ANNEXE
au
Règlement 14/XXX/ILR du XX XXXX 2014

Lawful interception of electronic communications :

National Specifications for Luxembourg

Table of contents

1 Introduction

These specifications describe the technical implementation of lawful interception of telecommunications in Luxembourg. Implementation is carried out on the basis of the relevant ETSI specification (refer to 3); this document describes the options and amendments that have been defined for Luxembourg.

2 Scope

This document is written in English and will be provided to the NWO/AP/SvP upon request. It applies to any Network Operator, Access Provider or Service Provider (NWO/AP/SvP) in the Grand Duchy of Luxembourg that is obligated to comply in lawful interception.

3 Basis of this specification

This document includes the ETSI documents listed below, which are applicable in the version noted as follows or in later versions, and are to be observed.

[1]	**ETSI TS 101 671**	**V3.12.1**	**(2013-11):**	**Lawful Interception (LI); Handover Interface for the lawful interception of telecommunications traffic**
[2]	**ETSI TS 133 108**	**V11.4.0**	**(2012-10):**	**Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Handover interface for Lawful Interception (LI)**
[3]	**ETSI TS 102 232-1**	**V3.5.1**	**(2013-10):**	**Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery**
[4]	**ETSI TS 102 232-2**	**V3.6.1**	**(2013-10):**	**Part 2: Service specific details for messaging services**
[5]	**ETSI TS 102 232-3**	**V3.3.1**	**(2013-10):**	**Part 3: Service specific details for internet access services**
[6]	**ETSI TS 102 232-4**	**V3.1.1**	**(2012-02):**	**Part 4: Service specific details for Layer 2 services**
[7]	**ETSI TS 102 232-5**	**V3.2.1**	**(2012-06):**	**Part 5: Service specific details for IP Multi Media services**
[8]	**ETSI TS 102 232-6**	**V3.2.1**	**(2013-07):**	**Part 6: Service specific details for PSTN/ISDN services**
[9]	**ETSI TS 102 232-7**	**V3.2.1**	**(2013-07):**	**Part 7: Service specific details for Mobile Packet Services**

If existing the chosen options and national amendments to these ETSI documents are listed in the following chapters. If no options or amendments are existing for a document, then it is applicable without change in the version specified above or a later version.

4 List of abbreviations

Abbreviation	Description
3GPP	3rd Generation Partnership Project
AP	Access Provider
ASN.1	Abstract Syntax Notation One
CC	Content of Communication
CCLID	CC Link IDentifier
CUG	Closed User Group
DSL	Digital Subscriber Line
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GGSN	Gateway GPRS Support Node
GLIC	GPRS LI Corellation
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HI 1	Handover Interface 1
HI 2	Handover Interface 2
HI 3	Handover Interface 3
ID	Identifier
IPSec	Internet Protocol Security
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIID	Lawful Interception Identifier
NEID	Network Element Identifier
NID	Network Identifier
NWO	Network Operator
ROSE	Remote Operation Service Element
RTP	Real-Time Transport Protocol
SGSN	Serving GPRS Support Node
SMS	Short Message Service
SSD	Service-Specific Details
SvP	Service Provider
TCP	Transmission Control Protocol
TS	Technical Specification
UDP	User Datagram Protocol
ULIC	UMTS LI Corellation
UMTS	Universal Mobile Telecommunication System
UPS	Uninterruptible power supply
UUS	User to User Signalling
VPN	Virtual Private Network

5 Options that are chosen and amendments

5.1 Re [1] (TS 101 671)

Options that can be chosen in each country and amendments to [1] are listed in this chapter.

