NOKIA

Nokia Lawful Interception Gateway Release 4

Product Description

The information in this document is subject to change without notice and describes only the product defined in the introduction of this documentation. This document is intended for the use of Nokia's customers only for the purposes of the agreement under which the document is submitted, and no part of it may be reproduced or transmitted in any form or means without the prior written permission of Nokia. The document has been prepared to be used by professional and properly trained personnel, and the customer assumes full responsibility when using it. Nokia welcomes customer comments as part of the process of continuous development and improvement of the documentation.

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products cannot be considered binding but shall be defined in the agreement made between Nokia and the customer. However, Nokia has made all reasonable efforts to ensure that the instructions contained in the document are adequate and free of material errors and omissions. Nokia will, if necessary, explain issues which may not be covered by the document.

Nokia's liability for any errors in the document is limited to the documentary correction of errors. NOKIA WILL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT OR FOR ANY DAMAGES, INCIDENTAL OR CONSEQUENTIAL (INCLUDING MONETARY LOSSES), that might arise from the use of this document or the information in it.

Contents

Summary of changes

Changes between LIG Release 4 and LIG Release 3

The following new LIG functionalities have been added:

Support for new IP1260 HW platform, RoHS compliancy

IPSO platform release 3.8 support

Support for new LIE

- Nokia Flexi ISN
- LI support for Nokia IMS Connection Processing Server (CPS)

Enhanced performance

- support for ‘Tornado Phase’ Architecture with LIPv2

Enhanced user operability

- Command Line Interface (CLI) Admin commands
- LAAP (LIG Aided Authorisation Practice)
- LIG volume control licence
- SNMP admin alarm
- web interface usability improvements
- MultiSIM

Support for security

- LIPSec
- hardware accelerated encryption supported for IPSec with the IP1260 platform

Internet Protocol version 6 (IPv6) support

- full IPv6 support
- IPv6 in the operator backbone:
  - Lawful Interception Protocol (LIP) is transferred over IPv6 TCP in the LIC, LIB, GGSN/Flexi ISN, 2G SGSN, and CPS
  - web, file transfers, and CLI over IPv6 TCP
- IPv6 in the LIG user network:
  - Interception-Related Information (IRI) events and Communication Content (CC) headers can contain IPv6 addresses
  - web and CLI transferred over IPv6 TCP
  - intercepted data and alarms forwarded over IPv6

Location Dependent Interception (LDI)

- enhanced LDI with new parameters

New LIB element functionality

- LIB enhancements

New general functionality

- QoS parameters in IRI events (only with LIPv2)
- ASN.1 notifications for proprietary IRI events
- customisation improvements

1 About this document

This product description gives an overview of the Nokia Lawful Interception Gateway (LIG) Release 4.

1.1 Purpose

This document provides general information about the functionality of the Nokia Lawful Interception Gateway (LIG) and explains the versatile interception role of the LIG in the mobile network. This document describes not only the new features available in Nokia LIG Release 4, but also provides a description of the general LIG functionality.

This document points out the main functionalities and main benefits of Nokia LIG and how the LIG interacts with the Packet Core network elements.

1.2 Audience

This document is an introductory description of Nokia Lawful Interception Gateway Release 4 and is targeted at readers who need a general overview of the product functionality. Readers of this document should be familiar with IP networks and have knowledge about General Packet Radio Service (GPRS), 3G, and IP Multimedia Subsystem (IMS) networks. Knowledge about the drivers behind lawful interception is beneficial.

2 Introduction to Nokia LIG

Operators in most countries need to meet the local authority requirements on Lawful Interception (LI) before launching commercial GSM (GPRS) and UMTS packet switched domain network services. Nokia Lawful Interception Gateway (LIG) provides the essential network functionality within the 2G and 3G packet core infrastructures to practise LI. The Nokia LIG system allows Law Enforcement Agencies (LEA) to intercept both GSM and UMTS mobile data calls. The method of interception for packet switched domain networks is completely different from circuit switched domain call interception. In the circuit switched domain, interception is mainly voice-based audio recording, whereas in the packet switched domain the data is intercepted between the mobile station and the access point. Interception of IMS users is now also possible in GSM and UMTS networks.

IMSI, IMEI, or MSISDN and SIP URI or TEL URI (for IMS) can be used for identifying the subscriber to be intercepted. Both the Communication Content (CC) and the Interception-related Information (IRI) can be collected. CC is the user data sent or received by the target, and IRI is the control data information related to LI.

The Nokia LIG is a scalable system based on the same IPSO SW platform as in the Nokia Gateway GPRS Support Node (GGSN). It offers an ideal solution for building GPRS and UMTS interception systems. The HW platform is based on the new IP1260 HW but the earlier IP740 HW is also supported.

2.1 Nokia LIG in brief

The Nokia LIG system enables the lawful interception functionality in the Nokia packet core. Nokia LIG provides the following key functionalities:

- interception based on MSISDN, IMEI, and IMSI
- interception based on SIP URI, TEL URI (for IMS)
- interception from all relevant Nokia packet core network elements: 2G/3G SGSN, GGSN, Flexi ISN, and CPS (CSCF in IMS)

- separate interception for LI control data (Interception-related Information, IRI) and LI payload data (Communication Content, CC)
- output data format can be adjusted according to country-specific requirements
- scalable hierarchy between Lawful Interception Controllers (LIC), Lawful Interception Browsers (LIB), and Lawful Interception Extensions (LIE)
- several independent user groups for administration (Admin user), auditing (Audit user), authorising authorities (AA users) and law enforcement agencies (LEA users)

2.2 Benefits of Nokia LIG

The main benefits of Nokia LIG Release 4 are outlined below.

Support for Lawful Interception Extension (LIE) for Nokia packet core elements

LI is possible with all Nokia packet core network elements: 2G/3G SGSN, GGSN, and Flexi ISN. Communication is based either on LIPv1 and/or LIPv2.

Support for LIE for Nokia CPS in the IP multimedia subsystem

Nokia LIG interconnects with Nokia CPS (CSCF functionality) for intercepting IP Multimedia Subsystem (IMS) traffic. Communication between the LIG system and LIE is based on LIPv2.

New ‘tornado phase’ architecture enables LI for large traffic volumes

Distributing the target databases to the intercepting nodes ensures the reliable handling of interception in the presence of real mass-traffic in the operator networks. The distributed databases significantly reduce the control traffic (1 / 100), which results in faster network element start-ups and assures that there are no gaps in the interception starts. Communication between the LIG system and LIE elements is based on LIPv2. For backward compatibility also LIPv1 is supported.

Scalable and robust architecture

There can be several LIG systems within one network, and all interceptions, users, and other definitions can be specific inside the LIG system. The Nokia LIG system consists of a Lawful Interception Controller (LIC) and one or several Lawful Interception Browsers (LIB). Each LIC can control a number of LIB elements. The LI capacity can be increased by increasing the number of LIB and/or LIC elements. In addition load balancing can be applied.

Support for a number of independent users in four user groups

There are four independent user groups for an LIG system: Administrator (Admin user), Auditor (Audit user), Authorising Authority (AA), and Law Enforcement Agency (LEA). There is one Auditor and Administrator, and several LEA and AA users for each LIG system.

Location Dependent Interception (LDI) with high granularity

LDI filtering can be based on an interception area defined by the CGI, SAI, or RAI. Now LI can also be based on an interception area specified by the Mobile Country Code (MCC), MCC+ Mobile Network Code (MNC), or MCC+MNC+ Location Area Code (LAC).

Nokia LIG solution follows the standards

The Nokia LIG solution is in accordance with the 3rd Generation Partnership Project (3GPP) and European Telecommunications Standards Institute (ETSI) standards.

Flexible configuration through Voyager or CLI

Nokia LIG provides a user friendly Voyager Graphical User Interface (GUI) for configuration. The same rule handling can be done with the Command Line Interface (CLI).

Security for traffic, stored data, LEA, AA, and Admin

Many security methods can be used. For securing data transfer all relevant security methods are supported. All internal and external interfaces can be secured with IPSec. Depending on the required capacity, additional VPN platforms can be added to support higher loads of encrypted traffic. Also SSL, SSH/SCP and LIPSec (as new) are supported. All locally stored data is encrypted using Blowfish.

