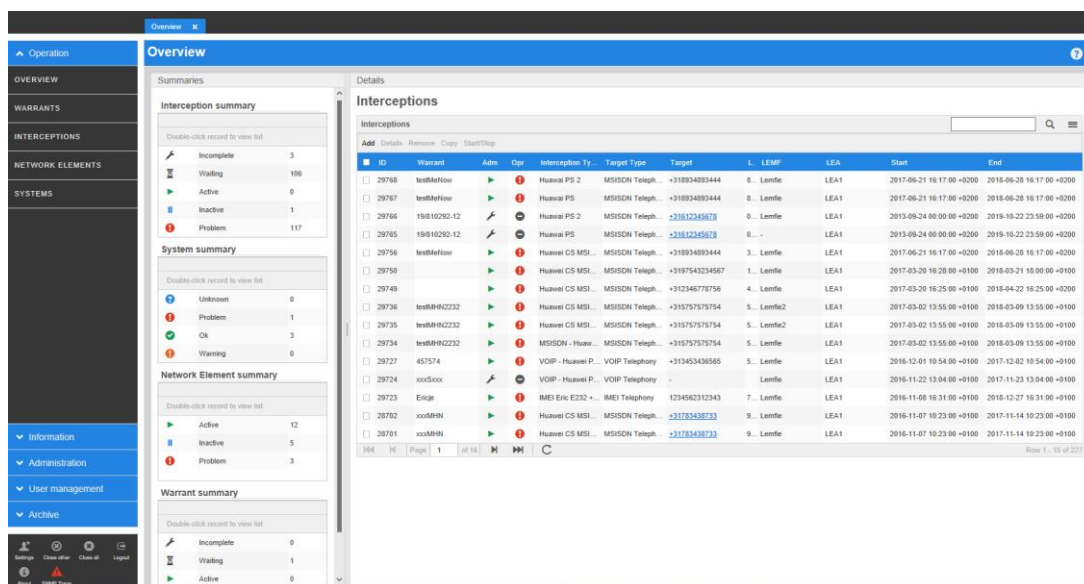


Figure 1: Main window LIMA Management System

#### 2.1.1.1 Wizards

For data types like interceptions or NEs, a lot of data has to be entered. In these cases a wizard is used. This means that the data to be entered is split up in multiple input screens to make entering of the data easier for the user.

#### 2.1.1.2 Search and sorting

Overviews 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 be specified are supported.

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 of LIMA MS. 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 warrants, interceptions and NEs will be updated automatically.

### **2.1.1.3 Lockout function**

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.

## **2.1.2 User Management**

The User Management module of the LIMA MS is used to manage the access to the system. It supports role-based access by allowing the administrator to define roles and assign accounts to it.

### **2.1.2.1 Accounts**

For each user that needs access to the LIMA MS an account is created. A user account has several security settings that can be configured:

- Password expiry date
- Password policy
- Account expiry date
- Account lock

Users log in using their username and password. LIMA User Management may limit simultaneous logins for the same user, guard subsequent failing login attempts etc. Each connected GUI client session is treated independently, even within the same browser and/or using the same login credentials. The connections between client and server and between server and the access manager consist of secure HTTPS connections.

### **2.1.2.2 Directory Service Support**

Next to the internal authentication mechanism, authentication against an external Corporate Directory server is supported. Currently the authentication against LDAP and Active Directory (AD) server is supported.

The system will use authentication profiles (or domains) to determine if internal or external authentication shall be applied. A profile is assigned to each of the accounts to determine which authentication shall be applied. Typically, only the admin user will (initially) use internal authentication, other user accounts will use external authentication.

To login, the user selects the correct authentication profile and provides credentials in the GUI login page. Subsequently, the user is authenticated externally by the LDAP/AD server or internally against the stored credentials.

Authorization remains an internal process; this implies that the users still have to be created in the LIMA Management System and have roles and privileges assigned.

### **2.1.2.3 Two-Factor authentication (2FA)**

Within the LIMA Management System, two-Factor Authentication (2FA) can be used to complement the internal or external authentication methods. The default 2FA method available is based on the Time-Based One-Time Password (TOTP) algorithm which allows commonly used 2FA tools like Google Authenticator to be used as part of the authentication process.

### **2.1.2.4 Roles**

The roles define the functionality that a user has access to. They are used to define which optional modules can be accessed. Next to this, roles also define the type of access: read-only or full-control.

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, NE provisioning, Integrity checking, etc.
- System administrator – manages LEAs, LEMFs, NEs, Provisioning Plans, Provisioning Interfaces, Contacts, Schedulers
- User repository administrator – manages users, user groups, user roles and privileges, user access configuration and session management
- Security – generic audit log access, access log

### **2.1.2.5 Privileges**

To control the access to a data set, privileges can be used. Although a user has access to a certain functionality based on his or her role, the access to the data within that function is defined by the privileges a user has. For example, privileges can be defined for government agencies (LEA's), NE groups, service providers and configuration settings. This makes it possible to limit user access to data which is related to that LEA or NE only.

## **2.1.3 Internationalization**

### **2.1.3.1 Language**

The LIMA MS supports language packs that are independent of the presentation services. The customer default language will be configurable at installation time; users will be able to select their own preferred language. After selection, the GUI interface is available for the selected language.

The following languages are supported: English, Spanish, German and Arabic. The default system language is English. Online help and documentation are provided in English only.

### **2.1.3.2 Time**

The LIMA MS 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.

### **2.1.3.3 Configuration**

The LIMA MS makes use of a Service Component Architecture (SCA) framework which manages modules that implement various services. One of the modules in the SCA framework is the property manager. This service maintains properties / configuration values for other modules running in the SCA Framework. By changing the settings in the property manager settings of many of the LIMA MS modules can be managed.

## 2.2 LIMA Warrant Management

### 2.2.1 Warrant Management Introduction

LIMA Warrant Management provides the user the possibility to add multiple interceptions for one warrant automatically and simultaneously into the Management System, instead of adding multiple interceptions for one warrant separately. The system supports the creation of interceptions for multiple target types, multiple instances of the same target type, multiple services, multiple operators and multiple **networks**. For example, if a warrant contains interception information for one target to be set in a heterogeneous network environment, LIMA Warrant Management takes care of rolling out the interceptions in every network. It is not needed to add an interception for each network type separately.

The current version of Warrant Management supports 2 major functions;

- 1 Import of Warrants (ETSI-ip.nl XML files)
- 2 Manual creation of Warrants

#### 2.2.1.1 Import a Warrant (activation or modification request)

In this scenario the warrant information is issued by a LEA and delivered to the Operator as an XML file. The XML file itself contains the signed warrant, in PDF format. LIMA Warrant Management supports the functionality to import the warrant requests or import of warrant modification requests embodied in the XML file (XSD version 3.0). The XML is either of type warrant activation or warrant modification request.

Note: It is required that the format of the received XML file complies with the standard ETSI-IP.nl).

To import a warrant the following basic steps have to be performed;

- 1 The warrant overview must be opened.
- 2 The warrant XML file, as issued by a LEA, needs to be imported in the system.
- 3 The Operator needs to verify the imported warrant details and interception details against the legal documents (pdf and XML). If necessary the Operator can change some warrant and or interception details.
- 4 The Operator has to 'create' the warrant and provision the warrant related interceptions in the system.

Note; an electronic handover interface (HI-1) to handle warrant request completely automated can be offered as an option. Here, warrant requests issued by a LEA can be executed directly, or after review by CSP personnel.

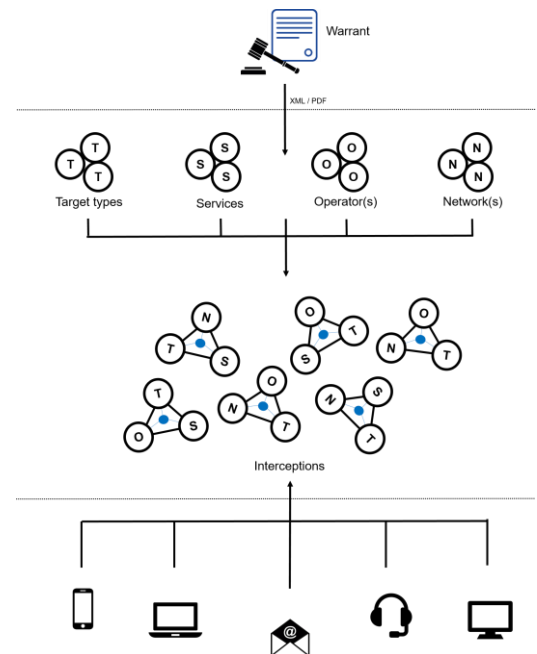


Figure 2: Warrant Management overview

## 2.2.1.2 Manually create or modify a warrant

The manual warrant creation process supports the manual creation and modification of warrants. Interceptions related and derived from the warrant are automatically created and can be modified if necessary. The basic principle of LIMA Warrant Management is that it must be as easy and as intuitive as possible to create a warrant and to create the related interceptions.

To create a new warrant manually the following steps must be followed;

- 1 Open the warrant overview.
- 2 Enter the warrant and target details.
- 3 Check the interception details.
- 4 Create the warrant and provision the warrant related interceptions.

## 2.2.2 Import warrant functionality (e-Warrants)

### ▪ Import XML (warrant activation or modification request)

An operator can import an electronic warrant (XML). The XML file is selected using a document selection box. LIMA Warrant Management will parse the selected XML file and will process all the information contained in the XML file into a new warrant in LIMA MS. The following information is automatically created in the new warrant;

- 1 Warrant details (warrant id, warrant name, warrant start and end date/time, LEA).
- 2 Warrant documentation (request XML, legal warrant document (pdf)).
- 3 Target details (target type, target identifiers, services and networks).
- 4 Interceptions details (all interceptions that can be set, based on the information in the warrant XML file. Including LEMF, Info type (IRI or IRI\_CC and delivery information).

### ▪ View warrant and related warrant documents

An operator can verify the warrant details described above with the legal documentation. Therefore the warrant XML and or the legal warrant document (pdf) can be opened in a new screen.

### ▪ Modify warrant

If necessary an operator can intervene after import and modify/add mandatory input data.

