

NOKIA

**Release 4
Nokia Lawful Interception Gateway**

Auditor's Guide

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.

This document and the product it describes are considered protected by copyright according to the applicable laws.

NOKIA logo is a registered trademark of Nokia Corporation.

Other product names mentioned in this document may be trademarks of their respective companies, and they are mentioned for identification purposes only.

Copyright © Nokia Corporation 2005. All rights reserved.

Contents

Summary of changes4

1 Lawful Interception in the GPRS and UMTS5

1.1 Why Lawful Interception is needed5

1.2 Description of the GPRS, UMTS, and IMS.....6

1.3 Users of the Lawful Interception Gateway.....7

1.4 LIG architecture.....8

1.5 Standardisation10

2 Auditing lawful interception13

2.1 The Auditor's task.....13

2.2 LIG configurations for the Auditor.....13

2.3 Interpretation of audit alarms and log files14

2.3.1 Alarm format.....14

2.3.2 Log files.....17

References21

Glossary22

Summary of changes

Changes between releases 4 and 3

Changes in content

IMS interception is now supported.

SIP URI and TEL URI can be used for identifying the target of an interception.

CLI user can act as an Administrator user in addition to LEA and AA user.

Collecting interception data from the CPS is now possible.

Supported hardware platforms have changed.

Administrator can receive alarms using the SNMP protocol in addition to file transfer.

New audit alarms have been added and the content of the alarms updated.

Two log message fields have been removed.

New 3GPP requirements are reflected in the content.

Changes in documentation

Figure *GPRS and UMTS architecture* in Chapter *Description of the GPRS, UMTS and IMS* has been updated.

Chapter *Users of the Lawful Interception Gateway* has been modified to include information about a new feature; CLI user can also act as Administrator.

Chapter *LIG Architecture* has been modified and new content added.

Chapter *Standardisation* has been modified and new content added.

Figure *LIG elements and interfaces in LIG* in Chapter *LIG Architecture* has been updated.

Figure *GPRS ETSI lawful interception network elements and their corresponding Nokia LIG elements* has been removed.

Chapter *Interpretation of audit alarms and log files* has been modified and new content added.

The references and glossary have been updated.

1 Lawful Interception in the GPRS and UMTS

1.1 Why Lawful Interception is needed

The lawful interception functionality is implemented so that a network operator can fulfil national lawful interception requirements. Nokia Lawful Interception Gateway (LIG) Release 4 is compatible with second generation (2G), General Packet Radio Service (GPRS), and third generation (3G), Universal Mobile Telecommunications System (UMTS). Consequently, Nokia LIG Release 4 provides the authorities with the ability to intercept 2G, 3G mobile data calls, and the IP Multimedia Subsystem (IMS).

The level of interception services required varies from country to country. In most countries, operators have to provide an interception service before they can start the commercial use of the GPRS or UMTS. In some other countries, though, interception is not a mandatory service. An EU directive published in 1995 states that lawful interception for telecom services is mandatory (EU COUNCIL RESOLUTION, 96/C 329/01).

The LIG provides access to the Communication Content (CC) and the Intercept-Related Information (IRI) of the mobile target for Law Enforcement Agencies (LEAs). The target is the subject of interception, whose International Mobile Subscriber Identity (IMSI), International Mobile Station Equipment Identity (IMEI) or Mobile Subscriber International ISDN Number (MSISDN) numbers or Session Initiation Protocol Universal Resource Identifier (SIP URI) or Telephone Universal Resource Identifier (TEL URI) can be used for identification. The CC is the data sent or received by the target, and the IRI is a collection of information associated to telecom services involving the target. The intercept data is the CC and/or IRI data.

The LIG enables auditing of the interception activity. For this purpose, the authorisation additions/deletions/modifications of an Authorising Authority (AA) cause a text file (audit alarm) to be sent to the Auditor's computer.