Flexibility

There are many configuration options for the Admin, AA, and LEA users in both the LIB and LIC. In addition the output format for Interception-Related Information (IRI) and Communication Content (CC) can be customised according to country-specific requirements, if required.

Reliable hardware and software platforms

Nokia LIG Release 4 is delivered with the industry proven IP1260 hardware platform. A software upgrade to LIG Release 4 for IP740 hardware is also supported. Hard disk mirroring, dual power supply, cooling fans, and hot-swappable interface cards ensure high availability. The LIG uses the Nokia Ipsilon Router Operating System (IPSO) software platform, which is also used in many other network elements delivered by Nokia.

2.3 System overview of the Nokia LIG

The Nokia LIG implementation is based on distributed network architecture spanning over the operator backbone. The Nokia LIG elements consist of the Lawful Interception Controller (LIC) and the Lawful Interception Browser (LIB). The interception data is collected from the Lawful Interception Extensions (LIE), which are integrated in the packet core network elements. The LIG system components have the following functionalities:

- The LIC controls the interception sessions.
- The LIB receives and filters the intercepted data and forwards the intercepted data to the Law Enforcement Agency (LEA) users.
- The LIE functionality collects the LI data, which it provides to the LIB and LIC elements.
- The LEA activates authorised interceptions.
- The AA (Authorisation Authority) creates, maintains, and authorises interceptions to the LEA users.
- The Auditor (Audit user) audits the authorisations on a larger, for example, national level.
- The Administrator (Admin user) handles the configuration and maintenance work for the network elements

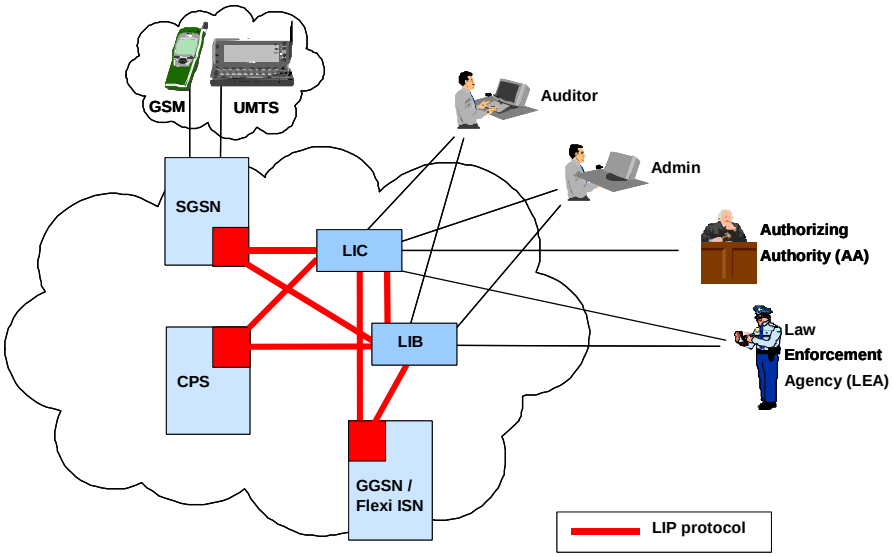

Figure 1. Nokia LIG system

2.4 Nokia LIG follows the standards

The Nokia LIG solution is in accordance with the Third Generation Partnership Project (3GPP) and European Telecommunications Standards Institute (ETSI) standards 3GPP TS 33.106, 3GPP TS 33.107, 3GPP TS 33.108, and ETSI TS 101.671. In Nokia's implementation, the Lawful Interception Controller (LIC) network element fulfils the Administration Function (ADMF), and the Lawful Interception Browser (LIB) element fulfils Delivery Functions 2 and 3 (DF2 and DF3). Refer to Figure 2 and Figure 3 below for the reference configuration used in 3GPP TS 33.107.

It should be noted, though, that there is no implementation specification for the X-interfaces. This leads to the fact that all lawful interception solutions on the market are proprietary. Thus also the Nokia LIG can be used only with Nokia packet core network elements

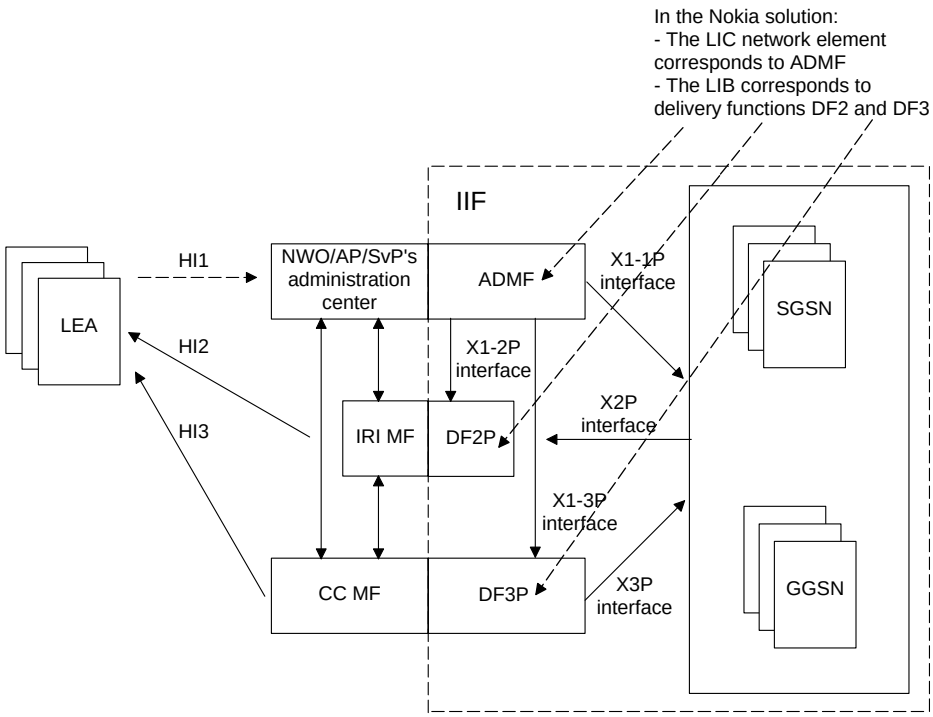

Figure 2. GPRS ETSI lawful interception network elements and their corresponding Nokia LIG elements

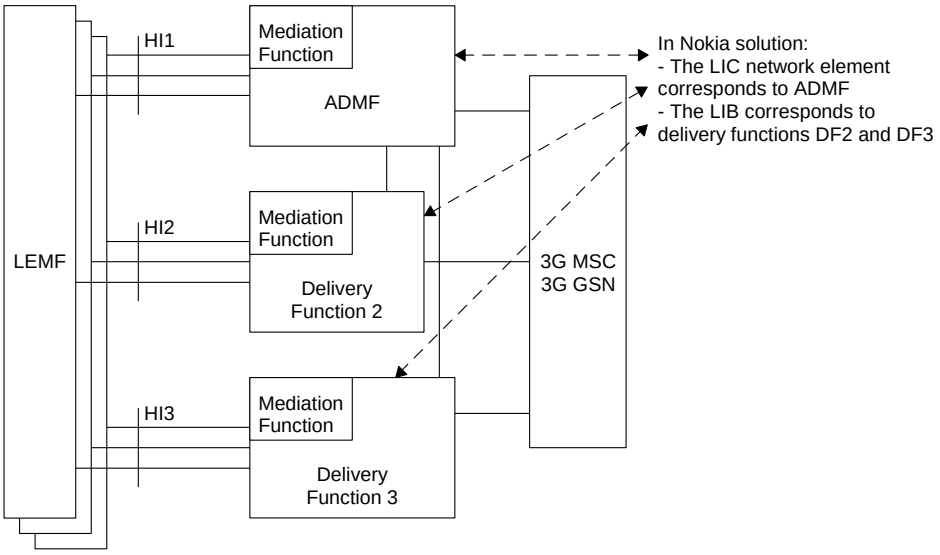

Figure 3. 3GPP MS packet switched lawful interception network elements and their corresponding Nokia LIG elements

Refer to Appendix A for the relevant 3GPP and ETSI compliance.