### ▪ Validate warrant and interceptions. Several control functions are available;

- Check if warrant has already been imported, in order to prevent doubling.
- Validation of the input data. The required properties of the target identifiers can be configured on target type level and on interception type level (switch specific).
- Check with LEA filters. This feature allows an operator to control the target identities that may or may not be intercepted by the LIMA MS.
- The system uses a consistent method for error warning and notification. So that the user is aware of the situation and knows what the follow up action should be.

### ▪ Create warrant and provision interceptions

At warrant creation the selected interceptions will be provisioned into the network. The actual interception of the target is scheduled to start on the indicated start date/time.

## 2.2.3 Manual creation and modification of warrants

- **Create warrant details**  
 After creation of a warrant a number of required Warrant details can be configured in advance like;
  - Default warrant period defined.
  - Default Info type (IRI or IRI\_CC delivery).
  - Default settings for LIID generation (ETSI compliance or dynamic LIID generation).
  
- **Document management functionality**  
 LIMA Warrant Management contains a document upload function to attach one or more document to the Warrant (pdf, XML or txt). The documents are shown as hyperlinks and can be opened in a separate screen.
  
- **Creation of target details**  
 Alike the warrant details, a number of required target details can be configured in advance (if necessary and available).
  - Available target types per network (Telephone number, IMSI, IMEI, etc.).
  - Available primary service types per network (telephony, IP, etc.).
  - Available CSP's (operators, only if more than 1 operator is configured).
  - Available network(s) (only if more than 1 network is configured).

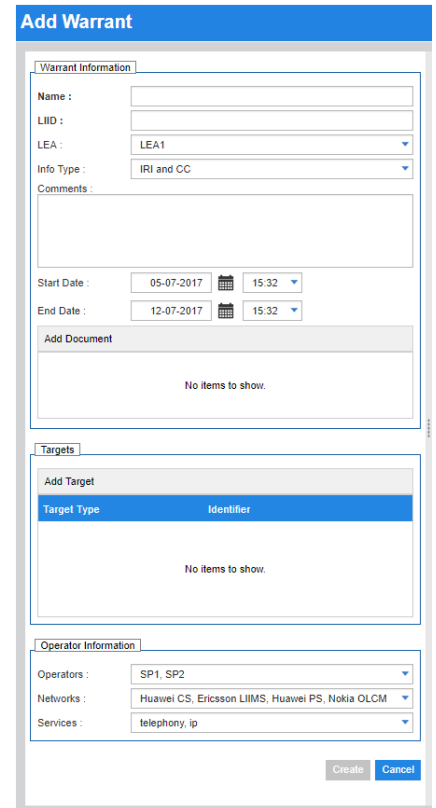


Figure 3: Create Warrant manually

The system supports the creation of interceptions for multiple target types, multiple instances of the same target type, multiple services, multiple CSP's and multiple Networks.

- **Dynamic creation of interceptions**  
 After the warrant and target details have been entered or selected the LIMA MS dynamically creates the related interceptions automatically. The interceptions are shown using a tree and can be de-selected (and re-selected) before actual provisioning. If necessary relevant details can be modified on interception level, the details can be modified in the interception tree itself. The user doesn't need to open more than one window for the complete warrant handling process.
  
- **Validate warrant and interceptions.**  
 Several control functions are available. The control functions have been described in chapter 2.2.2.
  
- **Create warrant and provision interceptions**  
 At warrant creation the selected interceptions will be provisioned into the network. The actual interception of the target is scheduled to start on the indicated start date/time.
  
- **View warrant details**  
 A warrant can be opened in view mode. All warrant details, document details, target type details and interception details will be visible. Compared to the warrant creation and modification screen,



in the warrant view screen the screen the administrative and operational status of the interceptions is visible (also refer to 2.3.1.1).

## 2.2.4 General warrant management functionality

- **Manage warrants (Overview, View, Modify, Copy, Delete)**
  - Overview warrants; the practical overviews deliver insights of warrants and related interceptions. In the warrant overview screen the administrative and operational status of the warrant is visible (also refer to 2.3.1.1).
  - View warrant; a warrant can be opened in view mode. All warrant details, document details, target type details and interception details will be visible. Compared to the warrant creation and modification screen, in the warrant view screen the screen the administrative and operational status of the interceptions is visible (also refer to 2.3.1.1).
  - Modify warrant; after manually Warrant creation an operator can modify the Warrant details, the target details, add targets, remove targets, add and remove documents.
  - Copy; copy the info of a selected warrant to create a new warrant.
  - Delete; permanently remove a warrant.
- **Start/stop warrant**

Warrants can be stopped and started manually. This functionality is only available when the administrative state of the warrant is active. A warrant can only be stopped if the related interceptions are stopped and un-provisioned in the network.
- **View Event log**

The warrant event log shows the administrative history for this warrant. For every event the related date/time, type of event (ok/error), description of the event and user name of the performer of the action is given.
- **View IDR log**

The warrant IDR log shows the operational history (IDR log) for this warrant. For every event the local date/time is given, the related NE and the description of the event is given.
- **View Versioning**

The versioning of warrant gives insight in the change history of a warrant. For every version the date/time, the event, the username and change information is given.

## 2.2.5 Warrant Management Configuration

The following variables or customer specific information can be configured;

- **Warrant name**

The warrant name is a parameter that can be defined by a user. It will usually contain a representative name for the warrant that is easy to understand and easy to remember. A regular expression can be set that the system will use internally to verify the warrant name.
- **Warrant ID**

The warrant ID is a parameter that can be defined by a user. In some countries the LIID can be entered here by the user. In that case the format to which the LIID shall comply in that particular country can be configured. In some countries the warrant ID may be free format.

- **Warrant validity period**  
The default validity period is used when a user creates a new warrant manually. The warrant start date will be set to the current date and time.
- **Target types**  
A target consists of one or more target type (key) and identifier (value) combinations. The list of possible target types, supported by the operator, is configurable. The supported target types are configured in SCA properties table. The validation of target IDs (values) is also configurable. The configuration for the verification of target identifiers consists of two properties for each configured target type. The first property defines the regular expression that will be used to verify if the entered value for the target ID is valid. The second property is the message that will be presented to the user if the verification fails. Both values have a maximum length of 2048 characters. The length of the key name has a maximum of 100 characters.
- **Service names**  
This configuration parameter contains a list of all possible service for all CSP networks.
- **Network names**  
This configuration parameter contains a list of all possible CSP networks.
- **LEA configuration**  
It is configurable if the LEA field shall be displayed in the GUI or not.
- **LEMF configuration**  
In some countries it is not mandatory for LEAs to provide a LIID. In this case a LIID will be generated while LIMA still requires an LIID for each interception. This is called LIID generation or dynamic LIID. Another option is to use sequence numbers for LIID's assigned to interceptions.

## 2.3 LIMA Interception Management

Within LIMA Lawful Intercept, an interception is defined as a technical measure on a technical identity (e.g. MSISDN, IMSI or IMEI). The LIMA Interception Management module facilitates the operators with the day-to-day tasks operators carry out to handle lawful interception warrants.

The interception warrant information is entered into the system using the Interception Module. After entering all the interception details, the interception is stored in the internal database and is scheduled for interception according to the specified warrant start and end date.

The interception related information is derived from several sources;

1. Information received with the legal warrant; the requested service and the specification of the target and the LEMFs. Note; parts of this information might be delivered before or after the definition of the interception itself e.g., in case an electronic H11 interface is used.
2. Information added to the interception by the LIMA MS.  
An Interception Type has to be specified as this translates to choosing the correct Provisioning Plan. The Provisioning Plans determines how interceptions are provisioned in the network. Other optional information like contacts or free-format remarks is 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.

## 2.3.1 Supported Interception Management Functions

### 2.3.1.1 Basic functions

The following functions are supported:

- **Create (add) Interception**

when creating a new interception, a wizard guides the user through the generic, target info, delivery info and miscellaneous screens. The LEA, the LEMF, 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 delivery info and eventual comments.

- **View interception details**

Static and dynamic details of the interception are shown. The dynamic details contain information of the provisioned interceptions like the provisioning status, the IDR log and the versions of the interception.

- **View interception status on provisioned Network Elements**

In the interception overviews, two statuses are shown for each interception: the administrative status and the operational status.

The administrative states refer to state of the related item in LIMA MS. The following statuses are available; incomplete, scheduled, started, stopped and expired.

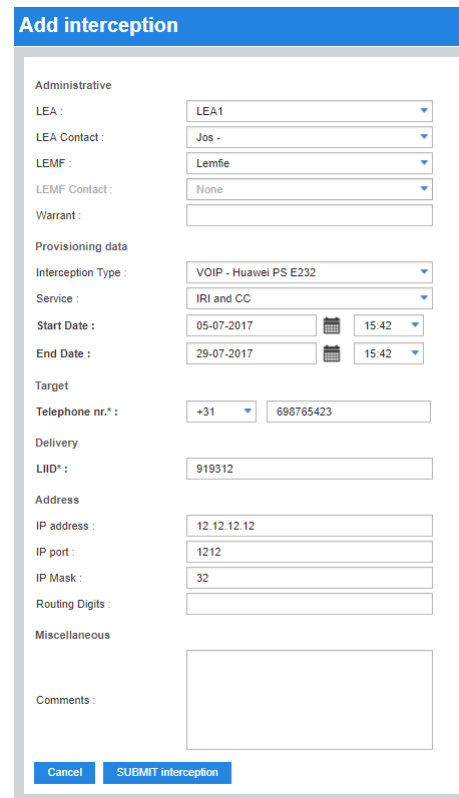
The operational states refer to the provisioning status of the related item in the network infrastructure. The following statuses are available; in progress, Set (ok), Set (error), not set and removed.

- **Manage Interceptions (View, Modify, Copy, Delete)**

- View interception; open an individual interception to view the interception details.
- Modify; change information of an interception. The information fields that can be changed depend on the administrative status of the interception. For each modification a new version of the interception is created.
- Copy; copy the info of a selected interception to create a new interception.
- Delete; permanently remove an interception.

- **Stop / start an interception**

Interceptions can be stopped and started manually. This functionality is only available when the



The screenshot shows a web form titled "Add interception" with the following sections and fields:

- Administrative:** LEA (dropdown: LEA1), LEA Contact (dropdown: Jos -), LEMF (dropdown: Lemfie), LEMF Contact (dropdown: None), Warrant (text input).
- Provisioning data:** Interception Type (dropdown: VOIP - Huawei PS E232), Service (dropdown: IRI and CC), Start Date (calendar: 05-07-2017, time: 15:42), End Date (calendar: 29-07-2017, time: 15:42).
- Target:** Telephone nr.\* (dropdown: +31, text input: 698765423).
- Delivery:** LIID\* (text input: 919312).
- Address:** IP address (text input: 12.12.12.12), IP port (text input: 1212), IP Mask (text input: 32), Routing Digits (text input).
- Miscellaneous:** Comments (text area).