5.1.1 Re [1], General section

Re. Section	Reference / Description	National provision / extension
5.1	**Handover interface 1 (HI1)** Design, electronic or manual	The HI1 interface will remain manual. If a legal basis is created for electronic implementation of the HI1 interface, this will be introduced at a later stage. Exception: LI Management Notifications (LI BEGIN, LI MODIFY, LI END, ALARM) must be sent via the electronic HI2 interface (pls. refer to [1], D.4).
5.2	**Handover Interface port 2 (HI2)**	The IRI records are transmitted individually.
6.1	**Lawful Interception Identifier (LIID)**	The LIID is defined by the LEA and the NWO/AP/SvP is notified.
6.2.1	**Network IDentifier (NID)**	The NID consists of the Operator ID and Network Element Identifier (NEID). The Operator ID consists of up to five characters; the nomenclature is defined and updated by the LEA. The NEID is 1-25 characters long, as defined in [1].
7.2	**LI notifications towards the LEMF**	LI Management Notifications (LI BEGIN, LI MODIFY, LI END, ALARM) must be sent via the electronic HI2 interface (pls. refer to [1], D.4).
8.1	**Data transmission protocols (HI2)**	Only FTP is to be used, there are no plans to use ROSE.
9	**HI3: Interface port for Content of Communication**	The Content of Communication (CC) must be presented as a transparent en-clair copy, if the encryption is managed by the network. Encryption not managed by the network, e.g. user provided end-to-end encryption, has not to be removed by the network.
10.1	**Timing**	If IRI cannot be transmitted, they must be buffered by the NWO/AP/SvP. Minimum buffer time: 3 days

11	**Security aspects**	ISDN transmission: An ISDN CUG (closed user group) is to be formed in accordance with the LEA. IP-based transmission: A VPN including IPSec encryption will be set up between the NWO/AP/SvPs obliged to provide for intercepts and the LEAs, refer to explanations in chapter 6.2 of this document.
12	**Quantitative aspects**	The following figures can be used as a basis for dimensioning the technical equipment installed at the NWO/AP/SvPs: • 50 targets for the first 10000 subscribers • an additional 20 targets for each further 10000 subscribers started (e.g.: NWO with 76000 subscribers shall be able to set up at least 50+7*20= 190 targets)

5.1.2 Re [1], Annex A circuit-switched network handover

re. Section	Reference / Description	National provision / Extension
A.1.1	**CC Link IDentifier (CCLID)**	As the option B (A.5.4.2) has been specified in A.5.4, the CCLID has to be set by the NWO/AP/SvP.
A.1.3	**Usage of Identifiers**	As option B (A.5.4.2) has been specified in A.5.4, the rules according to table A.1.1, right side, apply.
A.3.2	**Structure of IRI records**	Only IRI conforming to ASN.1-description are permissible.
A.3.2.1	**Control information for HI2, 5) date and time**	Date and time are to be transmitted as local time.
A.4	**HI3: Interface port for Content of Communication**	The Content of Communication (CC) must be presented as a transparent en-clair copy, if the encryption is managed by the network. Encryption not managed by the network, e.g. user provided end-to-end encryption, has not to be removed by the network.
A.4.1	**Delivery of content of communication (CC)**	Use of UUS1 has been specified. In order to enable sub-addressing as fall-back the LIID for circuit switched intercepts are implemented solely by number (LIID is set by LEA)
A.4.2	**Delivery of packetized content of communication (CC)**	Transmission of text messages (SMS) and UUS is only via the HI2 interface.
A.4.4.1	**Failure of CC links**	The NWO/AP/SvP has to make three attempts at an interval of five seconds.

A.4.4.2	**Fault reporting**	Error messages must be transmitted over HI2 in accordance with Annex D.4, if the system used by the NWO/AP/SvP supports this functionality.
A.4.5	**Security requirements at the HI3 interface port**	Refer to 5.1.1, re. 11. Security Aspects
A.5.4	**Multi party calls - general principles, options A, B**	Option B is used.
A.6.4.1	**Explicit call transfer, CC link**	Option 2.) has been specified, transferred calls are not intercepted.
A.6.22	**User-to-User signalling (UUS)**	Transmission via HI2 has been specified, also refer to A.4.2.
A.8.3	**HI3 (delivery of CC)**	Correlation information is transmitted in conformance with 5.1.2, sec. A.4.1.