2.5 LIG interfaces

Nokia LIG has both external and internal interfaces. The external interfaces provide the IP-based connectivity with the Law Enforcement Agency (LEA), Authorising Authority (AA), Auditor and Admin users. Both IPv4 and IPv6 are fully supported. The internal X interfaces provide the IP connectivity within the LIG system for connecting the LIC, LIB, and LIE network elements. In addition there is the management interface for configuring and monitoring the LIC and LIB elements. All interfaces can be secured with IPSec. The web-based interfaces can be secured with SSL.

2.5.1 HI1 interface

The HI1 interface is the controlling interface that the AA and LEA users have with the LIC. This interface is implemented as a web-based interface or as a Command Line Interface (CLI), and it is used for interception requests and related information.

The advantage of CLI is the ability to unify the authorisation procedures of different systems. In other words, special customer tailored interfaces can be used with CLI and the use of an external Law Enforcement Monitoring Facility (LEMF) is possible. With CLI it is possible to create scripts for commands, which can then be easily repeated.

The CLI interface of the LIC is strictly backward compatible. The preferred CLI level can be configured in the LIC with the parameter 'CLI compatibility'. This means that it is not mandatory to upgrade existing third party LEMF software at the same time as the LIG is upgraded. The new features of each LIG release are enabled in CLI according to the selected CLI compatibility level.

2.5.2 HI2 and HI3 interfaces

The Interception-Related Information (IRI) data is sent from the LIG system to the LEA users through the HI2 interface. The uplink and downlink Communication Content (CC) data between the LEA and LIB is carried through the HI3 interface. In the Nokia LIG solution HI2 and HI3 are combined.

The LEA users can browse the IRI data through a web interface. They can also receive the IRI data together with the CC data via file transfer. File Transfer Protocol (FTP), Streaming FTP (strFTP), or Secure Shell/Secure Copy (SSH/SCP) can be used for file transfer. The UMTS LI Correlation Header (ULIC) protocol is used for transferring only the CC data, not IRI data.

2.5.3 Management interface

The management of the LIG system can take place through a web-based interface or through a Command Line Interface (CLI). The web-based management interface is used for configuring and monitoring the LIC and LIB. The LIC also sends alarms, logs, and statistics by FTP or SSH/SCP to the Admin, LEA, AA, and Auditor users through this interface. The Admin user can receive alarms also through Simple Network Management Protocol (SNMP).

CLI can be used for administrating the LIC as well. CLI supports most of the administrative commands that are performed through the web interface.

For more details on O&M refer to Chapter 6.

2.5.4 Internal interfaces

In the Nokia solution the X interfaces are used to exchange real-time internal messages between the Nokia LIC, LIB, and LIE elements. The Nokia implementation of the X-interface is based on the Nokia proprietary Lawful Interception Protocol (LIP), which is TCP-based. The LIP version used up to

date has been LIPv1, but the new LIPv2 will be supported starting with LIG Release 4. Both LIP versions can be operable simultaneously within a LIG system. For more information on the new LIPv2 support in Nokia LIG Release 4 refer to Chapter 4.1 on the support for the new distributed architecture.

2.6 Licensing

There is licence checking and functionality restriction at the LIC. The functionality restriction is based on the number of intercepting nodes and the amount of active interceptions. The LIG enables the exact number of licensed interceptions, as agreed between the authorities, the operator, and Nokia.

3 The Nokia LIG system

The architecture and users of the implementation are illustrated in Figure 4 below. It includes the following main functional components: Lawful Interception Controller (LIC), Lawful Interception Browser (LIB) and Lawful Interception Extension (LIE). The LIB and LIC operate on separate hardware platforms.

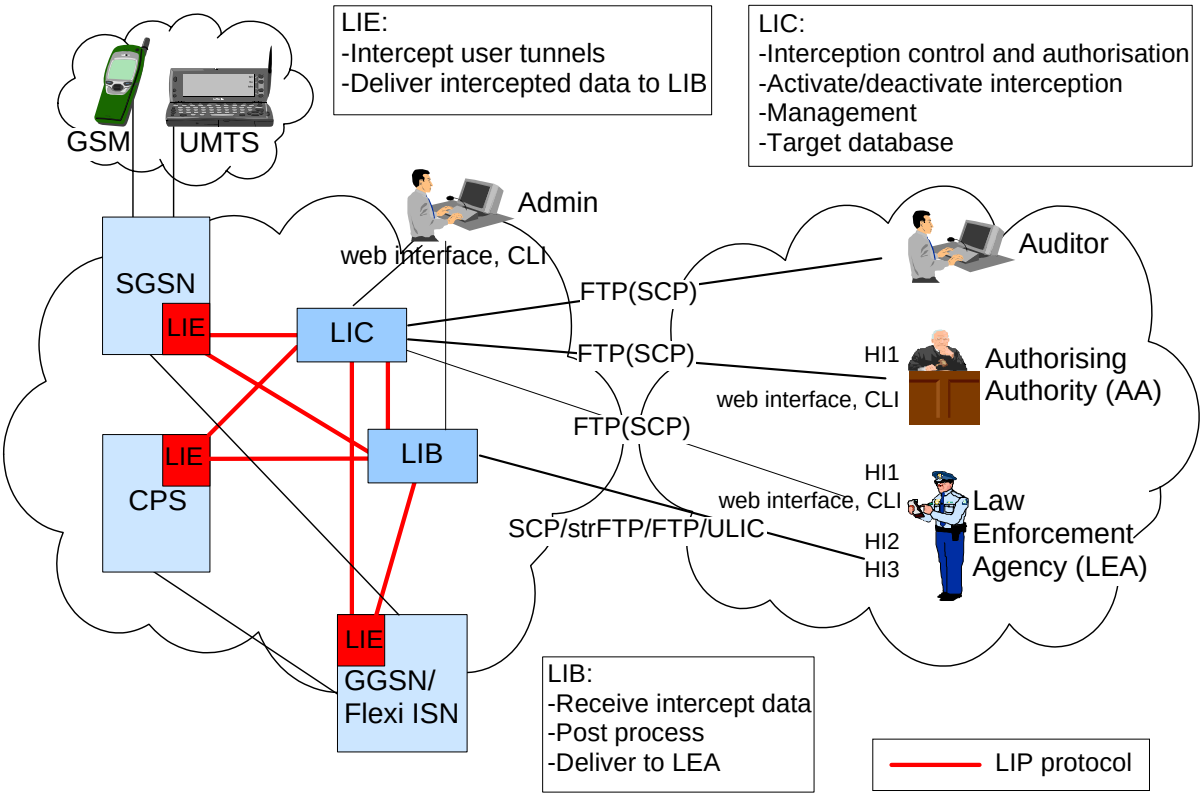

Figure 4. Main functions and interfaces of the LIG network elements

3.1 Lawful Interception Controller (LIC)

The LIC is a key element in the Nokia LIG system. The LIC runs on an IP1260 or IP740 hardware platform and it controls the interception sessions. The supported functionality is outlined below.

3.1.1 Controller within the LIG system

One or several LEA and AA users control the interception sessions through a secured web interface or the CLI interface from the LIC. The AA user grants permissions through this interface to intercept the targets. The targets are subscribers suspected of criminal activity. After the permission has been granted by the AA user, the LEA users have the authorisation to activate interceptions through the LIC. The target identifier for the interception (that is, the end user to be intercepted) can be based on International Mobile Subscriber Identity (IMSI), International Mobile Station Equipment Identity (IMEI) or Mobile Subscriber International ISDN Number (MSISDN). In Nokia LIG Release 4 also SIP URI and TEL URI can be used as subscriber identifiers for IP multimedia sessions.