1.2 Description of the GPRS, UMTS, and IMS

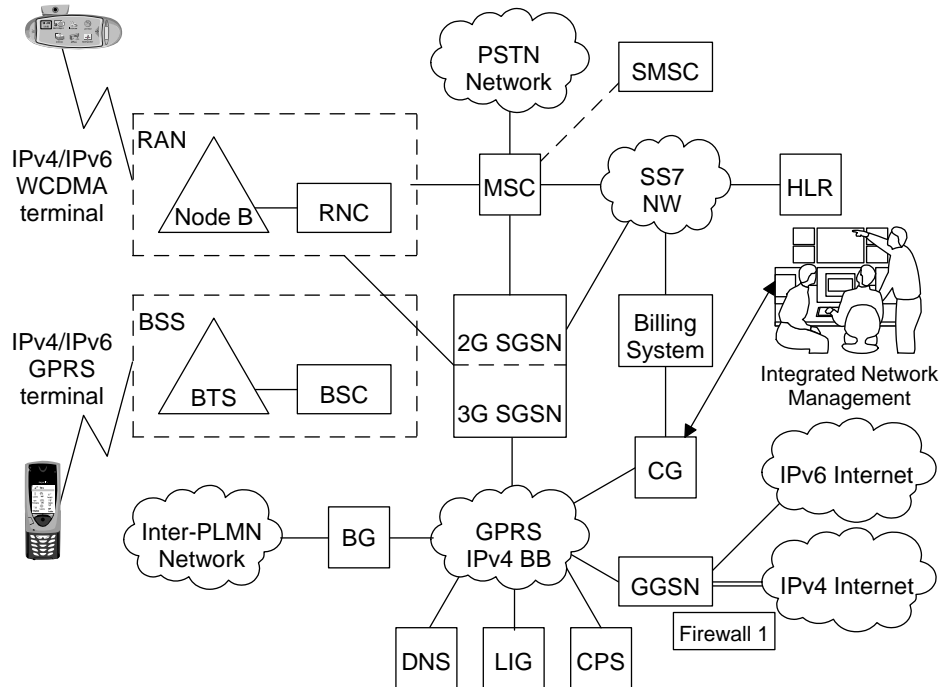


Figure 1. GPRS and UMTS architecture

The GPRS and UMTS enable cost-effective and efficient use of network resources for packet mode data applications, for example, for applications that exhibit one or more of the following characteristics:

- Intermittent, non-periodic (that is, bursty) data transmissions, where the time between successive transmissions greatly exceeds the average transfer delay.
- Frequent transmissions of small volumes of data, for example, transactions consisting of less than 500 octets of data occurring at a rate of up to several transactions per minute.
- Infrequent transmission of larger volumes of data, for example, transactions consisting of several kilobytes of data occurring at a rate of up to several transactions per hour.

Based on standardised network protocols supported by the GPRS/UMTS bearer services, a GPRS/UMTS network administration may offer (or support) a set of additional services, such as:

- *Retrieval services*, which provide the capability of accessing information stored in database centres. The information is sent to the user on demand only. An example of such a service is the World Wide Web (WWW).
- *Messaging services*, which offer user-to-user communication between individual users using storage units with store-and-forward mailbox, and/or message handling functions (for instance, information editing, processing and conversion).
- *Conversational services*, which provide bi-directional communication by means of real-time (no store-and-forward) end-to-end information transfer from user to user. An example of such a service is the Telnet application.
- *Tele-action services*, which are characterised by low data-volume (short) transactions, for example, credit card validation, lottery transactions, utility meter readings and electronic monitoring and surveillance systems.

From the end user's perspective, the main differentiator of the UMTS system is higher data rates. This is due to a completely new radio interface (Wideband Code Division Multiple Access, WCDMA, vs. Time Division Multiple Access, TDMA) in terminals and base stations. The higher data rates enable additional services, such as:

- *Location-based services*, which will become more important.
- New services and applications, including *Internet access and multimedia*, which will be available to wireless users with higher bit rates.
- *Wireless video services* become feasible, maybe even in a revolutionary way compared to video services in the fixed network.
- New services like *broadcasting and cash cards*, which may create business opportunities. The UMTS allows downloading of software to the terminal, for example, applications or a speech codec.

IP Multimedia Subsystem (IMS) offers new IP multimedia services like instant messaging and Voice over IP (VoIP). The Call State Control Function (CSCF) is one of the IMS network elements. In the Nokia Solution it is called the Connection Processing Server (CPS). The CPS is the only IMS network element which contains the Lawful Interception Extension (LIE) software and, therefore, the CPS is the only IMS network element from where the LIG collects intercept data.

1.3 Users of the Lawful Interception Gateway

An operator who has to provide the lawful interception functionality in the GPRS system, the UMTS, or the IP Multimedia Subsystem (IMS) needs to administer lawful interception services. The Lawful Interception Gateway (LIG) provides the Administrator a user account (admin) for this purpose. The

operator has no web access to the actual intercept data or even to the target information.

The Authorising Authority (AA) gives a permission to intercept a specific target and deliver the intercept data to a specific Lawful Enforcement Agency (LEA). There may be several AAs, but they are not aware of each other. An AA has no access to the intercept data itself. The LIG provides one user account, for example 'judge', for each AA. The Administrator (admin) creates the AA's user account.