Buttons at the bottom: Cancel, SUBMIT interception.

Figure 4 - Add interception details

administrative state of the interception is active.

- **View Event log**

The event log shows the administrative history for this interception. For every event the related date/time, type of event (ok/error), description of the event and user name of the performer of the action is given.

- **View IDR logs**

Show the operational history (IDR log) for this interception. For every event the local date /time is given, the related NE and the description of the event is given.

- **View Versioning**

The versioning of interceptions gives insight in the change history of an interception. A new version of an interception will be made when an interception is extended. For every version the date/time, the event, the username and change information is given.

### 2.3.1.2 Special functions

- **Test Call**

The test call function will initiate a Delivery test for an Interception and will test the connection between a Mediator and the Monitoring Center (LEMF).

- In configurations with Circuit Switched based delivery (e.g. ETSI TS 201 671) an actual test call is performed to the Monitoring Center.
- In case of Packet Switched delivery (e.g. ETSI TS 102 232) the connection to the Monitoring Center is established and an IP packet is delivered.

- **Re-submit**

The Re-submit function is used as a retry mechanism of the last action that was carried out. In case of persisting problems with provisioning NEs, an interception can remain in a 'un-provisioned' state when all automatic retries have failed. In this situation, the re-submit command will retry the provisioning process for this interception on demand.

- **Query**

The query function will display the interceptions that are applicable for the selected NEs.

- **Interception scheduling and distribution**

The LIMA Management System contains a scheduling and distribution system. The scheduling mechanism will handle the Warrant Start and Warrant End dates, making sure that interception only takes place within the validity period of the warrant. Actions required for provisioning, like activation or deactivation of interceptions, are automatically taken care of by the internal scheduler. 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.

The distribution mechanism handles the provisioning logic. Some network elements need to be provisioned only at the start of an interception (static provisioning). This is often the case with provisioning of VoIP and TDM switches and with the Mediator. Other network elements, like a Router in an IP network need to be provisioned when the user gets assigned an IP address and

de-provisioned when the IP address is released. This is referred to as dynamic provisioning (see also 5.2.3 Passive IP monitors).

Another 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.

- **‘SureTap’ Integrity Check**

Interceptions can be removed, added or altered on NEs for a number of reasons, including software upgrades, system restarts, etc. Therefore it is important to ensure the integrity of the provisioned information.

An integral part of the LIMA Management System is our ‘SureTap’ integrity check mechanism. A (configurable) scheduler will initiate actions to compare the interception information on network elements against the internal database of the Management System. Any differences will be logged and optionally corrected. This mechanism will remove interceptions from network elements that should not be active, add interceptions to network elements that should be present but are not, and update interceptions whose information does not match the interception database of the LIMA Management System.

SureTap works in three ways to maintain the integrity of the interception measures on the NEs:

1. Whenever the connection to a NE is restored
2. On configurable intervals
3. On demand

### 2.3.1.3 Interception tracking option

The interception tracking module allows the assignment of LEA’s to a specifically installed interception tracker. The main goal of assigning trackers is to do an action whenever something changes for an interception. The exact results and actions depend on the chosen Tracker Type.

Some examples that interception trackers can be useful for are:

- Automatically create the interception on a LEMF station.
- Send an email whenever an interception is activated / deactivated.
- Notify a “master LEA” that a “sub LEA” has entered a new interception.
- Notify a CDR analysis system of target identifiers and their accompanying LIIDs in order to visualize the connection of a targeted identifier within large bulk data.

Other goals might be able to achieve with this functionality and it is highly depending on the actual need. The implementation of Tracker Type is customer specific and requires a professional services activity.

## 2.4 Electronic HI-1 interface

The HI1 interface is used for the exchange of warrant and other information between LEAs and CSPs and can be either a manual or an electronic interface. The LIMA Management System provides supports for an electronic interface for HI1 traffic as an optional feature.

The default support e-HI1 interface is based upon standardized ETSI TS 103 120 specifications, but also many proprietary e-HI1 interfaces are supported.

## 2.5 Network Element Management

A NE is an element that is part of the measures that takes care of intercepting traffic and delivering it to the LEMF. Examples are Network components (switches, routers, etc.) with integrated LI functionality, Soft switches, DHCP / Radius monitors and Mediation devices. Basically, any component in the network that needs to be provisioned in order to set a certain type of interception is configured as a NE.

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

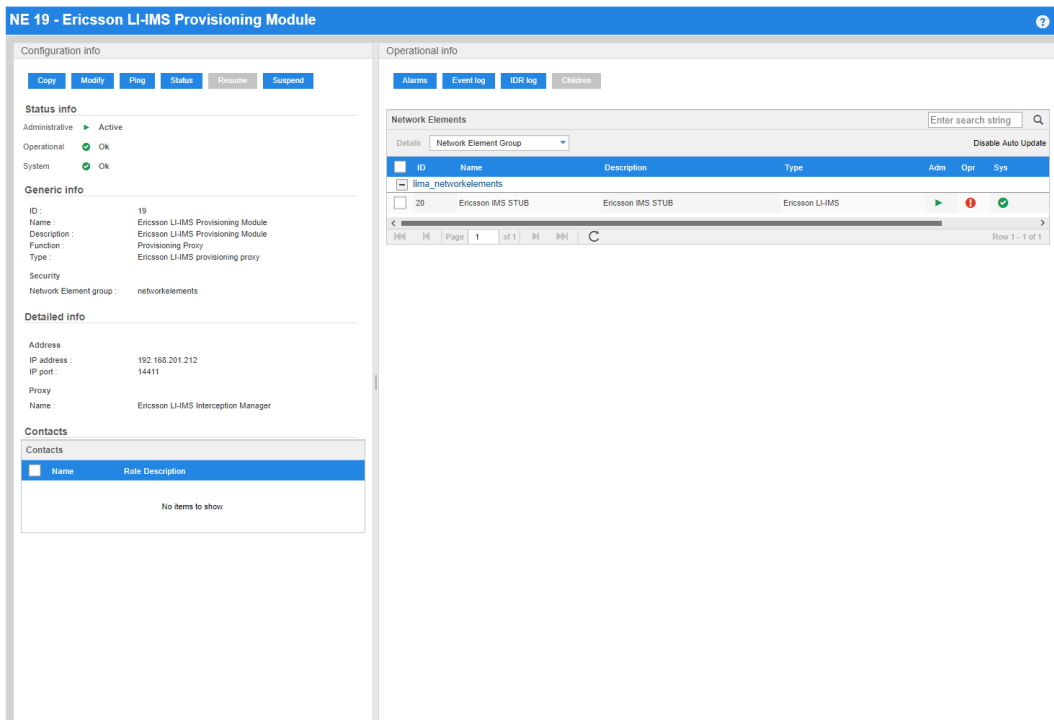


Figure 5: Network Element details

### 2.5.1 Basic Functions

The following functions are supported:

- **Create (add) Network Element**

When creating a new NE, a wizard guides the user through the generic, configuration, contacts info and miscellaneous screens. Generic info like the name of the NE and type of NE can be entered. The configuration screen contains the NE specific parameters. For each NE type different input fields can be used.

To help the administrator in configuring the system properly, a number of Configuration Manuals are available. This indicates the choices that must be made and the type of information that need

to be entered for Interception types and NEs for certain configurations.

- **View Network Element details**

Static and dynamic details of the NEs are shown. The dynamic details contain information of the NEs like the status, received alarms, the event log (administrative history), the IDR log (operational history) and a list function of the interceptions that are provisioned using this NE.

The integrity check show all the results of integrity checks executed with this NE involved (refer to 2.3.1.2). Although an automatic integrity-check is performed when the connection to a NE is established, and periodic integrity-checks can be configured, an integrity-check can be executed on demand also.

- **View Network Element status**

In the NE overviews, the administrative status, the operational status and system status are given. The administrative states refer to state of the related item in LIMA MS. The operational states refer to the provisioning status of the related item in the network infrastructure. The system status gives the status of the server the NE is operating on.

- **Manage Network Elements**

The following functionality is available to manage the NE;

- Modify; change the setting of a NE using the same wizard as used by creating a NE.
- Test the connection status of the NE using a ping function.
- Suspend or resume a NE.
- Delete a NE.

## 2.5.2 Special functions

- **Import Network Element list**

The import NEs function supports the import of SII NEs such as CMTS devices or (Core) Routers. A complete list or a subset of NE's given in the XML can be imported.

- **Discovery of a Network Element**

The discovery of a Network Element applies only to SII Devices. This function is used to determine the Network Element on which the interception for the provided IP address will be provisioned.

## 2.6 Configuration and maintenance usage

### 2.6.1 Interception types

Prior to handling interceptions, one or more Interception types need to be configured. An Interception type is a pre-configured template that is used to create interceptions.

The LIMA MS 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 etc. The LIMA MS can handle various types of interceptions in parallel.

Each Interception Type is linked to a number of NEs. By doing so, the LIMA MS'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 NEs, while the Provisioning Plan defines the behavior for the provisioning of interceptions in the network. By separating the provisioning behavior from the selection of NEs, two or more Interception Types can be defined that use the same behavior.

### 2.6.1.1 Basic Functions

#### ▪ **Create (add) Interception type**

When creating a new Interception type, a wizard guides the user through the various screens. The following functionality is offered during the create process;

- Enter Generic info; definition of name, delivery type, target type, Provisioning Plan and other features. Furthermore it is possible to restrict access to Interceptions types, for example to support multiple LEAs, by assigning access rights to the interceptions related to the Interception type.
- Enter field definitions; it is configurable which input fields for an intercept are required, optional or obsolete. On an interception level, the operator is only obliged to fill the mandatory fields and will not be confused with fields that have no meaning in this installation.
- Enter field restrictions; all fields have a certain built-in default values. In order to tailor the Interception type to a certain network specific situation, these defaults can be overridden by specifying a 'regular expression'. This regular expression is evaluated against the value that is specified by the user when creating an interception. Another field 'Violate message' allows for specifying a message that is shown to the user when an illegal value is entered.
- Define Interception Managers that allows for one interception to be provisioned in multiple networks (for example CS and PS).
- Exclude NEs from selection when an interception with this Interception type will be provisioned.
- Choose the LEMFs associated to this Interception type.
- Enter miscellaneous information for this Interception type.