The LIC sends the data collection requests to the LIE elements and it maintains the original target, user and network element databases. The LIC creates a unique request-ID for each authorisation request and each revocation or deactivation is done based on this unique request-ID. The LEA or AA can request to collect Interception-Related Information (IRI) and/or Communication Content (CC) data (both upstream and downstream). The LEA can choose where to store the interception data using file transfer configuration sets that the LEA has created. For confidentiality and security reasons the AA user has an option to set the allowed destination IP address ranges for the LEA users.

To see the role of the LIC in the Nokia LIG hierarchy, refer to Chapter 3.7 .

3.1.2 Management interface for LEA and AA users

The LIC provides a web-based interface for LEA and AA users. Several LEA and AA users are supported on the same LIC. The LIC distributes configuration parameters between the LIB and LIE within the LIG system. The LIC also manages the AA and LEA user accounts by providing access rights. To ensure security the HI1 interface between the LIC and LEA/AA is secured. To ensure confidentiality each LEA and AA user is allowed to access only their own information.

The LIC provides a lot of information to the LEA and AA users. It delivers error reports, statistical data, logs, active target lists and authorisation lists to the authorised users. The files are encrypted in case they are stored locally.

The LIC can also be operated outside the operator's backbone network (for example, in the LEA user's premises). The LIC can be accessed remotely from the Internet through a secured management interface. Optionally SSL, IPSec, or Virtual Private Network (VPN) can be used for providing a secured connection.

3.2 Lawful Interception Browser (LIB)

The LIB runs on a dedicated IP1260 or IP740 hardware platform. The LIB provides some of the main interfaces and facilities for using the LIG system. These are outlined below.

3.2.1 File transfer

The most important task for the LIB is to process the incoming intercepted data and forward it. The temporarily stored Interception-Related Information (IRI) and Communication Content (CC) are forwarded to pre-defined LEA users. The output format for the IRI and the CC is specified by 3GPP and by ETSI. If required, the IRI and CC contents can be customised according to country-specific requirements. All transfer protocols support ASN.1/BER encoding according to 3GPP TS 33.108 and optionally by ETSI TS 101.671. In addition Type-Value (TV) ASCII characters and Type-Length-Value (TLV) binary encodings are supported. All files, which are permanently stored in the LIB, are encrypted.

FTP, ULIC, SSH/SCP, or strFTP transport protocols can be used when transferring the data from the LIB. It is possible to forward the IRI and CC to different destinations. The IRI data can also be browsed remotely through the web-based LEA interface.

strFTP is a near real-time transfer method based on standard FTP. The data is forwarded to an LEA user immediately when it is ready in the LIB and the data is sent for each LEA user separately. TV, TLV, and ASN.1/BER encoded outputs are possible.

UMTS LI Correlation Header (ULIC) is a standardised transfer method for delivering the CC data to a Law Enforcement Monitoring Facility (LEMF). It is implemented according to the 3GPP TS 33.108 specification using ULIC header version 1. TCP/IP is used for transport.

In fault situations all CC data (HI3) is dropped and IRI data (HI2) is stored in the LIB.

3.2.2 Browsing

The LIB supports temporary viewing of intercepted IRI data using an SSL-secured web interface, that is, IRI browsing. This option is available for LEA users. The browse data has the same content as the data sent to the LEA user with file transfer. The browsing option is enabled separately for each interception by the AA/LEA users in the LIC. The browse data has a limited lifetime in the LIB, from 15 minutes to 1 day, as configured by the LIB admin user.

Note

IRI browsing is not intended for mass usage, and it has an effect on the system performance and the usage of system resources.

Critical events, which have been recorded in log files, can also be browsed if they have not been transferred.

3.3 Lawful Interception Extension (LIE)

The LIE functionality, which is integrated in the packet core network elements, runs on the following network elements: Nokia 2G and 3G SGSN, Nokia Flexi ISN, Nokia GGSN, and Nokia CPS (in IMS). The LIE takes care of the LI data collection of an end user. The main functionality is outlined described below.

3.3.1 Collection of interception data

Based on the command given by the LIC, the LIE sends the CC and/or IRI data to the LIB, which has been defined by the AA. The interception type (IRI/CC) can be changed on the fly during an ongoing interception session assuming the LEA has been authorised for full IRI and CC type of interception by the AA.

Collecting interception data is a process, which takes place in the ‘background’, assuring that the intercepted target (end user) is never aware of a possible interception. There is no way of finding out from the LIE of a possible interception taking place.

The collecting of LI data has no effect on the performance on the network element.

3.3.2 LIE in Nokia packet core network elements

The following Nokia elements have the LIE functionality embedded: Nokia 2G/3G SGSN, Nokia GGSN, Nokia Flexi ISN, and Nokia CPS. The LIE functionality is delivered as part of the standard functionality.

3.3.2.1 LIE in Nokia 2G SGSN

Nokia 2G SGSN contains a lawful interception extension (SGSN LIE) that collects IRI and CC interception data from roaming and non-roaming mobile targets. There is a configurable option in the LIC that defines how the 2G SGSN handles the interception of non-roaming users. For example, the SGSN can collect and transports the Communication Content (CC) for those roaming subscribers that use the GGSN of another GPRS network. It also collects SMS and location information at Cell Global Identifier (CGI) level of these mobile targets, which is part of the IRI data. It provides connections towards the LIB and LIC. The current LIPv1-based LIE implementations for all Nokia 2G SGSNs is based on the software implemented in Nokia 2G SGSN Release 2.0.

3.3.2.2 LIE in Nokia 3G SGSN

Nokia 3G SGSN contains a lawful interception extension (SMM-LIE) and a lawful interceptor (SMM-SLI) that are responsible for duplicating the data and handling external communication towards the LIC and LIB. There is a configurable option in the LIC that defines how the 3G SGSN performs the interception of non-roaming users similarly as in the 2G SGSN. The SGSN can collect and transport the CC for those roaming subscribers that use the GGSN of another GPRS or 3G networks. The current LIPv1-based LIE implementations for all Nokia 3G SGSNs is based on the software implemented in Nokia 3G SGSN Release 1.0.

3.3.2.3 LIE in Nokia GGSN and Nokia Flexi ISN

The GGSN or Flexi ISN LIE can also collect part of the intercept-related information. Normally the GGSN/Flexi ISN is responsible for collecting most of the communication content, namely the transferred user data. Also the roaming end-users are intercepted here. Together with Nokia Flexi ISN 3.0 all internal and external interfaces can optionally be secured with Internet Protocol Security (IPSec) using the IPSO platform IPSec support. The current LIPv1 based LIE implementations for all Nokia GGSNs is based on the software implemented in Nokia GGSN Release 1.3. Support for the LIPv1 LIE in Nokia Flexi ISN is starting from release 2.0 ED2.

3.3.2.4 LIE in Nokia CPS (CSCF in IMS)

LI in IP Multimedia Core Network Subsystem (IMS) consist of Session Initiation Protocol (SIP) messages and some extra information carried along the messages. SIP interceptions are activated in the Nokia CPS network element. The CPS (CSCF) handles only signalling data therefore SIP interception

product is always IRI data. The CPS LIE delivers the IRI data to the LIB network element.

The CC interception of an IMS user is performed in a separate GPRS interception. When Nokia packet core is the access network used for IMS (and the Go interface is in use between the networks), the interception may be automatically activated in the GPRS.

The LIE in the CPS node is based on software from IMM2 Release 2.0 or later. The LIE is included in the CPS product and cannot be ordered separately. The CPS LIE collects the IRI, which can be associated to the CC interception data of roaming and non-roaming mobile targets collected from the GGSN or SGSN. It provides IP connections to the LIB and LIC. The LIE implementation for the CPS is LIPv2-based.

3.4 User groups in the Nokia LIG system

There are four different user groups in the Nokia LIG system:

- LEA (Law Enforcement Agency)
- AA (Authorisation Authority)
- Auditor (Audit user)
- Administrator (Admin user)

The LEA is the authority that gets the intercepted data, which is then used in the criminal investigations. The LEA's role is activating and managing the authorised interceptions. The LEA user can alter the interception parameters only within the limits set by the AA user, and the LEA is not allowed to exceed the given limits. Normally the police act as the LEA user.