An LEA may activate the interception of a target according to the given permissions. There may be several LEAs, and each LEA only sees its own target information and the provided authorisations. The LIG provides one user account, for example 'police', for each LEA. An AA creates the LEA's account.

With the Command Line Interface (CLI), a user may connect to the LIC through Telnet or Secure Shell (SSH). The CLI makes it possible to perform Admin, LEA, and AA actions through a command line interface instead of the usual web interface. CLI users can see all information visible to any LEA and AA user, and they can act as any AA or LEA, or as an Administrator user. There may be several separate CLI users in one LIC, but only one CLI user who can act as Administrator user. The LIG provides one user account, for example 'cliUser', for each CLI user. The Administrator (admin) creates a CLI user.

An Auditor is a person who audits the AA's actions. The LIG sends a small text file (audit alarm) to the Auditor whenever the AA creates, modifies, or deletes an interception. The LIG also sends an audit alarm when the Administrator generates a new password to the LIG user, and if the LIG removes log files to prevent overfilling of log transfers. All actions executed through the web interface or CLI are logged. These log files are forwarded periodically to the Auditor. The Auditor does not have a user account in the LIG.

1.4 LIG architecture

The Nokia Lawful Interception Gateway (LIG) Release 4 contains two network elements:

- Lawful Interception Controller (LIC), which controls an interception, and
- Lawful Interception Browser (LIB), which forwards intercept data.

Both elements are based on the Nokia IP740 or IP1260 hardware platforms.

The Lawful Interception Extension (LIE) software collects the intercept data in

- Nokia Gateway GPRS Support Node (GGSN) network element Release 1.3 or later software, and/or
- Nokia 2G Serving GPRS Support Node (2G SGSN) Release 2.0 or later software, and/or

- Nokia 3G Serving GPRS Support Node (3G SGSN) Release 1.0 or later software.
- Nokia IMS Release 2 Connection Processing Server (CPS) network element
- Nokia Flexi ISN Release 2.0

The LIE software is included in the corresponding product. It cannot be ordered separately.

The LIG contains the following interfaces used by the Administrator, Auditor, LEA, or AA (see Figure *LIG elements and interfaces*):

- The HI1 control interface between the LIC and the AA/LEA is implemented as a web interface. The AAs authorise the LEAs' interceptions, and the LEAs activate and deactivate interceptions according to these authorisations.
- An alternative textual HI1 interface in the LIC is called the Command Line Interface (CLI). Most Admin/AA/LEA actions can be performed alternatively using the CLI. The CLI provides an external machine command line interface with a Lawful Interception Management System (LIMS) device.
- The Administrator has their own web interface on the LIC.
- The Auditor receives audit alarms by file transfer from the LIC.
- The Administrator user receives LIG-related alarms by file transfer or Simple Network Management Protocol (SNMP) from the LIC.
- The AA and the LEA users receive LIG-related alarms by file transfer from the LIC.
- HI1 notifications are sent through the HI2 interface.
- The combined HI2 and HI3 interface between the LIB and the LEA is based on data transfer and a web interface.
- The Administrator uses a web interface to manage the LIB.
- The Auditor receives web log files by file transfer from the LIC and LIB.
- The Auditor receives CLI log files by file transfer from the LIC.