#### • **View Interception type details**

An overview of all Interception types is available. Per Interception type static and dynamic details are shown. The dynamic details contain the provisioned interceptions based on the selected Interception type. Per interception the administrative and operational status is given.

#### • **Manage Interception types**

The following functionality is available to manage the Interception types;

- Modify the setting of an Interception type using the same wizard as used by creating an Interception type.
- Copy an Interception type.
- Delete an Interception type. Only Interception types with no associated active interceptions can be deleted.



## 2.6.2 LEA Management

A Lawful Enforcement Agency (LEA is an authority that is allowed to issue a lawful warrant. The LIMA MS allows specifying predefined LEAs. LEAs are applied throughout the management system to identify associated LEMFs, Interceptions and Provisioning Interfaces.

### ▪ **Create (add) LEA**

When creating a new LEA, a wizard guides the user through the various screens. The following functionality is offered during the create process;

- Enter Generic info; definition of name, contact information and user access.
- Enter contacts (optional); enter contact information for the assigned LEA contacts.
- Assign LEA filter table (optional), refer to description
- Enter miscellaneous information for this LEA

### ▪ **Manage LEAs**

The following functionality is available to manage LEAs;

- Modify the setting of a LEA using the same wizard as used by creating a LEA.
- Copy a LEA.
- Delete a LEA. A LEA cannot be deleted if it is connected to an active interception and if a LEMF is associated with it.
- View associated Interceptions and LEMF.

### ▪ **LEA filter tables**

LEA filter tables allow for checking a target against a 'predefined target list' for each interception request that is entered. The effect of this target check is that, if a target number is specified that is not allowed according to the selected filter tables, the operator will be notified that the number is not accepted.

### ▪ **Restrict User Access**

A user of the LIMA MS can be restricted to certain LEAs only. This enables to have dedicated groups of operators for different LEAs.

## 2.6.3 LEMF Management

A LEMF is an authority to which the NEs will deliver the intercepted HI-2 and HI-3 information. LEMFs can be preconfigured in the LIMA MS. New interceptions can be linked to a predefined LEMF. This automatically selects the correct HI-2 and HI-3 delivery information for that interception, avoiding errors when entering this information.

### ▪ **Create (add) LEMF**

When creating a new LEMF, a wizard guides the user through the various screens. The following functionality is offered during the create process;

- Enter Generic info; the name and optionally the HI-1 IP address.
- Select LEAs associated with this LEMF.
- Select Interception types associated with this LEMF.
- Select contacts (optional); select associated contacts.
- Enter miscellaneous information for this LEMF.

Next, delivery types (see below) can be associated to this LEMF.

- **View LEMF details**  
An overview of LEMFs is available. The LEMF details also show the active Interceptions related to this LEMF.
- **Manage LEMFs**  
The following functionality is available to manage LEMFs;
  - Modify the setting of a LEMF using the same wizard as used by creating a LEMF.
  - Copy a LEMF.
  - Delete a LEMF. A LEMF cannot be deleted if it is connected to an active interception.
- **Manage delivery type**  
Delivery type information is used to pre-fill the delivery information for an interception when this LEMF is chosen. This makes entering the interception more user-friendly and less error-prone. Next to this the delivery information defines which types of interceptions can be entered for a chosen LEMF. Only Interception types are presented that matches the delivery types of that LEMF. LIMA MS offers functionality to add, modify and delete delivery types.

## 2.6.4 Contact Management (optional)

Contact person information is used when sending information to the LEAs and LEMFs.

The following functionality is offered;

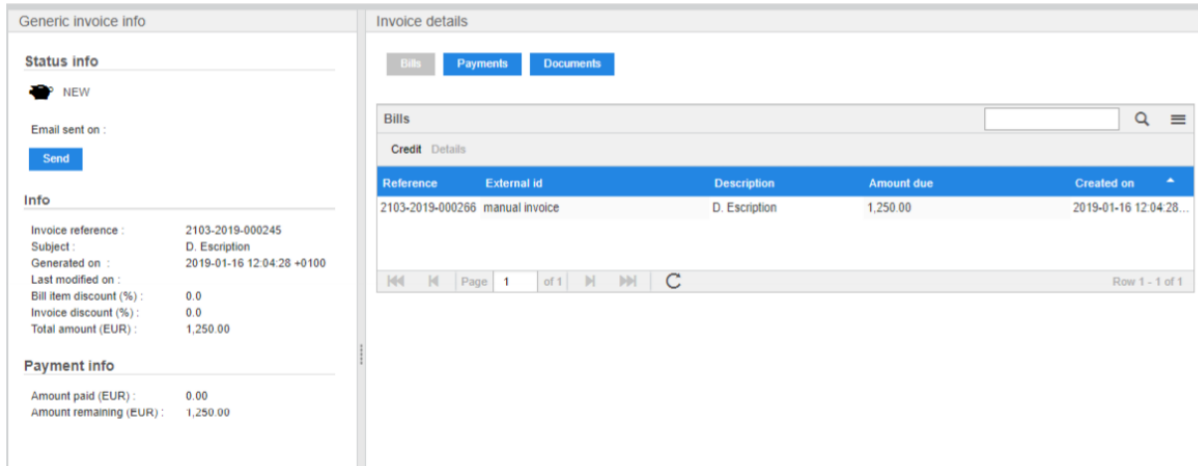
- **Add contacts**  
Administer communication details per contact.
- **View Contacts**  
An overview of all Contacts is available. Per contact detailed information is given about the contact's communication details, associated LEA, LEMFs and NEs.
- **Manage Contacts**  
The following functionality is available to manage Contacts;
  - Modify the contact details
  - Copy a contact.
  - Delete a contact

## 2.6.5 System Administration

- **Clean up function**  
The Clean-up function removes all operational, logging and configuration data of the selected objects from the data or the file system.
- **LEA filter tables**  
As described above in paragraph 2.6.2 LEA Management
- **'Sure tap' Integrity Check**  
As described in paragraph 2.3.1.2 Special functions

## 2.7 Billing and Invoicing Module

For countries where there is a provision to charge the government or the LEAs for the handling of interceptions or warrants, the LIMA Management System can optionally be extended with the LIMA Billing Module. The LIMA Billing Module allows for the configuration of billable items and the generation of invoices. Through this module, the list of generated invoices can be viewed; the status of payments can be checked, which enables the operator to answer questions on specific invoices. The LIMA Billing Module also allows for custom integration with external billing or payment systems to generate and process Excel files for exchanging information with SAP.



The screenshot displays the 'Generic invoice info' and 'Invoice details' sections. The 'Status info' section shows a 'NEW' status and an email sent on date with a 'Send' button. The 'Info' section lists invoice details such as reference, subject, generated on, last modified on, discounts, and total amount. The 'Payment info' section shows the amount paid and remaining. The 'Invoice details' section includes tabs for 'Bills', 'Payments', and 'Documents'. Below these is a 'Bills' table with columns for Reference, External id, Description, Amount due, and Created on. The table contains one row of data for a manual invoice.

Reference	External id	Description	Amount due	Created on
2103-2019-000266	manual invoice	D. Escription	1,250.00	2019-01-16 12:04:28...

## 2.8 Reporting

Via a dedicated reporting module, various statistics can be maintained on the usage and performance of the LIMA MS.

The Reporting function allows authorized users to generate pre-defined Management Reports. The reports may have one or more parameters to be entered at runtime to customize the generated report, like the reporting period or the related LEA.

The following functions are supported:

- Generate reports
  - Create report (choose report template, choose report parameters)
  - Store generated report
- Overview reports
  - List reports per template
  - View report details
- Download report details to a PDF file.

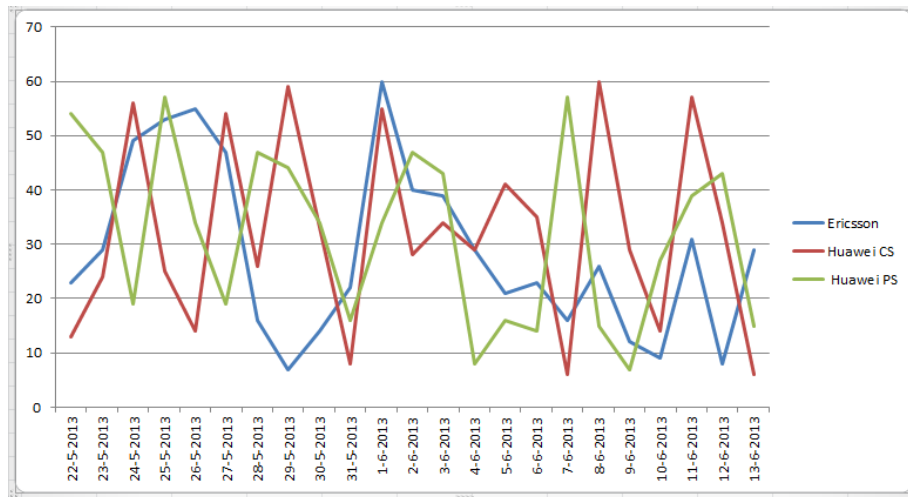


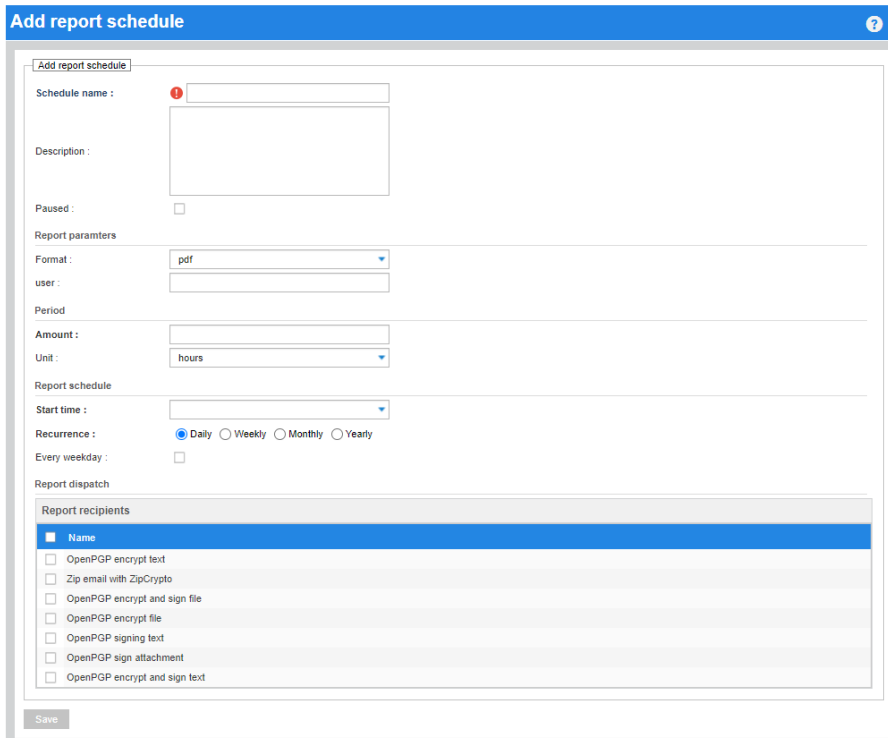
Figure 6: Reporting example; number of interceptions over time