The authorisation for practising Lawful Interception (LI) is granted by the AA. The authorisation to perform LI is given only to the LEA and the AA has no access to the intercepted data. The AA user also sets a list of parameters for each LI authorisation, which includes:

- target of the LI (for example, IMSI)
- LIB
- validity time for the LI
- interception area
- interception type (either CC or IRI or both)
- interception options (browse, file transfer, or both)

The AA has the power also to revoke the authorisation for an ongoing LI at anytime. Normally a judge from a court of law acts as the AA user.

The Auditor audits the authorisations on a high level, for example, on a national level. The Audit user sees the authorisations, but does not have access to the LIG system. The Audit user has no access to the LI data either. Normally a high-level judicial authority or a high-level government official acts as an Audit user. There is one Auditor for each LIG system.

The Administrator handles the configuration and maintenance work for the network elements and creates the AA users. The Admin user is not involved in the LI activities interceptions at all and is normally a representative of the network operator.

The reason for having such a large number of user groups is to have flexibility when adapting to different country-specific legislation needs. In practice one user can be an authorised representative for several or even all the user groups.

3.5 Redundancy

The hardware platforms (IP740 and IP1260) support hard disk mirroring (RAID level 1). Backup and restore functionality for both LIC and LIB network element databases enables periodical backups for restoring a malfunctioning network element. After restoration the LIG system will fully operational in exactly the same way as before the backup. This will include the information of all the active ongoing interceptions at the time the backup started.

The redundancy of the LIB, LIE, and LEA traffic is implemented in the form of optional duplicated interception sessions and on separate LIB hardware.

3.6 Capacity figures

Nokia Lawful Interception Controller (LIC) and Lawful Interception Browser (LIB) are compact Nokia units with minimal configuration required.

1000 - 5000 active interception sessions can be performed simultaneously for each LIB unit, depending on the file transfer protocol used. The total number of interception sessions for each LIC is 50 000.

The maximum figures for dimensioning are listed in the table below.

Table 1. Nokia LIG Release 4 maximum values for IP740 and IP1260 (with 2GB RAM installed)

Feature	Maximum value

Feature	Maximum value
LIC	
Total number of interceptions	50 000
Maximum number of simultaneous LIP connections	2048
LIB	
Peak input capacity	50 Mbps
Maximum number of simultaneous interceptions • FTP, SSH/SCP, ULIC • Browsing only	1000
Maximum number of simultaneous interceptions • strFTP	4000
Max number of simultaneous interceptions	5000 (1000+4000)
Maximum number of simultaneous file transfer configurations (FTC's)	2000
Maximum number of simultaneous LEA users using streaming FTP (strFTP)	50
Maximum number of simultaneous LIP connections	2048
Supported number of simultaneous interceptions using browsing	1000
Supported number of simultaneous browse files in LIB	10 000
LIE	
Recommended maximum number of LIEs	50
Simultaneous Law Enforcement Agency (LEA) interceptions for the same target	10
Active PDP context interception sessions for each GGSN (GGN5)	2500
Active PDP context interception sessions for each Flexi ISN	1% of max PDP context licence
Active interception sessions for each 2G SGSN (SG5)	6400
Active interception sessions for each 3G SGSN (SGN3)	5000
Number of simultaneous interceptions collecting data in CPS	2300 *)

Feature	Maximum value
Number of intercepted targets in CPS database	100 000

*) tentative figure

3.7 Hierarchy in the Nokia LIG system

The Nokia LIG system has a hierarchical structure. There can be several independent LIG systems within one operator network, but in most cases only one is needed (one LIG system consists of one LIC and one or several LIB elements). All interceptions, users, and other definitions are LIG system - specific.

In the Nokia LIG system each LIC can control a number of LIB elements. The LI traffic volumes and number of simultaneous sessions determine the number of LIB elements needed (refer to the previous chapter on capacity figures). In many cases one or two LIB elements are sufficient.

If there is more than one LIC element, each LIB element can have one, and only one, controlling LIC element. Packet core LIE elements on the other hand can be connected to a number of LIC and LIB elements.

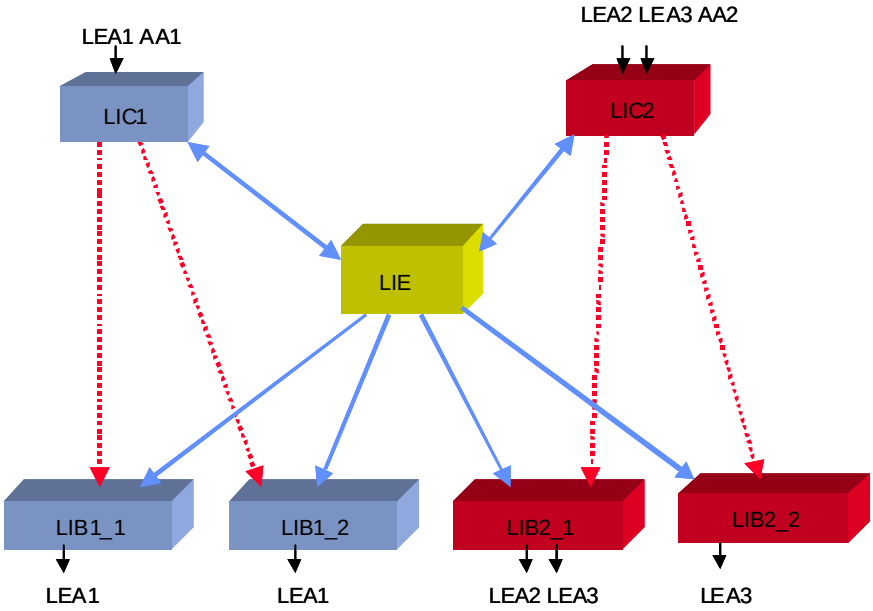

Figure 5. Hierarchy of network elements in the Nokia LIG system

4 New software functionality in LIG Release 4

Nokia LIG Release 4 provides many new functionalities and enhancements for both the platform and application software. On the platform side IPSec and IPv6 have now full support. On the application side there are the following new functionalities:

- new distributed database architecture (support for ‘Tornado Phase’)
- interception for IMS end users (in CPS)
- support for Nokia Flexi ISN
- improved user practice by LAAP (LIG Aided Authorisation Practice)
- operability enhancements in SNMP admin alarms, web interface usability improvements, and CLI Admin commands
- enhancements in location dependent interception (with new parameters)
- QoS parameters in IRI events (requires LIPv2)
- application-level security: LIPSec
- interception of end users with MultiSIM
- ASN.1 notifications for proprietary IRI events
- LIG volume control licence (based on the amount of intercepting nodes and active interceptions)
- enhancements in LIB

Some of the main functionalities are described in more detail in the following chapters.

4.1 Distributed architecture

The ‘Tornado Phase’ architecture is based on distributed database architecture, where the databases are distributed throughout the LIG system, including packet core network elements. The major benefit of this new architecture compared to the earlier centralised architecture is that now the database information is always there where it is needed. This significantly reduces the signalling need between the LIG system and the packet core. The reduced signalling load enables the deployment of large networks with large data volumes. A new lawful interception protocol (LIPv2) has been introduced to support the new distributed architecture.

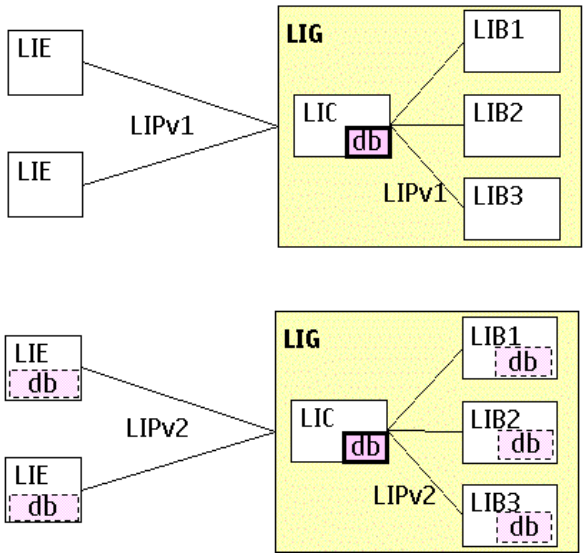

Figure 6. Centralised (above) and distributed (below) architectures

The main advantages of the distributed architecture are:

- reliable handling of interception data ensured in congested operator networks
- significantly less control traffic (1/100)
- fast network element start-up as there is no need to reactivate all the interceptions
- no gaps in interception start
- LIG scalable according to the number of PDP contexts
- LIPv2 provides many protocol-related enhancements, such as new HI2-HI3 parameters

The Nokia LIG system supports the simultaneous use of LIPv1 and LIPv2. The version to be used depends on the support in the LIE.