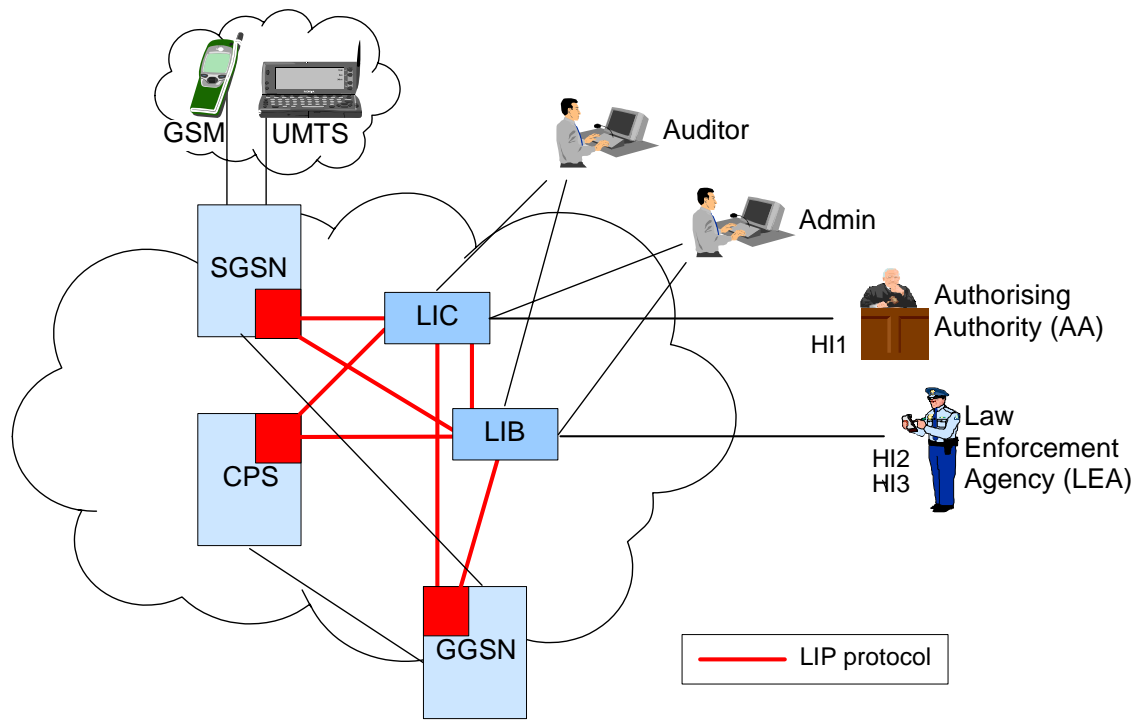


Figure 2. LIG elements and interfaces

File transfer can be secured using Secure Shell (SSH) or, alternatively, the Internet Protocol Security (IPSec), and the web interfaces can be secured using the Secure Sockets Layer (SSL). The LIC controls what intercept data is collected, the GGSN LIE, SGSN LIE, and CPS LIE collect the requested intercept data, and the LIB formats and forwards the collected intercept data.

These five network elements need to communicate with each other, and since the amount of data can occasionally be considerably high, fast network connections should be in place between these network elements. Nokia LIG Release 4 uses a proprietary Transport Control Protocol (TCP)-based protocol internally.

1.5 Standardisation

There are four documents on the General Packet Radio Service (GPRS) and Universal Mobile Telecommunications System (UMTS) Lawful Interception standards:

- 3GPP TS 33.106 deals with lawful interception Stage 1 specification
- 3GPP TS 33.107 deals with lawful interception Stage 2 specification

- 3GPP TS 33.108 and ETSI TS 101.671 deal with handover interfaces for lawful interception.

See Figure 3GPP MS packet switched lawful interception network elements and their corresponding Nokia LIG elements for the reference configuration used in 3GPP TS 33.107.

