NOKIA

Nokia Lawful Interception Gateway (LIG) Release 1 Product Description

Introductory Document

Contents

1 Introduction

This document gives an overview of the Nokia Lawful Interception Gateway (LIG) Release 1 for GPRS describing the functionality, architecture, interfaces, capacity, operating environment and documentation of the product.

2 Description of the Nokia LIG

The Lawful Interception Gateway (LIG) is an essential network functionality within the General Packet Radio Service (GPRS) infrastructure, providing the authorities with the ability to intercept GPRS mobile data calls. This new method of interception for the GPRS network is completely different from the GSM call interception. In GSM, interception is mainly voice-based audio recording, and in GPRS, the data is intercepted between the Mobile Station and the Access Point.

Operators in most countries, among them all EU member countries, need to fulfil their local authority requirements before the commercial launch of a GPRS network.

The Nokia LIG is a scalable system based on the same proven industry standard platform as the Gateway GPRS Support Node (GGSN) and offering an ideal solution for building the GPRS interception system.

In Nokia's implementation, the Lawful Interception Controller (LIC) network element corresponds to the ADMF (Administration Function) and the Lawful Interception Browser (LIB) element corresponds to the delivery functions DF2 and DF3 of the ETSI standard.

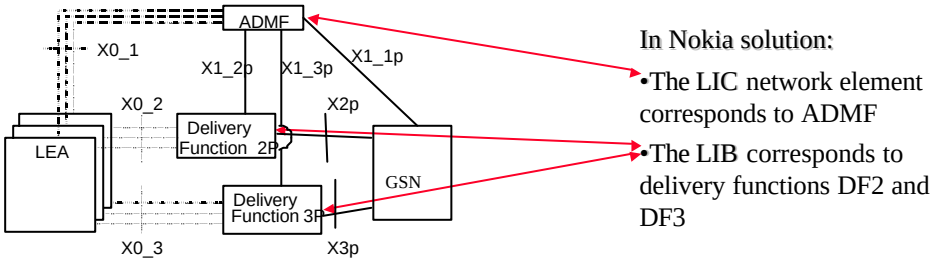

Figure 1. ETSI network elements and their correspondecies in Nokia LIG

The architecture of the implementation is illustrated in Figure 2. It includes the following main components and functionalities:

- The **Lawful Interception Controller** (LIC) is based on the Nokia/IPRG IP650 router product. This network element controls the interception and contains a secured Web interface for one or more Lawful Enforcement Agencies (LEAs) and the Authorisation Authorities (AA). The AA gives permission through this interface (depending on the country-specific practices) to intercept subscribers. A LEA activates and deactivates interceptions through this interface by using International Mobile Subscriber Identity (IMSI) or Mobile Station ISDN Number (MSISDN) as target identifiers. In further releases also the International Mobile station Equipment Identity (IMEI) identifier can be used.
- The **Lawful Interception Browser** (LIB) is also based on the Nokia/IPRG IP650 router product. This network element temporarily stores the Interception-Related Information (IRI) and Communication Content (CC) which are sent as such to the defined LEA(s). The data is transferred by FTP and it can be secured with Secure Shell (SSH). The IRI data can be browsed remotely through the Web based LEA interface.
- The **Lawful Interception Extension** (LIE) in the GGSN node is based on the GGSN Release 1.1 software. It collects part of the IRI and is responsible for collecting the communication content, namely the user (mobile) data transferred.