4.2 Interception of IMS end users

IP multimedia services offer real-time SIP services delivered over the packet switched network. The ability to intercept the signalling of IP multimedia services is a mandatory requirement. The signalling data consists of SIP signalling messages and some extra information carried along the messages. The outcome of IMS end user interception is always IRI data.

Local authorities may require intercepting the user data of the IP multimedia sessions as well. The CC of an IMS user can be intercepted in the GPRS packet switched domain, if required. With the full Nokia packet core and Nokia IMS solution, the interception of packet switched CC is done automatically (this requires the Go interface between the networks).

The new target identifiers for IMS interception are SIP URI and TEL URI.

The IMS interceptions are activated by the LIC, similarly as in a normal GPRS interception. The CPS LIE delivers the IRI data to LIB network element. The Call Processing Server (CPS) is the Nokia equivalent for the P-CSCF and S-CSCF functionality of the IMS.

Interception at PoC is not supported in this LIG release.

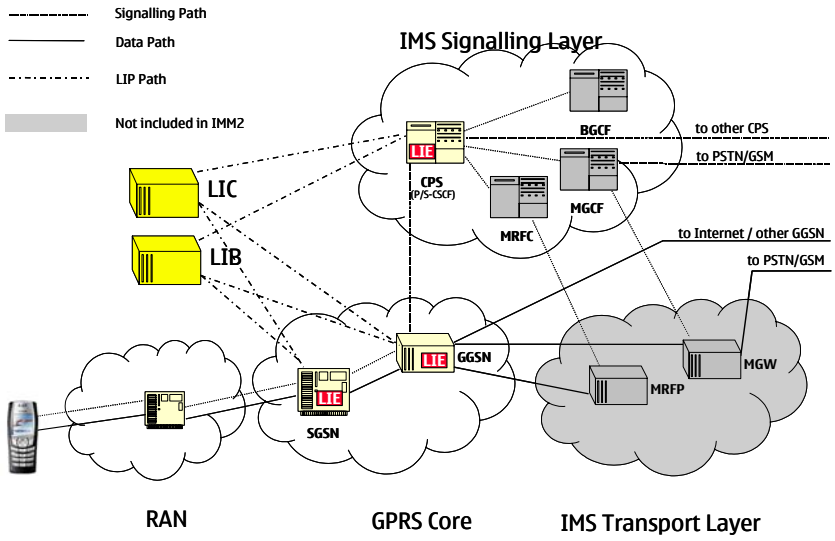

Figure 7. Lawful interception support for IP multimedia core

4.3 Improved user practices and operability enhancements

User practices have been significantly improved with LIG Aided Authorisation Practice (LAAP). LAAP makes the authorisation of interception requests quicker, smoother, and more secure by offering electronic processes through the LIG web interface. The earlier authorisation procedure (which was based, for example, on the use of faxes) can now be replaced by using the LIG. The users involved are AA users (typically local court) and LEA users (typically local police). The use of LAAP is optional.

Sending LIG admin alarms to the Nokia NetAct system is now also possible through SNMP. All alarms are sent through the Nokia enhanced NE3S interface, which also supports the IPSO platform alarms.

The HI1 notifications can be ASN.1/BER encoded for proprietary IRI events (as defined in ETSI TS 101 671 v2.12.1).

Usability of the Voyager web-based interface has been improved according to a usability study based on the feedback given from existing LIG users. Especially usability focusing on error prevention has been improved.

Using the Command Line Interface (CLI) for admin commands is now also possible.

4.4 Enhanced location dependent interception

In Location Dependent Interception (LDI), the interception takes place only when the target is inside a pre-defined Interception Area (IA). In other words, interception is not performed if the target is not located in the IA. So far the IA has been restricted to national level, and the IA has been defined as a set of cells identified by RAI, CGI, and SAI.

In LIG Release 4 the IA has been extended to allow country and network-specific LI. The following new parameters have been added to specify the interception area:

- MCC (Mobile Country Code)
- MCC+MNC (Mobile Network Code)
- MCC+MNC+LAC (Location Area Code)

The authorisation to use an IA is given by the AA user and the Admin user will define the codes defined above. The IA location check will take place every time a MS is attached, every time a cell is updated, or when a location dependent interception is activated.

4.5 Interception of end users with MultiSIM

Interception of MultiSIM targets is now possible. The MultiSIM service allows a single subscriber to use several physical mobile phones (for example, one at work and one at home) with the same phone number (MSISDN) by having several IMSIs. A MultiSIM subscriber is a subscriber who is using the MultiSIM service. Full MultiSIM interception support requires LIPv2 support in the LIE.

4.6 Enhancements in LIB

The following enhancements have been implemented to the LIB:

- file naming B for FTP/SCP as defined in 3GPP 33.108
- zero file browsing and IRI browsing for strFTP
- all interception modifications allowed without deactivating the interception
- increase in overall performance
- zero file creation logic

5 Hardware and software platforms

Most of the transactions in the LIG require real-time traffic handling. Real-time handling of subscriber IP traffic and interactive user transactions, not to mention also the interaction with the other network elements, set high performance and availability criteria. To guarantee fast, reliable, and uninterrupted traffic handling, the industry proven Nokia IP Platform hardware and Nokia IPSO operating system have been selected as the hardware and software platforms.

5.1 Software platform

The Nokia LIG Release 4 application runs on IPSO 3.8 NET, which runs on top of the IP1260/IP740 series hardware. The IPSO 3.8 NET software platform supports the following new features:

- unlimited memory allocation
- Jumbo frames support in Gigabit Ethernet
- IP input scheduling (traffic prioritisation with input queues)
- IPv6 management MIB
- COPS/PIB support for IPSec, including IPv6
- new Key Performance Indicators (KPI) for peak interface capacity, CPU utilisation, and QoS

5.2 Supported hardware platforms

Nokia LIG Release 4 is delivered on the Nokia IP1260 hardware platform. This is a new hardware platform for Nokia LIG Release 4, but is used already extensively by the Nokia GGSN and TA applications. Both RoHS compliant and non-RoHS compliant versions of IP1260 hardware are supported by LIG. Upgrading the LIG Release 4 software on the IP740 hardware is also possible.

The supported hardware platforms are equipped with two hard disks, four onboard Ethernet interfaces and several slots for additional high-speed interfaces.

Note that the RoHS compliant IPSec hardware accelerator card (Viper4) is currently not supported by IPSO 3.8NET. Support is planned for forthcoming software releases. Meanwhile, software-based IPSec acceleration or a non-RoHS compliant hardware accelerator card (Viper3) has to be used.

The design of Nokia LIG makes field service and maintenance user-friendly. All interface cards are accessible from the front without opening the housing. The unit can be mounted in a 19" rack, or it can be stacked.

Both the LIC and the LIB are operated on separate hardware platforms.

Nokia LIG Release 4 does not include support for the earlier IP650 series hardware.

5.2.1 IP1260 hardware

Figure 8. Nokia LIB and LIC based on IP1260 hardware

The Nokia LIG based on the IP1260 has dual power supplies and cooling fans. The Dual 6U PMC Expansion Carriers are hot swappable.

The hard disk drives are used in a mirrored mode. If one drive fails, the other one continues the operation without loss of data. If a new disk is inserted while the system is operating, the system automatically prepares the disk image and builds a mirrored copy of the first disk.

The Nokia LIG complies with the European Union RoHS Directive 2002/95/EC on the restriction of the use of certain hazardous substances in electrical and electronic equipment. The directive applies to the use of lead, mercury,

cadmium, hexavalent chromium, polybrominated biphenyls (PBB), and polybrominated diphenyl ethers (PBDE) in electrical and electronic equipment put on the market after 1 July 2006.