5.1.3 Re [1], Annex C HI2 delivery mechanisms and procedures

re. Section	Reference / Description	National provision / Extension
C	**ROSE or FTP**	Only FTP is to be used, there are no plans to use ROSE.
C.2.2	**Usage of FTP**	Method B is to be used.

5.1.4 Re [1], Annex D Structure of data at the handover interface

re. Section	Reference / Description	National provision / Extension
D	**ASN.1 object tree**	Additional national parameters will be established, refer to Annex A for the definition.

5.1.5 Re [1], Annex E Use of subaddress and calling party number to carry correlation information

re. Section	Reference / Description	National provision / Extension
E.2	**Subaddress options**	**According to Table E.2.1 in [1], the default value for *Type of subaddress* is *"user specified".***

E.3.2	**Field order and layout**	To distinguish between "old" transmission and transmission in accordance with this specification, the octets 16-23 are allocated as follows: If 'old' transmission: no entry If transmitting according to this specification: "Xa.bb.cc" X: E for ETSI a: main version TS101 671 bb: technical version cc: editorial version (Example: E3.12.01 for TS 101 671 V3.12.1)

5.1.6 Re [1], Annex F GPRS HI3 interface (includes 3GPP as referenced in [1])

re. Section	Reference / Description	National provision / extension
F.1	**Functional architecture**	GGSN and SGSN interception are to be set as standard in order to obtain a maximum of information. If for technical reasons only one kind of interception is possible, then SGSN interception is to be set up.
F.3	**HI3 Delivery of Content of Communication (CC)**	Transmission by GLIC/TCP or FTP/TCP is allowed, GLIC/UDP is not allowed.
F.3.2.2	**Usage of FTP**	Method B is to be used.
F.3.2.2	**Usage of FTP**	The following triggers have been specified: send timeout = 10s volume trigger = 10 MByte

5.1.7 Re [1], Annex D.5 ASN.1 - description of IRI (HI2)

All parameters described in the ASN.1 Notation MUST be transmitted, even if they have been marked as optional, insofar as they are available with regard to the respective message.

ASN.1-Reference	Reference / Description	National provision / Extension
04022.1.10	**Location**	In case of a mobile connection, the following parameters must be set: - globalCellID - gsmlocation or umtslocation or epslocation
04022.1.10	**Location/gsm Location/ GeoCoordinates**	The AZIMUTH value must be set except in the case of an omni-directional antenna (360° antenna).

04022.1.10	**National HI2-ASN1parameters/ LuxParameters**	National parameters have been defined in addition to the ASN.1 Description in [1]: the description can be found in Annex A.
04022.1.10	**partyinformation**	An individual partyinformation must be sent for EACH party involved in a communication.
04022.1.10	**partyinformation/partyidentity**	All existing parameters must be set, depending on the means of communication used.

5.2 Re [2] (TS 133 108)

The options that can be chosen in each country and amendments to [2] are listed in this chapter.

5.2.1 Re[2], General section

re. Section	Reference / Description	National provision / Extension
4.5	**HI2: Interface port for intercept related information**	If it is not possible to transmit the IRI, they must be buffered by the NWO/AP/SvP. Minimum buffer time: 3 days
4.5.1	**Data transmission protocols (HI2)**	Only FTP is to be used, there are no plans to use ROSE.
5.1.2.1	**Network IDentifier (NID)**	The NID consists of the Operator ID and Network Element Identifier (NEID). The Operator ID consists of up to five characters; the nomenclature is defined and updated by the LEA. The NEID is 1-25 characters long, as defined in [1].
5.2.2.1	**Control information for HI2, 5) Date and Time**	Date and time are to be transmitted as local time.
5.3.1	**Delivery of content of Communication (CC)**	Use of UUS1 has been specified. In order to enable sub-addressing as fall-back the LIID for circuit switched intercepts are implemented solely by number (LIID is set by LEA)
5.3.3	**Security requirements at the interface port of HI3**	ISDN transmission: An ISDN CUG (closed user group) is to be formed in accordance with the LEA.
5.4.4	**Multi party calls - general principles, options A, B**	Option B is chosen.
5.5.4.1	**Explicit call transfer, CC link**	Option 2.) has been specified, transferred calls are not intercepted.
5.5.15	**User-to-User signalling (UUS)**	Transmission via HI2 has been specified.
6.2.1 7.2.1 8.2.1 9.2.1 10.2.1 11.2.1	**Timing**	If IRI cannot be transmitted, they must be buffered by the NWO/AP/SvP. Minimum buffer time: 3 days
6.3 7.3 8.3 9.3 10.3 11.3	**Security aspects**	IP-based transmission: A VPN including IPSec encryption will be set up between the NWO/AP/SvPs obliged to provide for intercepts and the LEAs, refer to explanations in chapter 6.2 of this document.