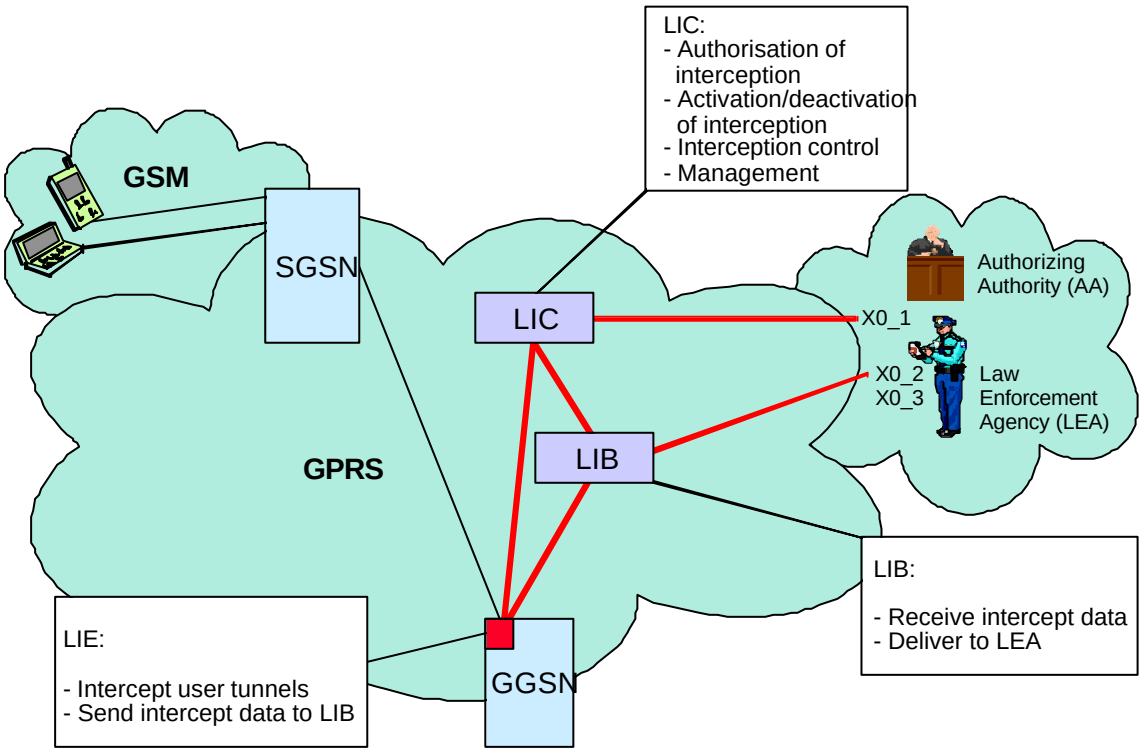

Figure 2. Network elements and their main functions in LIG Release 1

The main features of the Nokia LIG functional components are presented below.

LIC

Management of LEA and AA users' user rights

- Web-based LEA and AA interfaces
- One LEA or AA uses only one LIC
- The possibility of several LEAs and AAs using the same LIC
- Distribution of configuration parameters related to the basic data collection of the LEA to other network elements
- Distribution of configuration parameters related to the data delivery of the LEA to other network elements
- Adding and deleting AAs and LEAs
- Handling of AAs' or LEAs' encryption keys
- Authentication of the AAs or the LEAs by password
- Authorisation of AAs and LEAs

Services for LEA and AA

- Delivery of error reports to the AA and the LEA
- Delivery of active target list to the LEA on request
- Delivery of authorisation list to the AA
- Authorisation/activation of interception by the AA/LIC on request when the IMSI is used as a target identifier
- Authorisation/activation of interception by the AA/LIC on request when the MSISDN is used as a target identifier
- Deauthorisation/deactivation of interception by the AA/LIC on request using a request identifier given in activation
- Request of data collection for Interception-Related Information (IRI), Communication Content (CC) or for IRI and CC

Co-operation between network elements

- Sending data collection activation/deactivation requests to the GGSN by IMSI
- Sending data delivery activation/deactivation information to the LIB
- Receiving tunnel start notification from the GGSN. If the target is intercepted, the LIC sends data collection activation request back and requests for data delivery activation from the LIB
- Receiving tunnel end notification from the GGSN. If the target is intercepted the LIC deactivates the data delivery.

LIC management

- Web-based management interface
- Maintaining a target database of the currently intercepted targets
- Generating a unique request identifier for each intercept activation request
- Collecting a target log about interception activations for LEA
- Collecting an interception log about interception authorisations for AA
- Browsing of AA log items for centralised auditing
- Collecting an error log for debugging and recovery
- Sending notifications by file transfer
- Sending notifications about the error situations of the LIC
- Forwarding notifications sent by the LIB
- Forwarding notifications sent by the GGSN LIE
- Distributing the needed configuration parameters to all GSNs
- Distributing the needed configuration parameters to LIBs

Security

- LIC remote management interface uses Secure Webserver based on Apache and SSLeay/OpenSSL (SSL) secured Web
- LIC allows each LEA and AA to access only to its own information
- The LIC – LEA/AA interface uses SSL secured Web
- Enhancement of security in LIC by applying the optional firewall feature of the IP650 router

Time management

- LIC updates time using NTP

LIB:

External (public) interfaces

- Providing X0_2 and X0_3 interfaces to the LEA using a Web interface and file transfer initiated by the LIB
- Providing an interface to GGSN
- Providing an interface to LIC
- Providing a Web based user interface for an administrator
- Supporting multiple physical interfaces towards LEA
- Protection of the physical interfaces of the LIB against unauthorised use

Packet receiving/transmitting & processing facilities

- Processing incoming intercept data and storing or forwarding it
- High "store and forward" performance
- No interference between different LEAs
- The intercepted target cannot detect the ongoing interception

Browsing facility

- The availability of the browsable IRI data after delay
- Prevention of LIB users from seeing each other's targets and data
- Web-based IRI data target selection and viewing

Management facility

- Web based management
- Authentication and authorisation based on usernames and passwords

Fault management facility

- Storage of X0_2 data (IRI) at failure
- Dropping X0_3 data (CC) at failure
- Initiating failure reports to System Administrator, LEA and AA

Data storage facility

- Logging critical events to log files
- Log files are browsable

Other features

- Possibility to synchronise the real time clock via NTP

LIE:

Performance and Capacity

- Such high performance that target cannot detect interception
- Delivery of the intercept data to the LIB in real time speed
- Real time notification by the GGSN to the LIC when the PDP context is created
- Possibility to intercept several PDP contexts simultaneously

Intercept Data Collection

- Possibility to activate the PDP context for interception during PDP context activation
- Possibility to activate the PDP context for interception when PDP context is active
- Possibility to deactivate interception for a PDP context

- Possibilty for several LEAs to intercept the same PDP context simultaneously
- Provision of Intercept Related Information from PDP Context Activation/Deactivation/Update events by the GGSN
- Collection of Communication content for an intercepted PDP context by the GGSN

External Interfaces

- Provision of connection to the LIC by the GGSN
- Provision of connection to the LIB by the GGSN

Security

- No access for outsiders to the intercept data
- No access for outsiders to the intercept targets because target information is stored only in volatile memory

Configuration management

- Possibility to configure initial LIBs via LIC

Fault management

- The GGSN can send failure notifications to the System Administrator
- The GGSN can send lawful interception specific alarms to the NMS

3 The architecture of the Nokia LIG

The architecture of the Nokia LIG hardware is based on two Nokia/IPRG IP650 units; one for the Lawful Interception Controller (LIC) and one for the Lawful Interception Browser (LIB) (1+1). The mechanical construction of the LIC and the LIB makes field maintenance and service user friendly. All interface cards are accessible at the front without opening the cover. The unit can be mounted to a 19” rack as well as it can be stacked.

Figure 3. The Nokia LIC and LIB hardware

The Nokia LIG is based on latest Intel technology available, Pentium II processor and NLX motherboard using Compact PCI (CPCI) add-on cards.

The processor used in the LIC and the LIB is a 450MHz Intel Pentium II. The NX440LX motherboard is designed and manufactured by Intel and it is based on industry standard NLX form factor that connects to the CPCI riser card via board edge connector. The motherboard has one 32-bit PCI bus to connect to the riser card.

The riser card incorporates six CPCI slots for network interface cards and storage media.

The LIC and LIB units have dual redundant and hot swappable power supplies.

3.1 LIG software architecture

The LIC and LIB functional softwares are based on the IPSO operating system made by Nokia. IPSO software is developed on the FreeBSD. The GGSN LIE software extension is based on the Nokia GGSN Rel.1.1 software.

Running the GGSN LIE interception functions on the same GGSN device does not have an impact on the GGSN performance.

3.2 Redundancy and service lifetime

The Nokia LIC and LIB units have redundant and hot swappable power supplies.

Planned hardware reliability figures:

- Mean Time Between Failure (MTBF): 50 000 hours
- Mean Time To Repair (MTTR): 30 min

4 LIG interfaces

The Nokia LIG Release 1 has the following IP-based external interfaces towards the LEA, the AA and the LIG administrator.

4.1 X0_1

X0_1 is the interface between the LIC, the AA and the LEA for interception requests and related information. This interface is implemented as a secured Web interface. It also sends alarms by FTP and SCP to the System Administrator, the LEA, the AA and the audit users. (See Figure 2.)

4.2 X0_2 and X0_3

X0_2 is the interface for Interception-Related Information (IRI), and X0_3 is the interface for Communication Content (CC) between the LIB and the LEA. These interfaces are combined in the Nokia LIG solution. The LEA is able to browse the IRI data via a secured Web interface or to receive it together with CC data via Secure Shell (SSH) secure file transfer. The LEA can specify for instance the direction of the desired interception data. These interfaces also send alarms by FTP and SCP to the System Administrator, the LEA, the AA and the audit users.