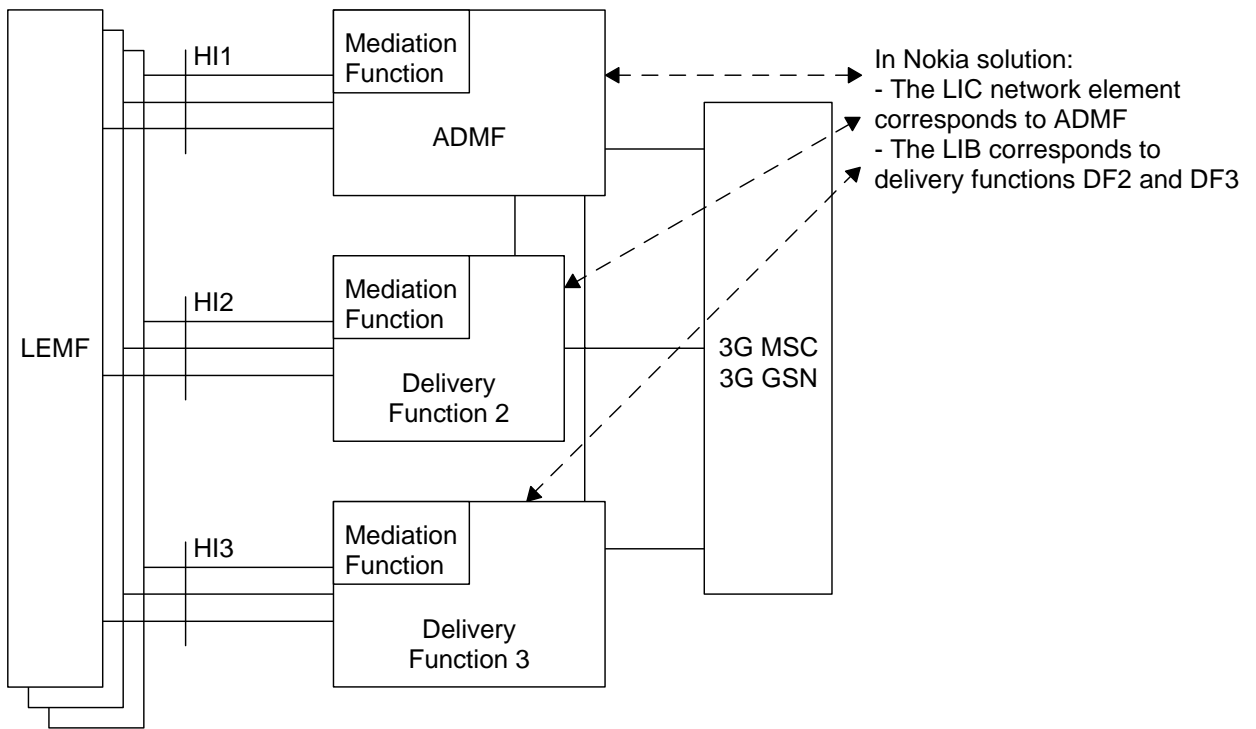


Figure 3. 3GPP MS packet switched lawful interception network elements and their corresponding Nokia LIG elements

In Nokia's implementation, the Lawful Interception Controller (LIC) network element corresponds to the Administration Function (ADMF), and the Lawful Interception Browser (LIB) corresponds to Delivery Functions DF2 and DF3. In the standard, DF2 is the Interception-Related Information (IRI) delivery function, and DF3 is the Communication Content (CC) delivery function.

The standard is not detailed enough for developing open network elements, which would allow for co-operation between the different manufacturers' products. Interfaces HI1, HI2 and HI3 between the LEA/AA and ADMF, or LEMF and DF2/DF3 are defined in 3GPP TS 33.108.

Nokia LIG Release 4 implements the following features mentioned in the standard:

- Interception takes place in the Serving GPRS Support Node (SGSN).

- Interception takes place in the Gateway GPRS Support Node (GGSN).
- Interception takes place in the Call Session Control Function (CSCF) which corresponds to CPS network element in Nokia's solution.
- Target identity is International Mobile Subscriber Identity (IMSI).
- Target identity is International Mobile Station Equipment Identity (IMEI).
- Target identity is Mobile Subscriber International ISDN Number (MSISDN).
- Target identity is Session Initiation Protocol Universal Resource Identifier (SIP URI).
- Target identity is Telephone Universal Resource Identifier (TEL URI).
- IRI event for attach is collected.
- IRI event for detach is collected.
- IRI event for Packet Data Protocol (PDP) context activation is collected.
- IRI event for start of intercept with PDP context active is collected.
- IRI event for PDP context modification is collected.
- IRI event for PDP context deactivation is collected.
- LI notification for start of interception
- LI notification for end of interception.
- IRI event for end of interception.
- IRI event for cell and/or Routing Area (RA) update is collected.
- IRI event for a Short Message Service (SMS) event is collected.
- IRI event for PDP context update (and consequently the current SGSN address).
- IRI event for SIP message is collected.
- ADMF collects target log file.
- IRI/CC data is transmitted securely.
- Location Dependent Interceptions are possible.

Nokia LIG Release 4 contains the following features that are not mentioned in the standard:

- IRI event for start of intercept with no PDP context active is collected.
- IRI event for start of intercept with no context is collected.
- IRI event for SIP session activation.
- IRI event for SIP session update.
- IRI event for SIP session deactivation.

2 Auditing lawful interception

2.1 The Auditor's task

The Auditor's responsibility is to ensure that all interceptions are based on a valid authorisation, and that no unauthorised interceptions are made. The Authorising Authority (AA) gives permissions to intercept a specific target and deliver the intercept data to a specific Law Enforcement Agency (LEA). The LEA uses this authorisation to activate a target's interception. No other interceptions are allowed.

The Auditor is notified when an interception authorisation is created, removed or modified. The information is sent as text files called 'audit alarms'. The audit alarm file name has the format `alarm.n`, where `n` is the sequence number of the alarm. For example, `alarm.00010` is the tenth audit alarm sent by one Lawful Interception Controller (LIC).

Whenever the Auditor receives an audit alarm from the Lawful Interception Controller (LIC), the Auditor checks it to make certain that the interception is based on a valid authorisation, in other words, that no unauthorised interception has been created. (The audit alarms are described in more detail in Chapter *Interpretation of audit alarms and log files*.) It is up to the Auditor to ensure that there is always enough disk space available for the alarm files and log files on the Auditor's computer.