6.4 7.4 8.4 9.4 10.4 11.4	**Quantitative aspects**	The following figures can be used as a basis for dimensioning the technical equipment installed at the NWO/AP/SvPs: • 50 targets for the first 10000 subscribers • an additional 20 targets for each further 10000 subscribers started (e.g.: NWO with 76000 subscribers shall be able to set up at least 50+7*20= 190 targets)
6.6	**IRI reporting for packet domain at GGSN**	This option does not have to be implemented in Luxembourg.
6.7	**Content of communication interception for packet domain at GGSN**	The option has been chosen. All target traffic, which is available at the interception node, is to be routed to the LEA.

5.2.2 Re [2], Annex A HI2 delivery mechanisms and procedures

re. Section	Reference / Description	National provision / Extension
A	**ROSE or FTP**	Only FTP is to be used, there are no plans to use ROSE.
A.2.2	**Usage of FTP**	Method B is to be used.
A.2.2	**Usage of FTP**	The following triggers have been specified: send timeout = 10s volume trigger = 10MByte

5.2.3 Re [2], Annex C UMTS and EPS HI3 interface

re. Section	Reference / Description	National provision / Extension
C	**UMTS and EPS HI3 interfaces; Methods of transmission**	Only ULICV1 via TCP stream is to be used.
C.2.2	**Usage of FTP**	Method B is to be used.

5.2.4 Re [2], Annex J Use of subaddress and calling party number to carry correlation information

re. Section	Reference / Description	National provision / Extension

J.2.3.2	**Field order and layout**	To distinguish between "old" transmission and transmission in accordance with this specification, the octets 16-23 are allocated as follows: If 'old' transmission: no entry If transmitting according to this specification: "Xa.bb.cc" X: E for ETSI a: main version TS101 671 bb: technical version cc: editorial version (Example: E3.12.01 for TS 101 671 V3.12.1)

5.2.5 Re [2], Annex B ASN.1-description

All the parameters described in the ASN.1 Notation, even if they are marked as optional, MUST be transmitted, insofar as they exist with regard to the respective message.

ASN.1 - Reference	Reference / Description	National provision / Extension
04022.4	**General**	The provisions in [2] remain unchanged.

5.3 Re [3] (TS 102 232-1)

The options that can be chosen in each country and amendments to [3] are listed in this chapter.

5.3.1 Re [3], General Section

re. Section	Reference / Description	National provision / Extension
5.2.3	**Authorization country code**	Specified as "LU".
5.2.4	**Communication identifier**	The Operator ID consists of up to five characters; the nomenclature is defined and updated by the LEA.
6.2.3	**Aggregation of payloads**	Combined transmission of IP packets is authorised, but must not delay transmission unnecessarily. The delay must not last longer than a few seconds.
6.2.4	**Sending a large block of application-level data**	Segmentation is not used.
6.2.5	**Padding data**	Padding is not used.
6.2.6	**Payload Encryption**	Payload encryption is not used.
6.3.1	**General**	TCP/IP socket connections are used.
6.3.2	**Opening and closing connections**	The NWO/AP/SvP shall make three connection attempts at an interval of ten seconds. The socket connection is to be closed by the NWO/AP/SvP after 2 minutes of inactivity.
6.3.4	**Keep alives**	Using Keep-Alives can be used if desired, but must be agreed between NWO/AP/SvP and LEA. The preferred method is closing the connection after 2 minutes of inactivity according to 6.3.2. If the LEA requests Keep-Alives, the function must be implemented.
6.4.2	**TCP Settings**	The following port numbers have been specified: 50100 for HI-2 (IRI for e.g. XDSL) 50110 for HI-3 (CC for e.g. XDSL)
7.2	**Security requirements**	IP-based transmission: A VPN including IPSec encryption is to be set up between the NWO/AP/SvPs and the LEAs; please refer to Explanations in 6.2.