5.2.2 IP740 hardware

The IP740 hardware is not delivered with the new LIG Release 4 software. The IP740 hardware is supported for backward compatibility reasons. Before a LIG 4 upgrade the IPSO platform software must be upgraded to IPSO 3.8.NET. For further details refer to *LIG Release 4 Product Documentation: Installation Guide.*

5.3 Physical interfaces

The Nokia IP1260 hardware can be equipped with PMC network interface cards, which are housed in 6U dual PMC carrier expansion slots. The carriers are hot swappable, which makes it possible to change a failed network card without any interruption to the rest of the system. IP1260 has a total of four PMC slots, four built-in 10/100 Ethernet ports, two serial ports, and two PCMCIA slots (see Figure 9 below).

The Nokia IP1260 hardware supports the following physical network interface cards:

- Four-port 10/100Base-T, RJ 45 Ethernet PMC interface card (10/100 Mbps)
- Dual-port Fibre-optic 1000Base-SX Gigabit Ethernet PMC interface card (MMF, 1000 Mbps)
- Dual-port Copper Gigabit Ethernet 1000Base-T, RJ-45 PMC interface card (10/100/1000 Mbps)

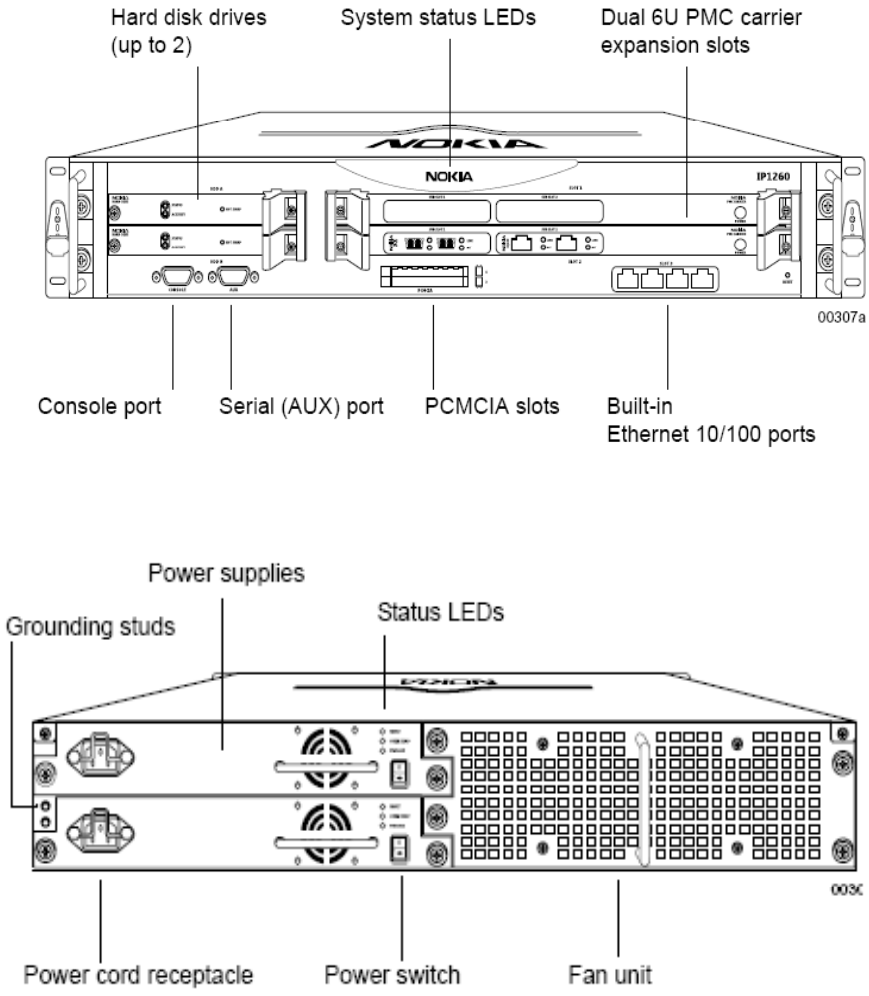

Figure 9. General sample picture of LIB/LIC component locations (subject to changes)

6 Operation & Management

The Nokia LIG system is equipped with several different network management interface options to fulfil the numerous requirements in the network management area. The following management interfaces and protocols are supported:

- Voyager web interface for configuration and administration of the LIC
- Simple Network Management Protocol (SNMP & NE3S) for collecting alarms and performance indicators for both the platform and application
- Command Line Interface (CLI) over Telnet for connecting the Law Enforcement Monitoring Facility (LEMF) to the LIC
- Network Time Protocol (NTP) for synchronising the LIG internal clock
- File Transfer Protocol (FTP) for software image download, configuration data backup and restore functions
- SSH/Telnet for configuration and maintenance operations

Access to the LIG is controlled through user names and passwords. Access control is protected through encrypted communication using Secure Shell (SSH) or Secure Sockets Layer (SSL) technology and supports one-time passwords using S/Key.

Network access to the LIG can be allowed or restricted for FTP (includes definition of a separate FTP port), Telnet, admin login, and com port login. The Voyager web access can be turned on or off, and defined for a separate port.

6.1 Application management for Nokia LIG

Most of the application management of Nokia LIG takes place through the LIC. The LIC collects, for example, fault information from the LIE, LIB, LEA, and AA. The main management tool for Nokia LIG is the web-based Nokia Voyager. It is delivered as preinstalled. Voyager provides an extensive set of configuration parameters and element monitoring features.

The Nokia Voyager management tool provides a Graphical User Interface (GUI) for configuration, monitoring and control. It can be used remotely over a secured SSL connection. Nokia Voyager can be accessed by a web browser and can thus be run basically on any host.

The web interface also provides access to the LIG online documentation and includes an online help feature for additional information on each administrative task. Voyager can be accesses through the Network Management System (NetAct).

6.1.1 Configuration of LIG

Configuring the LIG can be done through the Voyager web access and Telnet access. The Voyager web interface is used by the Administrator, the AA, and the LEA users. In Telnet access CLI is normally used. For more details on LIG configuration refer to *LIG Release 4 Product Documentation: Reference guide* and *CLI User's Guide*.

6.1.2 Logs for statistics and alarms

The LIG collects both the statistics and logs of the LIG network. The information is stored and then transferred to LIG users, which include:

- Administrator (Admin)
- LEA
- AA

The statistics are collected in a file, which is transferred through FTP or SCP periodically to the LEA, AA, or Admin. The statistics can be collected based on traffic or interception type, or as a total statistics collection. Statistics can be collected on:

- Traffic statistics
- Interception statistics

The Admin user can configure the statistics collection through the web interface (Voyager). The Admin, AA, and LEA users also use the Lawful Interception Controller (LIC) web interface to browse the statistics.

The figure below shows the position of statistics in the LIG system. The statistics from the LIBs are transferred to the LIC using the internal interface.

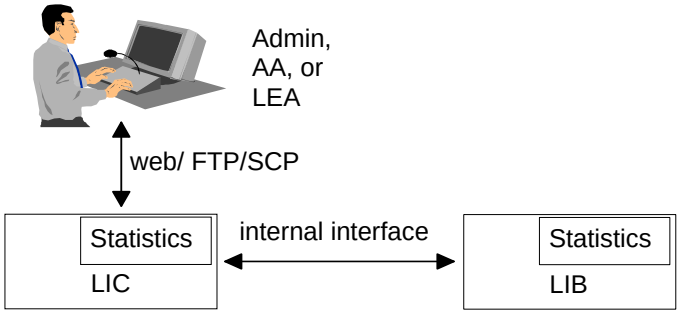

Figure 10. Statistics position in the LIG system

Statistics are stored in non-volatile memory, thereby protecting them from being lost in an unexpected power shutdown. The LIC generates a history log for each log file. Cleanup and transfer actions are recorded in the history log. Log files can be transferred to their owners. When the log is cleared it can also be sent to the owner of the log file. Each user can define the transfer destination for their files. The Admin user can also disable the log file transfer of each user type.