The Auditor can monitor all changes made to the LIC/LIB databases through the web interface. The Auditor uses the web log for this purpose.

The Auditor can monitor all requests and responses which were exchanged through the CLI. The Auditor uses the CLI log for this purpose.

2.2 LIG configurations for the Auditor

The Auditor has no access to the actual Lawful Interception Gateway (LIG) system. When starting to use the LIG, the Auditor needs to contact the LIG

Administrator and give the file transfer configuration information where audit alarms and log files should be sent. The LIG must be able to establish a File Transfer Protocol (FTP) or Secure Shell (SSH) connection to the computer. The computer may be located at the Auditor's or the Administrator's premises.

Depending on which connection type is selected, the following configuration information is needed:

- for FTP: the IP address of the Auditor's computer, the file path where the audit alarms and log files should be sent, the user account, and the password for the computer where the audit alarms and log files are sent. If the computer is in the LIG Administrator's premises, the Auditor only needs to request access to it. The FTP server must be enabled on the receiver's end.
- for SSH: the IP address of the Auditor's computer, the file path where the audit alarms and log files should be sent, and the public key of the computer's root user where audit alarms and log files are sent. The SSH server must be enabled on the receiver's end.

Once the Administrator has finished the initial configuration procedures, the Auditor can start monitoring the incoming audit alarms, Web and CLI activity logs.

If the Auditor wants to change the computer used for receiving alarms, the Auditor must first inform the Administrator of the changes.

2.3 Interpretation of audit alarms and log files

2.3.1 Alarm format

The Auditor receives small data files (audit alarms) from the Lawful Interception Controller (LIC) each time an AA adds, deletes or modifies interception authorisations. Below is an example of a typical audit alarm:

```
ALARM
Destination:      audit
Originator:       LIC
Originator address: 111.111.111.111
Error type:       1001
Severity:         4
Failure:          New authorisation was created
Sequence number:  32
Alarm time:       2005-03-01 14:46:53
```

```
Supplementary info: ReqId=500-22, AA=aa4, LEA=lea4,
                    IMSI=24500145015, IMEI=, MSISDN=,
                    SIPURL=, TELURL=,
                    validFrom=Tue Feb 1 01:46:00
                    2005, validTo=Sat Apr 1 14:50:00
                    2005,
                    Authorised type=7, Authorised
                    optionsIRI=3, warrant ID=echelon
```

The interpretation of the audit alarm is as follows:

- *Destination* is the receiver of the alarm. The Lawful Interception Gateway (LIG) has also other alarms, which are sent to the Administrator, Authorising Authority (AA) or Law Enforcement Agency (LEA). The destination of audit alarms is always *audit*.
- *Originator* is the type of the LIG device that sent the alarm. All audit alarms come from the LIC, since the LIC controls authorisations of interceptions.
- *Originator address* is the IP address of the device that sent the alarm.
- *Error type* identifies the type of the audit alarm. Actually, there is no error involved, but most of the other LIG alarms are related to different error situations, hence the field name. Auditing error types are:
 - 1001 - A new authorisation was created.
 - 1002 - The authorisation was removed.
 - 1005 - The existing authorisation was modified.
 - 1014 - Custom alarm from LIC Admin user
 - 1021 - Log files removed to prevent overflowing of log transfer (LIC)
 - 2271 - Log files removed to prevent overflowing of log transfer (LIB)
 - 4100 - New LIG user password generated
- The *severity* value is 4 in all audit alarms.
- *Failure* gives a short textual representation of the audit alarm. As in *error type*, there is actually no failure related to audit alarms.
- *Sequence number* is the literal sequence number of the audit alarm. The value is the same as in the file name. You can easily determine if you have received all audit alarms by checking that there are no gaps in sequence numbering. Each originator (LIC) uses its own sequence numbering.

Note

Each LIC sends files named `alarm.00001`, `alarm.00002`, and so on. The audit alarm destination for each LIC should be different.

- *Alarm time* is the time (local time) when the audit alarm was created.
- *Supplementary info* gives additional information related to the audit alarm depending on the error type.