5.3.2 Supplements to [3], Annex A ASN.1 syntax trees

All parameters described in the ASN.1 Notation, even if they have been marked as optional, MUST be transmitted, insofar as they exist with regard to the respective message.

ASN.1-Reference	Reference / Description	National Provision / Extension
04022.5	**General**	The provisions in [3] remain unchanged.

5.4 Re [4], [5], [6], [7] (TS 102 232 – 2...5)

5.4.1 Re [4], [5], [6], [7]; General Section

The provisions in the specified documents remain unchanged.

5.4.2 Supplements to [4], [5], [6], [7]; ASN.1 definitions

All parameters described in the ASN.1 Notation, even if they have been marked as optional, MUST be transmitted, insofar as they exist with regard to the respective message.

ASN.1-Reference	Reference / Description	National Provision / Extension
04022.5	**General**	The provisions in [4], [5], [6] and [7] remain unchanged.

5.5 Re [8] (TS 102 232 – 6)

5.5.1 Re [8]; General Section

REMARK: If the NWO/AP/SvP's equipment supports the delivery of CC via dedicated ISDN channels as described and defined in [1], this delivery shall be used for PSTN/ISDN services described in TS 102 232-6 as well.

If the delivery of CC via dedicated ISDN channels is not supported by the NWO/AP/SvP's equipment, the CC delivered via RTP according to [8] shall be coded in G.711.

The other provisions in the specified documents remain unchanged.

5.5.2 Supplements to [8]; ASN.1 definitions

All parameters described in the ASN.1 Notation, even if they have been marked as optional, MUST be transmitted, insofar as they exist with regard to the respective message.

ASN.1-Reference	Reference / Description	National Provision / Extension
04022.5	**General**	The provisions in [8] remain unchanged.

5.6 Re [9] (TS 102 232 – 7)

5.6.1 Re [9]; General Section

The provisions in the specified documents remain unchanged.

5.6.2 Supplements to [9]; ASN.1 definitions

All parameters described in the ASN.1 Notation, even if they have been marked as optional, MUST be transmitted, insofar as they exist with regard to the respective message.

ASN.1-Reference	Reference / Description	National Provision / Extension
04022.5	**General**	The provisions in [9] remain unchanged.

6 Technical Provisions

6.1 ISDN based transmission

Routing of CC (content of communication) is via ISDN dial-up lines using Euro ISDN (E-DSS1). An ISDN CUG (closed user group) between the NWO/AP/SvP and the LEA is to be formed.