The web interface of the LIC can be used to configure the statistics collection. Admin, AA, and LEA users may browse their statistics using the web interface.

6.2 IPSO platform management

The IPSO platform provides the means for monitoring, configuration and indication of alarms. The IPSO platform is capable of sending SNMP traps (Fault Management) in fundamental situations such as starting and linking up/down. Configuration can be done also through the Command Line Interface (CLI). IPSO provides the means for performing configurations based on trial and error. Returning safely to previously saved configuration sets is always possible. IPSO monitoring is also supported.

The IPSO platform includes an optional Network Management System (NMS) interface, which is used for polling the LIC and LIB hardware. Nokia NetAct is part of the core network management system and it can provide system level control, like clock synchronisation of the LIC and LIB by using Network Time Protocol (NTP). All hardware alarms generated by the IPSO platform can be delivered as LIG alarms.

6.3 Software and hardware upgrading to LIG Release 4

The LIG Release 4 software (separate software and hardware for both LIB and LIC) can be installed on two hardware platforms:

- IP1260
- IP740

The hardware platform for both the LIB and LIC require at least 2GB of RAM.

All features are compliant with the Release 4 software provided that all the announced hardware and platform software (IPSO) upgrades have been implemented. Nokia LIG Release 4 runs on top of IPSO 3.8 NET.

The upgrade procedure from release 3 to release 4 is further documented in *Upgrade instructions for LIG from Release 3 to Release 4*.

Note that the LIC and the LIB must always be from the same release.

Appendix A: LIG 4 data sheet

Table 2. Compliance

Compliance	
3GPP Base Line	3GPP Rel 6
Technical requirements. Stage 1	3GPP TS 33.106 v6.1.0
3G Security; Lawful Interception Architecture and Functions, (Release 6)	3GPP TS 33.107 v6.5.0
3G Security; Handover Interface for Lawful Interception (Release 6)	3GPP TS 33.108 v6.9.0 (for HI2 and HI3 descriptions)
ETSI	
Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic	ETSI TS 101.671 v2.12.1 (for HI1 descriptions)

Table 3. IP1260 dimensions

Dimensions IP1260	
Height	8.89 cm / 3.46 in. (2U)
Depth:	52.34 cm / 21 in.
Width	44 cm / 17 in. or 48 cm / 19 in. (rack mountable)
Weight	16 kg / 36 lbs
Power IP1260	
	85-139/170-264 VAC auto-ranging
	47 – 63 Hz
	360 W max.

Table 4. IP1260 environment

Temperature and altitude IP1260	
Operating: -5 ºC to +40 ºC / +23 ºF to +104 ºF	up to 3 000 m / 10 000 ft
Short Term Operational Temperature (less than 96 consecutive hours): - 5 ºC to +50 ºC / +23 ºF to +122 ºF	up to 3 000 m / 10 000 ft
Storage: - 40 ºC to +70 ºC /- 40 ºF to +160 ºF	up to 9 000 m / 30 000 ft
Relative humidity	
Operating	10 – 90 % non-condensing
Storage	5 – 95 % non-condensing
Electromagnetic Compatibility (EMC)	
CE Mark	
FCC Part 15, Subpart B Class A	
EN55022 (CISPR22, Class A)	
Safety	
UL60950	
CE Mark	
Can/CSA-C22.2 NO 950	
IEC950	
TUV EN60950	

Appendix B: Nokia LIG Release 4 reliability

Nokia Lawful Interception Controller (LIC) and Lawful Interception Browser (LIB) units have redundant, hot swappable power supplies and mirroring hard disks (RAID level 1).

Table 5. IP1260 hardware reliability

Mean Time Between Failures (MTBF)	
at 25 degrees Celsius	40,752 hours
at 40 degrees Celsius	29,915 hours
Mean Time To Recovery (MTTR)	20 minutes by direct replacement (first line repair)

References

1. Nokia IP1200 Series Security Platform Installation Guide
2. Nokia IP700 Series Installation Guide
3. CRP and line cards configuration in Voyager for IPSO 3.8NET
4. Fault management in Voyager for IPSO 3.8NET
5. Interfaces configuration in Voyager for IPSO 3.8NET
6. IPv6 configuration in Voyager for IPSO 3.8NET
7. System resources monitoring in Voyager for IPSO 3.8NET
8. Router services configuration in Voyager for IPSO 3.8NET
9. Routing configuration in Voyager for IPSO 3.8NET
10. Security and access configuration in Voyager for IPSO 3.8NET
11. SNMP configuration and asset management summary in Voyager for IPSO 3.8NET
12. Traffic management in Voyager for IPSO 3.8NET
13. System functions configuration in Voyager for IPSO 3.8NET
14. Nokia LIG Release 4 Product Documentation: Installation Guide
15. Nokia LIG Release 4 Product Documentation: CLI User’s Guide
16. Nokia LIG Release 4 Product Documentation: Auditor’s Guide
17. Nokia LIG Release 4 Product Documentation: LEA Interface Guide
18. Nokia LIG Release 4 Product Documentation: LeaViewer Guide
19. Nokia LIG Release 4 Product Documentation: Reference Guide
20. Upgrade instructions for LIG from Release 3 to Release 4
21. 3GPP TS 33.106 v6.1.0 (2004-06). See the respective SoC.
22. 3GPP TS 33.107 v6.5.0 (2005-06). See the respective SoC.
23. 3GPP TS 33.108 v6.9.0 (2005-06) and 3GPP TS 33.108v6.8.2 (2005-01). See the respective SoC.
24. ETSI TS 101 671 v2.12.1 (2005-08). See LIG3 SoC.

Glossary

3GPP	Third Generation Partnership Project
3GPP MS	Third Generation Mobile Communication System
AA	Authorising Authority
admin	Administrator user Account
ADMF	Administration Function
ASN.1	Abstract Syntax Notation One
BER	Basic Encoding Rules
BGCF	Breakout Gateway Control Function
CC	Content of Communication
CLI	Command Line Interface
CGI	Cell Global Identification
CPS	Connection Processing Server
CSCF	Call State Control Function
DF	Delivery Function
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HI	Handover Interface
HI1	Interface between the LIC and the AA and LEA for interception requests and related information (formerly X0_1)
HI2	Interface for IRI data between the LIB and LEA (formerly X0_2)
HI3	Interface for CC data between the LIB and LEA (formerly X0_3)
IA	Interception Area
IMEI	International Mobile Station Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPSec	IP Protocol Security
IRI	Interception-Related Information
ISDN	Integrated Services Digital Network

ISN	Intelligent Service Node
LAAP	LIG Aided Authorisation Practice
LAC	Location Area Code
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIB	Lawful Interception Browser
LIC	Lawful Interception Controller
LIE	Lawful Interception Extension
LIG	Lawful Interception Gateway
MCC	Mobile Country Code
MGCF	Media Gateway Control Function
MGW	Multimedia Gateway
MIB	Management Information Base
MNC	Mobile Network Code
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
MSISDN	Mobile Subscriber International ISDN Number
NE3S	Nokia Enhanced SNMP Solution Suite
NMS	Network Management System
NTP	Network Time Protocol
PMC	PCI (Peripheral Component Interconnect) Mezzanine Card
PCMCIA	Personal Computer Memory Card International Association
PDP	Packet Data Protocol
QoS	Quality of Service
RA	Routing Area
RAN	Radio Access Network
RAI	Routing Area Identity
RoHS	Restriction on the use of certain Hazardous Substances
SAI	Service Area Identifier
SCP	Secure Copy
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module

SIP URI	Session Initiation Protocol Universal Resource Identifier aka SIP URL
SIP URL	Session Initiation Protocol Universal Resource Locator aka SIP URI
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transport Control Protocol
TDMA	Time Division Multiple Access
TEL URI	Telephone Universal Resource Identifier aka TEL URL
TEL URL	Telephone Universal Resource Locator aka TEL URI
ULIC	UMTS LI Correlation Header
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
WCDMA	Wideband Code Division Multiple Access