For Error types 1001 and 1005 the set of values (separated by commas) has the following meaning:

- *ReqId* is the request identifier of the interception. It is a unique identifier used to identify the interception. The first number is the identifier of the LIC and the second number is the sequence number of the interception within the LIC. In the example above, the interception is the 22nd interception in LIC 500.
- *AA* is the AA who authorised the interception.
- *LEA* is the LEA who was authorised to perform the interception.
- *IMSI*, *IMEI*, *MSISDN*, *SIPURL*, and *TELURL* are the International Mobile Subscriber Identity (IMSI), International Mobile Station Equipment Identity (IMEI), Mobile Subscriber International ISDN Number (MSISDN), Session Initiation Protocol Universal Resource Locator (SIPURL), and Telephone Universal Resource Locator (TELURL) of the intercept target. Interceptions are authorised by using one of these five identifiers (in the example above, the authorisation was based on the IMSI).
- *validFrom* and *validTo* define the validity period of the interception (local time), that is, the period during which the LEA is authorised to intercept the target.
- *Authorised type / type* is the type of the interception. The values are:
 - 1 Interception-Related Information (IRI) data
 - 2 Mobile-Originated Communication Content (CC) data
 - 3 Mobile-Originated CC and IRI data
 - 4 Mobile-Terminated CC data
 - 5 Mobile-Terminated CC and IRI data
 - 6 Mobile-Originated CC and Mobile-Terminated CC data
 - 7 Mobile-Originated CC, Mobile-Terminated CC and IRI data
- *Authorised optionsIRI / optionsIRI* are authorisations for how the LEA can access the intercepted data. The values are:
 - 0 Not defined
 - 1 Authorise the LEA to only browse the collected data on the LIB
 - 2 Authorise the LEA only to transfer the collected data to the IP address specified by the LEA

3 Authorise the LEA to browse the collected data on the LIB and to transfer the collected data to the IP address specified by the LEA.

- *warrant ID* is the warrant identifier given by the AA.

For Error type 1002, only the values *ReqId*, *AA*, *LEA*, and *warrant ID* are present. The meanings are defined above.

For Error type 1014, the LIC Administrator may write any message to the supplementary info field.

For Error type 1021 and 2271, the supplementary info field contains the name of the user whose log files are being removed.

For Error type 4100, the supplementary info field contains the name of the LIG user whose password was regenerated and the IP address of the network element where the password was overwritten.

2.3.2 Log files

The Auditor receives web logs and CLI activity logs periodically from the LIC. The Auditor receives web log files and CLI log files at intervals set by the Admin user. The intervals can be based on the age or size of the log files.

Log file messages have the following format:

```
<seq><yyyy-mm-dd><hh:mm:ss>,<severity>,<pid>,<uid>,<proc>,<msg>
```

Format of log message fields

The following fields are used in the web log and CLI log messages:

Table 1. Format of log message fields

Field	Description
<h:mm:ss>	The local time. Each log message contains the time when the log message was created. Its length is eight characters.
<msg>	The actual log message.
<pid>	The process identifier of the creator of the log message. The length is five characters for the identifier plus four characters for the string 'pid'.
<proc>	Process name.
<seq>	The sequence number. Each log message contains a sequence number. They are consecutive within the log file. Even log files, which are related to different Authorising Authority (AA) users (or Law Enforcement Agency, LEA,

Field	Description
	users), use different sequence numbers. The length of <seq> is six characters. Sequence numbering starts from one whenever the node is rebooted.
<severity>	The severity as an integer value. The length is one character for the value plus nine characters for the string 'severity'. For more information, see Section <i>Severity of log messages</i> .
<uid>	The user identifier of the creator of the log message. The length is five characters for the identifier plus four characters for string 'uid'.
<yyyy-mm-dd>	The date. Each log message contains the date when the log message was created. The used format makes it easy to order the log message based on the date. The length is ten characters.

Severity of log messages

Log messages found in log files (see *Format of log message fields* above) have always some severity. The following severity values are used (the integer value is shown in parentheses):

Table 2. Severity values for log messages

Value	Description
FATAL (0)	Fatal conditions that should be corrected immediately, such as corrupted database.
ERROR (1)	Error conditions, such as communication failures.
WARNING (2)	Warning messages.
NOTICE (3)	Conditions that are not error conditions but should possibly be handled separately.
INFO (4)	Informational messages.
DEBUG (5)	Messages that are only logged when debugging a program.

Web log

Web log files are produced both in the LIC and the LIB. A web log file's name as seen by the Auditor is as follows:

lic#<IP address of the LIC>#<timestamp>#liWeb.log

or

lib#<IP address of the LIB>#<timestamp>#liWeb.log

The web log file contains log messages containing information about web activity in the LIB or the LIC.