The following management report templates are available by default:

- Interceptions over time: reports the number of interceptions that were active per type of network, per LEA for a given time frame.
- Interceptions per LEMF: reports the number of interceptions per LEMF, per type of network for a given time frame.
- Current Interceptions; detailed report of all active interceptions giving insights in related LEA, LEMF, ID, LIID, Interception type, target ID, start and end date, operational and administrative status.
- Mediator usage w.r.t. interceptions place, received and delivered; this report gives an overview per mediator on:
  - Total number of provisioned taps and total number successfully provisioned taps (percentage).
  - Total number of received intercepts (related to IRI and CC) and total number of successfully managed taps.
  - Total number of delivered intercepts (related to IRI and CC) and total number of successfully delivered taps (percentage).

## 2.8.1 Report scheduling and dispatching

To automate the refresh and dispatch of report templates, reports can be scheduled by authorized users and the results can automatically be dispatched to authorized recipients via e-mail. ZIP and Open PGP encryption is supported for the dispatching of reports. With Open PGP, the user has the option to Encrypt, Sign and Encrypt & Sign the dispatching of reports.



**Add report schedule**

Schedule name : !  
 Description :  
 Paused :  
 Report parameters  
 Format : pdf  
 user :   
 Period  
 Amount :   
 Unit : hours  
 Report schedule  
 Start time :   
 Recurrence :  Daily  Weekly  Monthly  Yearly  
 Every weekday :   
 Report dispatch  
 Report recipients  

Name
<input type="checkbox"/> OpenPGP encrypt text
<input type="checkbox"/> Zip email with ZipCrypto
<input type="checkbox"/> OpenPGP encrypt and sign file
<input type="checkbox"/> OpenPGP encrypt file
<input type="checkbox"/> OpenPGP signing text
<input type="checkbox"/> OpenPGP sign attachment
<input type="checkbox"/> OpenPGP encrypt and sign text

## 2.9 Archiving

Archiving is the process where warrants, interceptions and all associated information are moved from the database to an external file. In the LIMA MS this is a two-step process.

### Step 1: Move to Archive List.

The first archiving step moves expired warrants and expired interceptions to respectively the Warrants and Interceptions Archive.

### Step 2: Move to Archive File.

The second step removes the warrants and interceptions from the Archive List to an Archive File. In this step the warrant, interceptions and all its associated information is removed from the database and written to a XML file.

- **Manual archiving to Archive List**  
 Warrants and interceptions are moved to the Archive list after they have been deleted by an operator. Here warrants and interceptions are still accessible from for a period of 30 days.
- **Scheduled archiving to Archive List**  
 Warrants and interceptions automatically archived by the system two days after they have expired.
- **Scheduled archiving to Archive File**  
 Archiving to a file on a predefined location on the server is automatically initiated 30 days after the warrants and interceptions have been moved to the Archive List. Associated information will also be removed.
- **View archived information**

The expired warrants and interceptions and archived files are accessible via the LIMA Management GUI. The Advanced Search option can be used to locate the warrants, interceptions or records associated with the archived file. After identification the archived file can be downloaded.

- **Archive Audit records**

Audit records are scheduled for archiving to an Archive File every 6 months. Each run of the archiving scheduler will create a new file.

- **Network Element Events**

NE Events are scheduled for archiving to an Archive File every month. NE events are grouped by NE ID and written to a single file per NE. Each run of the archiving scheduler will create a new file.

## 2.10 LIMA Management System non-functional aspects

### 2.10.1 Platform

#### 2.10.1.1 Hardware platform

The LIMA Management System platform is standard deployed on HP DL360 G10 servers. The CPU and memory configuration is dependent on the sizing aspects of the application.



Figure 7 - HP DL 360 G10

#### 2.10.1.2 Operating System

The LIMA Management System is installed on the RHEL 9 Operating System.

#### 2.10.1.3 Virtual deployment

Next to deployment of the solution on bare metal hardware, deployments in a virtual environment are also supported. E.g. the deployment of the LIMA Management System in a private cloud of a telecom operator is fully supported.

### 2.10.2 Logging and Alarming

The LIMA Management System provides functionality for IDR logging and NE-event logging.

### 2.10.2.1 Interception Detail Record (IDR) Logging

By inspecting the IDR log, authorized personnel can investigate what happened to the provisioning of an interception, NE or what actions the system has performed.

The IDR provides detailed operational information of the provisioning of interceptions and the mediation activities. It also provides traffic statistics (Monitor, Mediator) and connectivity problems that may occur (NEs, LEMFs).

The presented IDR log overview provides filter options, including per warrant and per interception filtering.

Access to the IDR log via the LIMA MS GUI is a dedicated security privilege.

Note: The IDR logs do not contain target-information.

### 2.10.2.2 NE-event logging

#### 2.10.2.2.1 Alarms

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 MS is able to receive and display SNMP traps in the GUI also.

#### 2.10.2.2.2 Status Events

When the status of a NE, Warrant or an interception is changed, a notification is to the LIMA MS. In this way, the actual operational state is shown in the GUI.

#### 2.10.2.2.3 E-mail Notifications

Based on changes in the 'Overview' boxes of the Warrants, Interceptions and NEs, the system is able to send an email. This allows the system to be used in 'unattended mode' where the operator is notified when he needs to login into the system in case of malfunctions of NEs and/or intercept deliveries.

An algorithm prevents that the receiver of the e-mails is overloaded with e-mails in case, for instance, a NE reports a failure, a success and a failure again.

The status of an alarm and the defined time interval parameters determine the frequency of notifications.

## 2.10.3 Security

### 2.10.3.1 Access Control

Access control is intended for managing users, user groups, and policies and provides secure user authentication, and role-based and privilege-based access management. The application may store user and user group information locally but optionally can connect to an existing LDAP or Directory server for user authentication. Enabling 2-factor authentication, based upon TOTP, adds an additional layer of protection against obtaining unauthorized access to the system. For more information, see also 2.1.2.

### 2.10.3.2 Cryptographic policies

The core cryptographic subsystems, covering the TLS, IPsec, SSH, DNSSEC, and Kerberos protocols are configured conform the System-wide cryptographic policies as provided by the RHEL 9 DEFAULT profile. See [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/9/html/single\\_security\\_hardening/index#system-wide-crypto-policies\\_using-the-system-wide-cryptographic-policies](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/single_security_hardening/index#system-wide-crypto-policies_using-the-system-wide-cryptographic-policies) for more information.

### 2.10.3.3 Data at Rest

Data at Rest refers to data stored on disk, in databases, files, etc. Target identifiers stored in the database are default encrypted (AES-256 / SHA-512). Log files, etc. never contain any target identifiers.

For solutions where Group 2000 provides the server hardware, we protect the data through HPE Smart Array SR Secure Encryption, which is FIPS 140-2 Level 1 validated enterprise-class encryption solution.

### 2.10.3.4 Data in Transit

For Data in Transit we use strong transport or payload encryption, conform the RHEL 9 cryptographic policies, see also paragraph 2.10.3.2.

Weaker encryption levels can be facilitated as an option at customer's own risk.

### 2.10.3.5 Hardening

For the hardening of the RHEL 9 operating system, we adopted the industry standard CIS level 2 for Server Profile benchmark.

### 2.10.3.6 Auditing

LIMA MS keeps a very detailed audit log that records any action carried out by users logged on to the system. If necessary, an investigation can be conducted related to activities carried out by authorized



users. The audit log provides documentary evidence of the sequence of activities that have, at any time, affected the LI procedures within LIMA MS.

By inspecting the audit log, authorized personnel can investigate what happened to a warrant, interception, NE or what actions a specific user has performed.

Each administrative activity in the GUI of the LIMA MS is logged; each time a user logs in or out to LIMA MS or has viewed or modified an entity the exact date/ time, the related action and the authenticated user of this action is logged.

The presented Audit log overview provides filter options, including per warrant and per interception filtering (amongst others).

Access to the logs is a dedicated security privilege.

## **2.10.4 Performance**

Based on the standardized ETSI X1 interface (ETSI TS 103 221-1 V1.13.1), the measured provisioning performance of the LIMA Management System is up to 800 interception measures per second. The test scenario used 100K interceptions spread over 20 Network Elements. The provisioning of proprietary X1 interfaces might show different results.

## **2.10.5 High Availability**

The flexible architecture of the LIMA Management System enables the deployment of a high availability configuration. In this setup the LIMA Management System platform is configured as a cluster consisting of an active and a standby server. When the active server fails, the distributed cluster manager software will shut down the active server and move to the standby system.

In case of issues with the software or hardware, the cluster manager will move the virtual IP address of the active server to the standby server and starts the Management System on the standby server. For the end-user the process is transparent as no manual interaction is required for the failover. After a failover of the Management System to the standby server, manual interaction is required to restore the failed server and restore the cluster.

The time taken from detection of fault until all applications are active again is roughly 5 minutes.

Additional availability measures are taken on platform level. LIMA servers have redundant disks (RAID-1) and redundant power supplies.

## **2.10.6 Backup**

To safeguard the LIMA Management System platform against data loss due to human errors or other disasters, procedures can be provided for performing a backup of the system, the data and the configuration of the platform.