4.3 Management

LIC and LIB management interfaces for configuration and monitoring are implemented as secured Web based interfaces.

A LIG management person (administrator) receives alarms via secured file transfers.

4.4 Internal interfaces

The Nokia LIG includes an interface to the GPRS Network Management System (NMS) for the polling of LIC and LIB. The system clocks of the LIC and the LIB can be synchronized using Network Time Protocol (NTP) which is provided for instance in the Nokia NMS/2000 Release T12.

4.5 TCP

Transmission Control Protocol (TCP) is used between the LIC, the LIB, and the GGSN to exchange internal messages.

5 Configuration and capacity

The Nokia LIC and LIB nodes are compact Nokia/IPRG IP650 units with minimum configurability options. Only one hardware configuration will be available for both the LIB and the LIC, which results in easier logistics.

5.1 Number of interceptions and attached LEAs

Of each GGSN's maximum active PDP contexts, 1% can be intercept. Thus, when GGSN's active PDP contexts can be 50 000 at the most, 500 interceptions can be performed simultanously. The number of PDP contexts simultanously under interception can be configured by the GGSN LIE.

Five LEAs in maximum can intercept the same PDP context simultaneously.

One LIC is able to manage up to 10 LIBs and one LIB can handle up to 25 GSNs. This means that one LIC and 1-4 LIBs are enough, depending on the number of GGSNs, interception cases and the national requirements. The interception processes do not affect the performance of the GSNs.

5.2 Physical interfaces

The Nokia/IPRG IP650 implements CompactPCI network interface cards. These cards are hot swappable, so a failed network card can be changed without restarting the LIG system.

The supported physical network interface card is the Four port Ethernet 10/100 adapter.

6 Mechanical design and power supply

The IP650 hardware used for the LIC and the LIB is mountable in a 19-inch rack with the following physical dimensions:

- Height 3.5 in / 9 cm
- Depth 21.5 in / 56 cm
- Width 17.5 in / 44 cm
- Weight 35 lbs / 16 kg

Power

- Volts 100-120/200-240VAC
- Amps 3.0/2.0A
- Cycles 50 - 60 Hz

7 Operating environment

Temperature:

- Operating +40 to +105 F / +5 to +40 C in up to 30 000 ft / 9000 m
- Storage –40 to +160 F / –40 to +70 C in up to 30 000 ft / 9000 m

Relative Humidity:

- Operating 10 to 90% non-condensing
- Storage 5 to 95% non-condensing

EMC:

- CE Mark
- FCC Part 15, Class A
- EN55022 (CISPR22, Class A)

Safety:

- UL1950
- CE Mark
- CUL/CSA 22.2 NO 950–M93
- IEC950
- TUV EN60950

8 Documentation

The Nokia LIG documentation includes the IP650 Platform Installation Guide and the Online Reference Guide.

Glossary

AA	Authorising Authority
ADMF	Administration Function
Audit user	Auditing AA authorisations (e.g. for statistics, auditing AAs etc.)
CC	Communication Content
CE Mark	Conformité Europeénne Mark
CPCI	Compact PCI
EN55022	Emissions limits for Information Technology Equipment (ITE).
ETSI	European Telecommunications Standards Institute
EU	European Union
FCC	Federal Communications Commission
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications (Groupe Spéciale Mobile)
GSN	GPRS Support Node
IEC	International Electrotechnical Commission
IMEI	International Mobile station Equipment Identity
IMSI	International Mobile Subscriber Identity
IRI	Interception-Related Information
ISDN	Integrated Services Digital Network
LEA	Lawful Enforcement Agency
LIB	Lawful Interception Browser
LIC	Lawful Interception Controller
LIE	Lawful Interception Extension
LIG	Lawful Interception Gateway
MSISDN	Mobile Station ISDN
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
NMS	Network Management System
NTP	Network Time Protocol
PCI	Peripheral Component Interconnect
PDP	Packet Data Protocol

SGSN	Serving GPRS Support Node
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TUV	Technischer Überwachungs-Verein
UL	Underwriters Laboratories
X0_1	the interface between the LIC and the LEA
X0_2	the interface for Interception-Related Information
X0_3	the interface for Communication Content (CC) between the LIB and the LEA