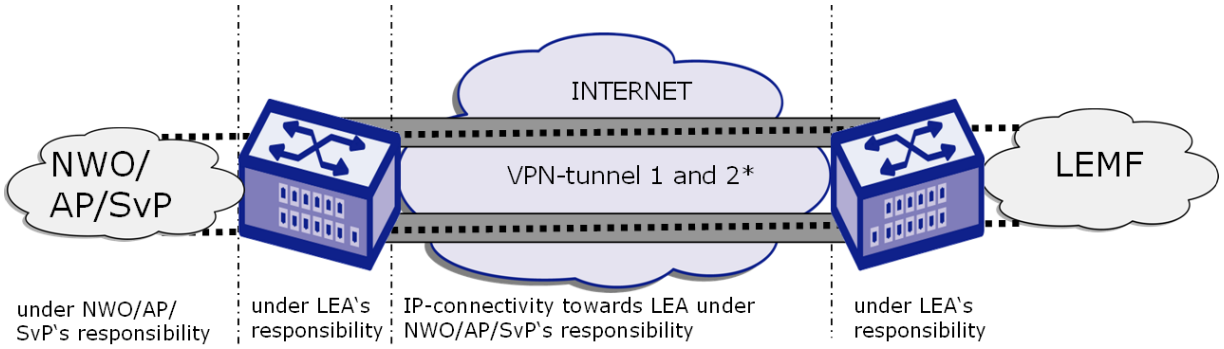
6.2 IP based transmission

IP-based transmission takes place over a VPN which is set up over the Internet. Provision, configuration and operation of the VPN components are the responsibility of the LEA.

The following components shall be provided by the NWO/AP/SvP:

- Transparent Internet access to each LEA:
  Internet access must be sized adequately, must have static, official IP addresses and must be equipped with maximum availability with regard to the infrastructure of the NWO/AP/SvP.
  Internet access needs to be planned and implemented in parallel if required by the LEA for introduction of redundancy. In this case both Internet accesses should be planned as independently as possible from one another, taking the infrastructure at the NWO/AP/SvP into account (e.g. separate physical entry points, routing, autonomous network components, independent Peering Points)

- Infrastructure at the handover point:
  The following components are to be supplied by the NWO/AP/SvP:
  - exclusive 19" rack, with lock
  - 2 X 230 VAC, 16 amp. power supply (connected to UPS)
  - waste heat < 1kW
  - installation in IT server room
  - transparent Internet access/Internet access terminates in this 19" rack (GigabitEthernet or faster)
  - handover from the provider's network takes place in this 19" rack (GigabitEthernet or faster)



* second Internet access on LEA's request

Annex A: National HI2-ASN.1 parameters

Additions to HI2-Operations

```
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
version18(18)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

Natparas
        FROM NatParameter;


National-HI2-ASN1parameters ::= SEQUENCE
{
countryCode [1] PrintableString (SIZE (2)),
-- Country Code (LU for Luxembourg) according to ISO 3166-1,
-- the country to which the parameters inserted after the extension marker apply.
-- In case a given country wants to use additional national parameters according to
-- its law, these national parameters should be defined using the ASN.1 syntax and
-- added after the extension marker (...).
-- It is recommended that "version parameter" and "vendor identification parameter"
-- are included in the national parameters definition. Vendor identifications can be
-- retrieved from the IANA web site (see annex H). Besides, it is recommended to
-- avoid using tags from 240 to 255 in a formal type definition.
natparas [2] Natparas,
-- Import from National Specifications for Luxembourg, Annex A
}
END -- HI2Operations
```

NatParameter

```
-- National parameter
-- Content defined by national law
-- Version of this ASN.1 specification of the national parameters: '1',
-- to be inserted into the parameter "specificationVersion"
-- The coding of all text fields shall be according to CODEPAGE 1252

NatParameter

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

Natparas ::= SEQUENCE
{
        natVersion      [1]     SEQUENCE
        {

                Version[1]      INTEGER(0..255)
        },

        locationDetails [2]     LocationDetails OPTIONAL
}

-- ***************************** Parameter begin **********************

LocationDetails ::= SEQUENCE
{
        radius                  [0]     INTEGER(0..2147483647) OPTIONAL,
        -- radius of a cell in metres

        radiationDirection      [1]     INTEGER(0..360) OPTIONAL,
        -- radiation direction of the main beam of a cell in degrees

        deflectionAngle[2]      INTEGER(0..360) OPTIONAL,
        -- deflection angle of the cell in degrees

        fieldIntensity  [3]     INTEGER(-200..0) OPTIONAL,
        -- field intensity of the mobile phone in [dbm]

        remark                  [4]     PrintableString (SIZE (256)) OPTIONAL
        -- free text for additional information
        -- (e.g. "antenna position Main Station, Building 16")
}

-- ***************************** Parameter end **********************

END
```