## 3 LIMA Mediator

Our LIMA Mediator can be integrated with a wide variety of Network Elements. Our mediator supports a wide range of delivery standards so they can be used to handle intercepted traffic in any network in virtually any country.

To accommodate this variety of situations, our LIMA Mediator is designed around the concept of using input and output adapters. On the network side input adapters handle intercepted X2 (IRI or CDC) and X3 (CC or CCC) traffic.

LIMA adapters exist for most network equipment commonly found in Telecom and ISP networks such as GSM, Mobile Data, LTE, 5G, IMS, xDSL and Cable Networks. Many adapters have been factory-tested with the Network Equipment vendors.

On the output side, the LIMA Mediator supports all commonly used Handover standards, implemented by Output Adapters, including many country specific handover formats.

The LIMA Mediator is available in 2 versions:

- Standard Performance Mediator (SPF)
- High Performance Mediator (HPF)

The HPF Mediator is particularly required for networks with high bandwidth requirements, e.g. FTTH networks or 5G Networks.

This chapter describes in more detail the functional and non-functional aspects of the LIMA Mediator.

### 3.1 Introduction

The main function of the LIMA Mediator is to convert intercepted traffic into a format suitable for delivery to the national authorities (the LEMF). A major strength of the LIMA mediator is its modularity. Built around a general lawful interception controller, it uses input and output adapters to communicate to network elements and to the LEA's monitoring facilities.

Connectivity is often the most complex challenge for any solution. Most interfaces to other equipment, though based on open standards, contain proprietary extensions or modifications making it a complex task to integrate a solution. To overcome this problem the LIMA Mediator uses adapters that can be tailored to comply with the interface specifications of either core network equipment or LEMF, without affecting other parts of the LIMA Mediator.

### 3.2 LIMA Mediator architecture

An important asset of the LIMA Mediator is the ease with which LI interfaces can be added, upgraded or removed. For this purpose the LIMA mediator modules provide a flexible routing mechanism to route the 'Intercept Related Information' (IRI) and the 'Content of Communication' (CC), received via the core network interfaces, to the appropriate LEMF interface.

Figure 8 gives a logical overview of the LIMA Mediator architecture.

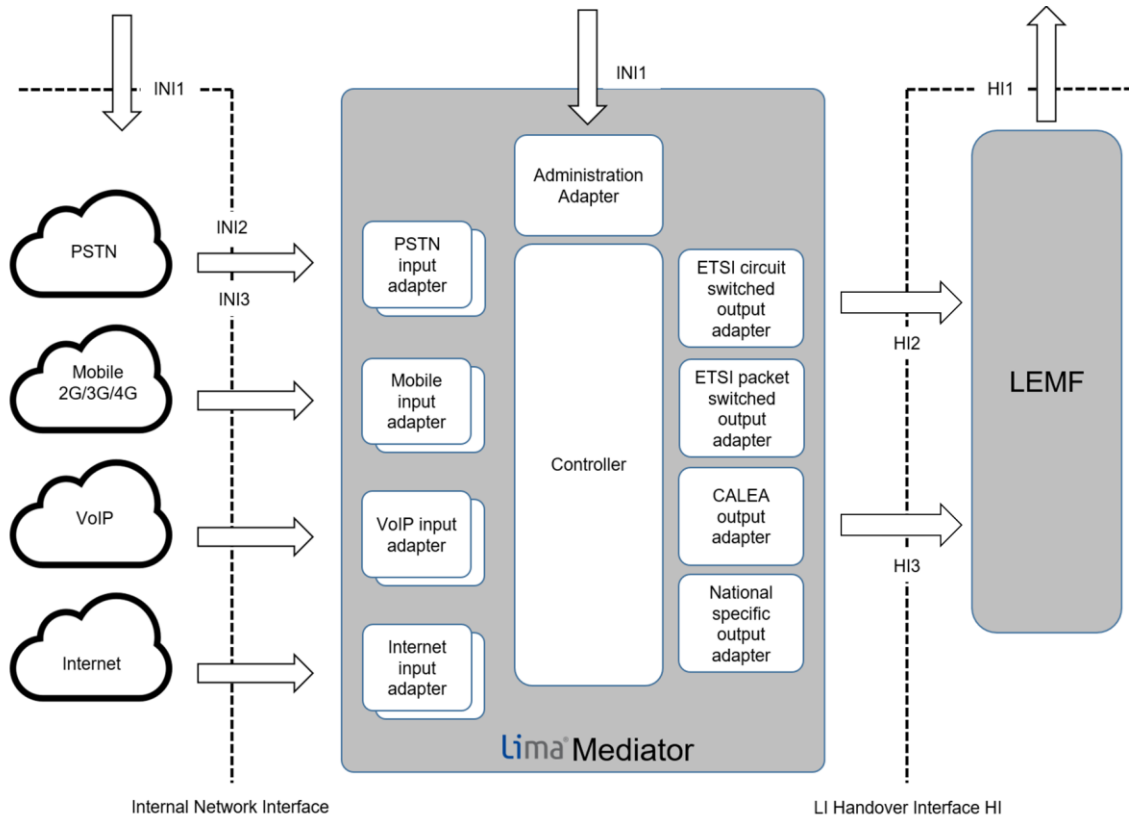


Figure 8 - LIMA Mediator architecture

The LIMA Mediator implements the following functions:

- The Conversion of the intercepted information from the format received at the INI-2 and INI-3 interfaces to the format required by the HI-2 and HI-3 interfaces.
- The actual delivery of the interception information at the required interface.

The input adapters implement the following interfaces with the different network elements:

- Interception Related Information (IRI). This is the so-called INI-2 interface.
- Content of Communication (CC). This is the so-called INI-3 interface.

The output adapters implement the following interfaces with the LEMF:

- Interception Related Information (IRI). This is the so-called HI-2 interface.
- Content of Communication (CC). This is the so-called HI-3 interface.

To connect to other LI management systems, (customized) administration adapters (INI-1) can be attached to the controller.

### 3.2.1 Input Adapters

Telecom operators have a multitude of networks (e.g. PSTN, VoIP, IP, GSM, UMTS, LTE and 5G) that are implemented using the network equipment of various vendors. Each network vendor has its own LI

interface. For the integration of the LIMA Mediator in these networks a number of input adapters are required.

Group 2000 has implemented input adapters for many network elements among which that of network vendors like Cisco, Ericsson, Huawei, Italtel, Juniper, Metaswitch, Nokia, Nortel, OpenWave, Ribbon and ZTE.

### 3.2.2 Output Adapters

The LIMA Mediators support different output adapters. Different output adapter for different types of traffic (e.g. CS or PS). But also, different output adapters for different handover interfaces, including the recent extensions in ETSI TS 103 120 and ETSI TS 102 232 part 1 and 7 for 5G support.

A specific output adapter supports a hand-over specification for a specific type of traffic for a specific legislation. In this way, LIMA can support different regulations in different countries by deploying different output adapters.

Besides the standard ETSI, 3GPP and CALEA-based output adapters, Group 2000 has implemented output adapters for different European countries for the delivery of intercepted information.

### 3.2.3 Buffering

The LIMA Mediator support buffering in memory, where the buffering time (in seconds) can be configured independently for both IRI and for CC. The amount of additional RAM memory in combination with the actual throughput and traffic profile would define the actual buffering time.

## 3.3 LIMA Mediator non-functional aspects

### 3.3.1 Platform

#### 3.3.1.1 Hardware platform

The LIMA Mediator platform is standard deployed on HP DL360 G10 servers. The CPU and memory configuration is dependent on the sizing aspects and performance requirements of the application.



Figure 9 - HP DL 360 G10

### 3.3.1.2 Operating System

The LIMA Mediator is installed on the RHEL 9 operating system. The LIMA HPF Mediator is deployed as an container, for which RedHat Enterprise UBI 9 Operating System is used. Check <https://access.redhat.com/support/policy/rhel-container-compatibility> for compatibility with host OS versions.

### 3.3.1.3 Virtual deployment

Next to deployment of the solution on bare metal hardware, deployments in a virtual environment are also supported. E.g. the deployment of the LIMA Mediator in a private cloud of a telecom operator is fully supported.

## 3.3.2 Management

The LIMA Mediator is typically managed through the LIMA Management System.

### 3.3.2.1 Alarming

The LIMA Mediator is capable of generating alarms on a number of exception situations that are sent to a remote Management System (e.g. the LIMA MS) using SNMP traps and are also stored internally in an Alarm log file.

### 3.3.2.2 Logging and Statistics

The LIMA Mediator keeps detailed logging of interception events handled on the system. The system is also capable of performing various levels of logging for troubleshooting purposes. For the following interception events logging is created:

**Admin adapters:**

- All events affecting interceptions in the LIMA Mediator System database

**Provisioning Adapters:**

- All events affecting interceptions in the LIMA Mediator System database

**Input Adapters:**

- Discarded IRI interception data (IRI records, Interception files)
- Discards CC records, out-of-sequence CC records, IRI data missing for CC record
- Numbers of received and discarded CC packets

**Output Adapters:**

- Discarded IRI records, sent IRI records
- CC connection opened / closed, discarded items
- Numbers of sent / discarded CC packets

The LIMA Mediator also generates statistics which can be viewed through the LIMA Management System. The data can also be requested through an SNMP-Request.

Example statistics (actual statistics depends on the types of adapters implemented):

- Current number of messages or calls in progress
- Maximum number of messages or calls in process
- Numbers of incoming messages or calls (input Adapters)
- Numbers of erroneous incoming messages or calls (input Adapters)
- Numbers of outgoing messages or calls (output Adapters)
- Numbers of erroneous outgoing messages or calls (output Adapters)
- Minimum processing time for a message or call
- Maximum processing time for a message or call

### **3.3.3 Security**

#### **3.3.3.1 Cryptographic policies**

The core cryptographic subsystems, covering the TLS, IPsec, SSH, DNSSec, and Kerberos protocols are configured conform the System-wide cryptographic policies as provided by the RHEL 9 DEFAULT profile. See [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/9/html/single/security\\_hardening/index#system-wide-crypto-policies\\_using-the-system-wide-cryptographic-policies](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/single/security_hardening/index#system-wide-crypto-policies_using-the-system-wide-cryptographic-policies) for more information.

#### **3.3.3.2 Data at Rest**

Data at Rest refers to data stored on disk, in databases, files, etc. Log files, etc. created by the LIMA Mediator never contain any target identifiers.