The following is an example of a web log file:

```
000001 2002-10-24 06:38:58,severity 3,pid 00363,uid 65534,usr_mgmt.cgi,
POST from admin in 131.228.43.43: user database of LIC updated

000002 2002-10-24 06:40:46,severity 3,pid 00385,uid
65534,change_alarm.cgi, POST from 131.228.43.43: alarm configuration
updated for user aal

000003 2002-10-24 06:41:04,severity 3,pid 00389,uid 65534,usr_mgmt.cgi,
POST from aal in 131.228.43.43: user database of LIC updated

000004 2002-10-24 06:41:14,severity 3,pid 00393,uid 65534,usr_mgmt.cgi,
POST from aal in 131.228.43.43: user database of LIC updated

000005 2002-10-24 06:41:44,severity 3,pid 00398,uid 65534,auth_mgmt.cgi,
POST from aal in 131.228.43.43: target database of LIC updated

000006 2002-10-24 06:42:33,severity 3,pid 00408,uid
65534,change_alarm.cgi, POST from 131.228.43.43: alarm configuration
updated for user leal

000007 2002-10-24 06:43:31,severity 3,pid 00422,uid 65534,int_mgmt.cgi,
POST from leal in 131.228.43.43: target database of LIC updated

000008 2002-10-24 06:48:32,severity 3,pid 00488,uid 00000,backup.cgi,
POST from 131.228.43.43: Backup configuration updated.

000009 2002-10-24 06:48:36,severity 3,pid 00488,uid 00000,backup.cgi,
Backup made.
```

CLI log

CLI activity log files are produced only in the LIC. A CLI activity log file's name as seen by the Auditor is as follows:

lic#<IP address of the LIC>#<timestamp>#liCLI.log

The CLI log file contains one log message containing information about each command request and each result of a command execution.

The following is an example of a CLI log file:

```
020755 2002-10-25 10:55:14,severity 4,pid 01171,
uid 00032,cli, User cliuser logged in.

020756 2002-10-25 10:55:14,severity 4,pid 01171,
uid 00032,cli, User cliuser executed command:

81?WarrantID=testwarrant&LIBaddr=192.168.182.181
&AAUsername=aal&LEAUsername=leal&ValidFrom=24.10.2002
&ValidTo=24.11.2002&StartTime=23:00&EndTime=23:00&
AuthorizedOptions=3&InterceptType=7&AuthorizedIntercept
Type=7&InterceptionOptions=6&FwdUsernameCC=lealFwd&
FwdPasswordCC=abc123&FwdAddrCC=192.168.182.187&
FwdPathCC=/home/lealFwd/cc_ftp&FwdDelayCC=10&FwdSize
CC=50000&InterceptionOptions=6&FwdUsernameIRI=lealFwd
&FwdPasswordIRI=abc123&FwdAddrIRI=192.168.182.187&
```

```
FwdPathIRI=/home/lealFwd/iri_ftp&FwdDelayIRI=10&
FwdSizeIRI=50000&IMSI=765434 with successful status.
Request ID 20-512 created.
020757 2002-10-25 10:55:14,severity 4,pid 01171,
uid 00032,cli, User cliuser logged out.
020758 2002-10-25 10:59:06,severity 4,pid 01178,
uid 00032,cli, User cliuser logged in.
020759 2002-10-25 10:59:10,severity 4,pid 01178,
uid 00032,cli, User cliuser executed command: 87 with successful status.
020760 2002-10-25 10:59:13,severity 4,pid 01178,
uid 00032,cli, User cliuser logged out.
```

For more information about the CLI log files, see *CLI User's Guide*.

References

LIG Release 4 documentation

1. Nokia LIG Release 4 Product Documentation: CLI User's Guide

Other references

1. Official Journal of the European Communities, 96/C 329/01: Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications.
2. 3GPP TS 33.107
3GPP TS 33.107 V6.5.0. 3G Security; Lawful Interception Architecture and Functions, (Release 6). 3rd Generation Partnership Project (3GPP).
3. 3GPP TS 33.108
3GPP TS 33.108 V6.9.0. 3G Security; Handover Interface for Lawful Interception (Release 6). 3rd Generation Partnership Project (3GPP).
4. ETSI TS 101.671
ETSI TS 101.671 V2.12.1. Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic.

Glossary

3GPP	The Third Generation Partnership Project
3GPP MS	Third Generation Mobile Communication System
AA	Authorising Authority
admin	Administrator User Account
ADMF	Administration Function
CC	Content of Communication
CLI	Command Line Interface
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)
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
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
LIMS	Lawful Interception Management System
MSISDN	Mobile Subscriber International ISDN Number
PDP	Packet Data Protocol
RA	Routing Area
SGSN	Serving GPRS Support Node
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
WCDMA	Wideband Code Division Multiple Access
WWW	World Wide Web