For solutions where Group 2000 provides the server hardware, we protect the data through HPE Smart Array SR Secure Encryption, which is FIPS 140-2 Level 1 validated enterprise-class encryption solution.

#### **3.3.3.3 Data in Transit**

For Data in Transit we use strong transport or payload encryption, conform the RHEL 9 cryptographic policies, see 3.3.3.1.

Weaker encryption levels can be facilitated as on option at customer's own risk.

#### **3.3.3.4 Hardening**

For the hardening of the RHEL 9 operating system, we adopted the industry standard CIS level 2 for Server Profile benchmark.

### 3.3.4 Performance

#### LIMA HPF Mediator deployed on Intel Xeon-Gold 6348 CPU based server

The LIMA HPF mediator solution has a maximum validated sustained throughput of 23Gbps under the following conditions:

- **Hardware:** HPE DL360 Gen10 Plus server, 1 x Intel Xeon-Gold 6348 CPU: 2.6GHz, 28-core hyperthreaded, 256GB RAM: 8 DIMMs, 3200MTps, 2 x 100Gbps Ethernet interface
- **Input:** 30 sessions with ETSI-221, TCP-based traffic
- **Output:** ETSI-232, TLS (AES256-GCM-SHA384), no country specific options
- **Traffic profile:** sustained flat rate, 80% 1514-byte packets, 20% 172-byte packets

For a single session, the maximum validated sustained mediation throughput is 3.9 Gbps.

#### LIMA HPF Mediator deployed on Intel Xeon-Silver 4210 CPU based server

When deployed on a HP DL360 Gen10 Server with Intel Xeon-Silver 4210 (2.2GHz/10-core) CPU, the LIMA HPF mediator solution has been validated up to 10Gbps sustained throughput for TCP based traffic, based on ETSI TS 102-232. For UDP based traffic a sustained throughput of up to 5Gbps can be achieved depending on the end-to-end network configuration<sup>1</sup>. Actual maximum sustained throughput depends on the exact offered hardware configuration as specified in below table.

Sustained TCP Throughput	CPU's	RAM
Up to 2Gbps	1x 10-core with hypertreading @ 2.2GHz, L3 Cache: 13.75MB	<ul style="list-style-type: none"> <li>• 16GB,</li> <li>• 2400MT/s (1 DIMM using 1 memory-channel)</li> <li>• Memory bandwidth at least: 17GBps</li> <li>• "Huge pages" must be switched off</li> <li>• DF-buffer storage space available: 9GB</li> </ul>
2 to 5Gbps	1x 10-core with hypertreading @ 2.2GHz, L3 Cache: 13.75MB	<ul style="list-style-type: none"> <li>• 64GB, 2400MT/s (4 DIMMS using 4 memory-channels)</li> <li>• Memory bandwidth at least: 59GBps</li> <li>• DF-buffer storage space available: 25GB</li> </ul>
5 to 10Gbps	2x 10-core with hypertreading @ 2.2GHz, L3 Cache: 13.75MB	<ul style="list-style-type: none"> <li>• 128GB, 2400MT/s (8 DIMMs using 4 memory-channels per CPU)</li> <li>• Memory bandwidth at least: 118GBps</li> <li>• DF-buffer storage space available: 40GB</li> </ul>

Table 1 - HPF Mediator Performance characteristics based upon HP DL360 G10 hardware

#### LIMA SPF Mediator

A single LIMA SPF mediator system running on a single DL360G9 server has been validated up to 900Mbps overall throughput, based on ETSI TS 102-232 delivery to 5 end-points, sustained flat rate, 80% 1514 byte packets, 20% 172 byte packets.

<sup>1</sup> Achieving a high throughput with UDP is not straightforward. Optimizations for throughput are necessary, e.g. with regard to the MTU-size, the packet sizes, tuning of Linux kernel parameters, and software thread affinity. For LI, Group 2000 cannot influence the packet sizes. Another important aspect is that the MTU-size on the CSP to Mediation Device shall be larger than the MTU size of the target communication in order to avoid IP-packet fragmentation on the CSP to Mediation Device connections.

## 4 LIMA LMISF

LI for VoLTE S8 Home Routing (S8HR) is described in 33.108 section 12.7.3 and introduces the need for an additional LI Mirror IMS State Function (LMISF) component. The LMISF is a LI specific function introduced to support the lawful interception of voice services in the VPLMN when S8HR is used as the roaming architecture and integrates with customers proprietary Bearer Binding Intercept and Forward Function (BBIFF) component.

### 4.1 LIMA LMISF solution architecture

The LI architecture for support of S8HR is shown in Figure 10

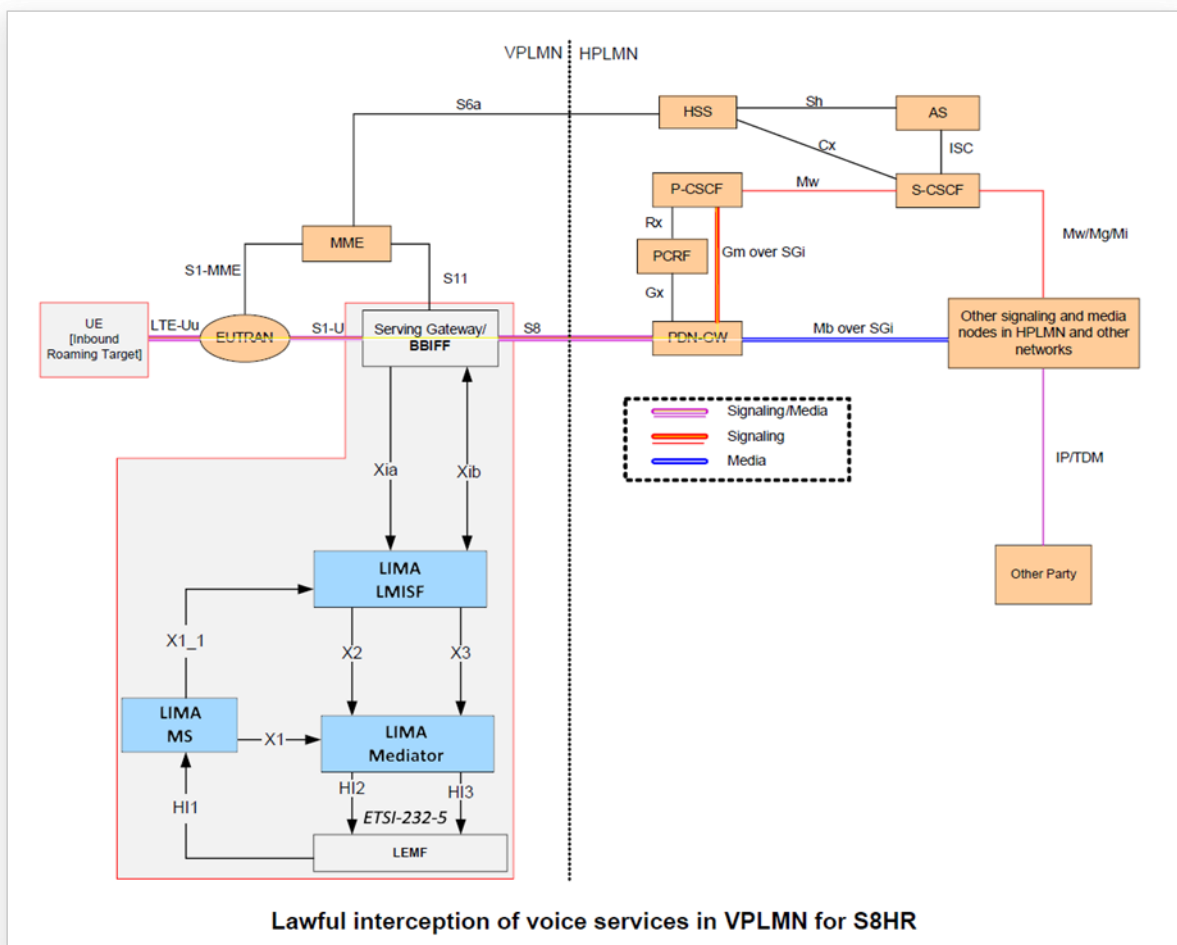


Figure 10 - S8 Home Routing support

#### Interfaces

The purpose of the interfaces are:

- X1\_1: provisioning from the LIMA MS to the LIMA LMISF.
- X2: the IRI of the intercepted VoIP calls.



- X3: the CC of the intercepted VoIP calls.
- Xia: Deliver the GTP packets for the IMS signalling bearers and the selected media bearers from the BBIFF to the LMISF.
- Xib: Instruct the BBIFF with packet forwarding rules and the intercepted IMS Signalling Bearer information.

### Process flow

After start-up, the LMISF will provision the configured APNs for inspection.

The bearer-notifications are received via the Xib interface.

The contents of the signalling bearer will be received over the Xia interface. The ULIC header contains correlation-information, and the payload contains the SIP signalling. The SIP signalling is processed in order to detect if the call must be intercepted.

If the call must be intercepted, the BBIFF will be provisioned to intercept the associated media bearer.

At the same time, IRI is generated and sent to the LIMA Mediator.

After dynamic provisioning of the media bearer, the contents of the media bearer will also be received over the Xib interface, but on a dedicated port. The ULIC header contains correlation information, and the payload contains the RTP packets.

### Handover format

The default handover format will be in the ETSI TS 102 232-5 format.

## 4.2 LIMA LMISF non-functional aspects

### 4.2.1 Platform

#### 4.2.1.1 Hardware platform

The LIMA LMISF platform is standard deployed on HP DL360 G10 servers. The CPU and memory configuration is dependent on the sizing aspects and performance requirements of the application.



Figure 11 - HP DL 360 G10

#### 4.2.1.2 Operating System

The LIMA LMISF is installed on the RHEL 9 operating system. The LIMA LMISF is deployed as an container, for which RedHat Enterprise UBI 9 Operating System is used. Check <https://access.redhat.com/support/policy/rhel-container-compatibility> for compatibility with host OS versions.

### 4.2.1.3 Virtual deployment

Next to deployment of the solution on bare metal hardware, deployments in a virtual environment are also supported. E.g. the deployment of the LIMA LMISF in a private cloud of a telecom operator is fully supported.

## 4.2.2 Security

### 4.2.2.1 Cryptographic policies

The core cryptographic subsystems, covering the TLS, IPsec, SSH, DNSSec, and Kerberos protocols are configured conform the System-wide cryptographic policies as provided by the RHEL 9 DEFAULT profile. See [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/9/html-single/security\\_hardening/index#system-wide-crypto-policies\\_using-the-system-wide-cryptographic-policies](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/security_hardening/index#system-wide-crypto-policies_using-the-system-wide-cryptographic-policies) for more information.

### 4.2.2.2 Data at Rest

Data at Rest refers to data stored on disk, in databases, files, etc. Log files, etc. created by the LIMA LMISF never contain any target identifiers.

For solutions where Group 2000 provides the server hardware, we protect the data through HPE Smart Array SR Secure Encryption, which is FIPS 140-2 Level 1 validated enterprise-class encryption solution.

### 4.2.2.3 Data in Transit

For Data in Transit we use strong transport or payload encryption, conform the RHEL 9 cryptographic policies, see 3.3.3.1.

Weaker encryption levels can be facilitated as an option at customer's own risk.

### 4.2.2.4 Hardening

For the hardening of the RHEL 9 operating system, we adopted the industry standard CIS level 2 for Server Profile benchmark.

## 5 LIMA Monitors

### 5.1 Introduction

For legal purposes each telecommunication operator and internet service provider is obliged to have legal interception solutions in their network. With the multifunctional IP monitor, Group 2000 combined all common IP protocols in one probe. In order to create the flexibility you need and create a solution which is powerful and cost effective with minimal impact for your customer operations and your network.

The passive nature of the LIMA IP monitor allows it to be easily installed in a network. In situations where warrants are handled only occasionally, hooking up the system to the appropriate links allows a person with only basic training to fulfil the interception obligation within a reasonable timeframe. Passive monitoring is also suitable in (semi-) permanent setups. Implementation of the interception solution can be done with minimal impact and visibility by avoiding integration with existing network elements.

The LIMA IP monitor is a robust, powerful and integrated IP probe which combines multiple IP interception functions in one physical system. The probe is able to intercept and capture all common IP, Email and VoIP traffic. One of the standard deployment options of the LIMA Monitor is the capability to include a mediation function. With this function, all intercepted data will be modified in such a format that each monitoring center is able to receive and analyze the intercepted data. The LIMA IP monitor is truly flexible, powerful and multi-functional whilst combining traffic analysis, interception and mediation in a single box.

The system is designed for each IP network, and is designed for non-complex environments to the most complex (multi country) IP or broadband networks.

### 5.2 LIMA Monitors (Filters)

The following section describes the various supported filter options on the LIMA IP Monitors for passive interception of IP based traffic.

#### 5.2.1 LIMA VoIP monitors

##### 5.2.1.1 LIMA SIP monitor

The Session Initiation Protocol (SIP) is a signaling communications protocol, widely used for controlling multimedia communication sessions such as voice and video calls over IP networks. SIP can be used for two-party (unicast) or multiparty (multicast) sessions consisting of one or several media streams. The voice and video stream communications in SIP applications are carried over another application protocol, the Real-time Transport Protocol (RTP). Parameters (port numbers, protocols, codecs) for these media streams are defined and negotiated using the Session Description Protocol (SDP) which is transported in the SIP packet body.

For passive monitoring of VoIP traffic, the LIMA portfolio contains a SIP monitor. Added to a LIMA configuration as a separate device it will monitor SIP traffic near a soft switch, filtering out target traffic.

SIP messages for targets will be sent to the LIMA Mediator. RTP traffic is intercepted passively using an RTP monitor.

The LIMA SIP Monitor is a network traffic monitor for the interception of VoIP calls. It analyses all SIP traffic on its connected/configured Ethernet devices and passes on only target data on to the LIMA Mediator for handover to the monitoring center.

The SIP Monitor reports detected targets to the LIMA MS and LIMA Mediator via IRI triggers. Via a trigger function it controls the RTP Monitor to intercept the associated RTP session data.

When using the LIMA RTP monitor, RTP is intercepted passively. This requires a copy of the correct voice and video IP traffic to be sent to the RTP monitor. In situations where this is problematic, the SIP monitor can also be combined with an SII module. In such a situation the associated RTP streams are actively intercepted on an SII capable device such as a CMTS or Router.

The LIMA SIP monitor complies with the following specifications:

- **RFC 3261** - SIP Session Initiation Protocol – version 2.0
- **RFC 4566** - SDP Session Description Protocol
- **RFC 2396** - URI Uniform Resource Identifiers (URI): Generic Syntax.

### **5.2.1.2 LIMA RTP Monitor**

The LIMA RTP monitor intercepts RTP traffic of a SIP call when triggered by a SIP monitor. It will capture the voice and video packets of a call and forward them to the Mediator in PCLI format (Packet Cable standard for Lawful Intercept)

## **5.2.2 LIMA Mail monitors**

### **5.2.2.1 LIMA SMTP monitor**

The LIMA SMTP monitor is used to passively monitor SMTP traffic. It filters SMTP traffic based on To: and From: mail addresses or a target IP address. It extracts IRI data as well as the contents of the email message. In combination with a LIMA Mediator it sends the intercepted traffic to a Monitoring Centre according to the ETSI 232 specification.

The SMTP Monitor reports detected targets to the LIMA MS and LIMA Mediator via IRI triggers and forwarding of session data for CC. Information about non-targets is neglected. Only statistics are assembled over non-target SMTP traffic (in addition to target SMTP traffic).

The LIMA SMTP monitor complies with the following specifications:

- **RFC 5321** - Simple Mail Transfer Protocol (ESMTP)
- **RFC 2920 - PIPELINING** - Command pipelining (PIPELINING)
- **RFC 2554 / RFC 4954 / RFC 4422** - Authenticated SMTP (AUTH).

### 5.2.2.2 LIMA POP monitor

The LIMA POP monitor complements the SMTP monitor to form a complete passive Email interception solution. Where the SMTP monitor intercepts incoming and outgoing email messages, the POP monitor generates events when an email message is downloaded from the server by a target. It checks all POP3 traffic seen on its connected/configured Ethernet devices. The POP Monitor passes on only target data on to the LIMA Mediator for handover to the monitoring center.

The LIMA POP Monitor reports detected targets to the LIMA MS and LIMA Mediator via IRI triggers and forwarding of session data for CC. Information about non-targets is neglected. Only statistical information is registered about non-target POP3 traffic (in addition to target POP3 traffic).

The LIMA POP monitor complies with the following specifications:

- **RFC 1939** - POP - Post Office Protocol - Version 3
- **RFC 5034** - POP3 SASL Authentication Mechanism

### 5.2.2.3 LIMA IMAP monitor

If IMAP is supported by a Mail Server for downloading messages, the LIMA IMAP monitor can be used to generate the mail download events. It is a network traffic monitor that checks all IMAP traffic seen on its connected/configured Ethernet devices. The LIMA IMAP Monitor passes on only target data on to the LIMA Mediator for handover to the monitoring center.

The LIMA IMAP Monitor reports detected targets to the LIMA MS and LIMA Mediator via IRI triggers and forwarding of session data for CC. Information about non-targets is neglected. Only statistics are assembled over non-target IMAP traffic (in addition to target IMAP traffic).

The LIMA IMAP monitor complies with the following specifications:

- **RFC 3501** – IMAP version 4rev1
- **Pipelining** - As per RFC 3051 section 5.5, an IMAP server shall support handling of new commands while previous commands are still processed. This feature is known as pipelining. Pipelining is supported by the LIMA IMAP Monitor.
- **RFC 4978** - The IMAP COMPRESS Extension

## 5.2.3 Passive IP monitors

### 5.2.3.1 LIMA Radius monitor

The LIMA Radius monitor is used to track IP assignments done via Radius. Provisioned with a user name the Radius monitor will monitor traffic to and from multiple Radius servers and triggers the LIMA MS when a match is found. The LIMA MS uses the provided IP address to dynamically intercept the associated IP stream. Combined with a LIMA Mediator, ETSI compliant IRI data will be sent to the Monitoring Centre providing accurate information about the target's internet access activities.

### **5.2.3.2 LIMA DHCP monitor**

The LIMA DHCP monitor is used to track IP assignments via DHCP. It tracks end user MAC addresses as well as OPTION82 MAC addresses of the Cable Modem. It will trigger the LIMA MS when a match is found and provide the IP address assigned to the user. The LIMA MS uses the provided IP address to dynamically intercept the associated IP stream. Combined with a LIMA Mediator, ETSI compliant IRI data will be sent to the Monitoring Centre providing accurate information about the target's internet access activities.

## Glossary

Abbreviations	Description
3GPP	3rd Generation Partnership Project
CALEA	Communications Assistance for Law Enforcement Act
CC	Contents of Communication
CS	Circuit Switched
CSP	Communications Service Provide
DHCP	Dynamic Host Configuration Protocol
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile communications
GUI	Graphical User Interface
IDR	Interception Detail Record
IMAP	Internet Message Access Protocol
IRI	Interception Related Information
ISP	Internet Service Provider
HI	Handover Interface
HI1	Handover Interface Port 1 (for Administration Information)
HI2	Handover Interface Port 2 (for Interception Related Information)
HI3	Handover Interface Port 3 (for Content of Communication)
IMEI	International Mobile station Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIID	Lawful Interception IDentifier
LIMA MS	LIMA Management System
MAC-address	Media Access Control address
MSISDN	Mobile Subscriber ISDN Number
NE	Network Element
POP	Post Office Protocol
POP3	Post Office Protocol 3
PS	Packet Switched
PSTN	Public Switched Telephone Network
RTP	Real-time Transport Protocol
SASL	Simple Authentication and Security Layer
SII	Service Independent Intercept
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Standard Network Management Protocol
URI	Uniform Resource Identifier

## 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.

Group 2000 is not liable for failure to perform the obligations of this proposal if such failure is as a result of Force Majeure including but not limited to fire, flood, earthquake, storm, hurricane, epidemic diseases or other natural disaster, war, invasion, act of foreign enemies, hostilities (regardless of whether war is declared), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation, terrorist activities, nationalisation, government sanction, blockage, embargo, labor dispute, strike, lockout or interruption or failure of electricity [or telephone service].

All trademarks are acknowledged.

## Non-disclosure notice

This document is disclosed for the use by Customer 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: +31 546 482 400  
Fax +31 546 482 401