

Lawful Interception - TBwiki

[Originalartikel](#)

[Backup](#)

<html> <p>A feature provided by service providers to law enforcement agencies (FBI, Interpol, RCMP, etc.) that allowing law enforcement agencies to intercept calls by receiving a copy of the audio of both parties and call information records.</p> <table id=„toc“ class=„toc“ readability=„0“><tr readability=„0“><td> <p> <h2>Contents</h2> </p> <li class=„toclevel-1 tocsection-1“>1 Overview <li class=„toclevel-1 tocsection-2“>2 Lawful Interception Requirements <li class=„toclevel-1 tocsection-3“>3 Intercepting Audio <li class=„toclevel-1 tocsection-4“>4 IRI records<li class=„toclevel-2 tocsection-5“>4.1 Types of IRI records <li class=„toclevel-2 tocsection-6“>4.2 Typical information found in an IRI record <li class=„toclevel-1 tocsection-7“>5 IRI records generating <li class=„toclevel-1 tocsection-8“>6 IRI records encoding <li class=„toclevel-1 tocsection-9“>7 IRI records values and files specification <li class=„toclevel-1 tocsection-10“>8 IRI records uploading to the agency <li class=„toclevel-1 tocsection-11“>9 Configuring Lawful Interception <li class=„toclevel-1 tocsection-12“>10 Lawful Interception Statistics <li class=„toclevel-1 tocsection-13“>11 IRI records decoding <li class=„toclevel-1 tocsection-14“>12 References </td> </tr></table><h2>Overview</h2> <div class=„thumb tright thumbinner c1“ readability=„5“> <div class=„thumbcaption“ readability=„6“> <div class=„magnify“></div> Schematic showing interception of a call already routed with a Tmedia</div> </div> Lawful Interception (process of intercepting a target's

conversation)

- Interception target (someone under investigation by law enforcement agency, and whom the agency wants to intercept calls)
- Law enforcement agency (an agency that has, by law, the power to request the interception of calls toward or from targets)
- A law enforcement agency sends, to the service provider, a list of targets to intercept (phone numbers)
- Service provider configures its equipment to intercept the targets, based on phone numbers
- When service provider equipment detect a call that involves a target to intercept, it
 - Forwards a copy of call audio (both directions) to the agency through forked calls (Content of Communication link (CC link) - a call toward the agency, carrying intercepted audio)
 - Sends information records ([IRI](https://docs.telcobridges.com/tbwiki/IRI "IRI") records) to the agency
- Telcobridges Lawful Interception implementation is based on specification ETSI ES 201 671 v2.1.1 (2001-09), and not CALEA, PCES, and ANSI T1.678

Lawful Interception Requirements

- Detecting target
 - Law enforcement agency provides a list of targets (Type of intercepted targets can be from: PSTN, ISDN, GSM (CS), TETRA, GPRS (PD), UMTS (CS))
 - LIID (Lawful Intercept Identifier, unique identifier assigned to a target by an agency) for the target
 - Phone number of the target
 - Start/end date and time for the interception
- Service provider updates targets in its equipment and equipment detect a matching calling or called number, and activates the interception
- Intercepting targets
 - In a call, each call leg can be an interception target
 - When a leg is an interception target, it's intercepted:
 - Audio &&from&&; this leg is forked to a new outgoing call
 - Audio &&to&&; this leg is forked to a new outgoing call
 - [IRI](https://docs.telcobridges.com/tbwiki/IRI "IRI") records are generated for this interception
 - Intercepting multiple targets
 - Both legs may be independently and simultaneously intercepted
 - 2 pairs of forked audio outgoing calls
 - 2 sets of [IRI](https://docs.telcobridges.com/tbwiki/IRI "IRI") records
- Intercepting Audio
- For each direction (audio &&from&& and &&to&& the target):
 - A new outgoing call leg is made, toward the agency
 - Audio is &&forked&& (half-duplex joined)
 - These outgoing call legs are made toward:
 - An outgoing NAP explicitly assigned to the agency
 - optionally, using specified calling/called numbers
 - Forking does NOT require DSPs
 - Audio forking is done as soon as possible
 - Immediately for the audio &&from&& the target (this may include even the ring back tone, or may include audio from incoming call during ringing)
 - Upon joining with other active leg for the audio &&to&& the target

IRI records

The call data (known as Intercept Related Information or [IRI](https://docs.telcobridges.com/tbwiki/IRI "IRI") in Europe and Call Data or CD in the US) consists of information about the targeted communications, including destination of a voice call (e.g., called party's telephone number), source of a call (caller's phone number), time of the call, duration, etc. Intercept Related Information record (IRI record) is a CDR-style record that contains IRI information on an intercepted call

Types of IRI records

- IRI-BEGIN: Indicate that the interception is starting at first event of the communication attempt, opening the IRI transaction
- IRI-CONTINUE: Indicate call state change at any time during the communication attempt within the IRI transaction
- IRI-END: Indicate the end of the interception at the end of the communication attempt, closing the IRI transaction
- IRI-REPORT: General use for any non-communication related events

For information related to an existing communication case, the record types 1 to 3 shall be used. They form an IRI transaction for each communication case or communication attempt, which corresponds directly to the communication phase (set-up, active or release).

For some packet oriented data services such as GPRS, the first event of a communication attempt shall be the Packet Data Protocol (PDP) context activation or a similar event and an IRI-BEGIN record shall be

issued. The end of the communication attempt shall be the PDP context deactivation or a similar event and an IRI-END record shall be issued. While a PDP context is active, IRI-CONTINUE records shall be used for CC relevant IRI data records, IRI-REPORT records otherwise.

Record type 4 is used for non-communication related subscriber action, like Subscriber Controlled Input (SCI) for service activation. For simple cases, it can also be applicable for reporting unsuccessful communication attempts.

The record type is an explicit part of the record. The 4 record types are defined independently of target communication events. The actual indication of one or several communication events, which caused the generation of an IRI record, is part of further parameters within the record's information content. Consequently, the record types of the IRI transactions are not related to specific messages of the signalling protocols of a communication case, and are therefore independent of future enhancements of the intercepted services, of network specific features, etc. Any transport level information (i.e. higher-level services) on the target communication-state or other target communication related information is contained within the information content of the IRI records.

For some packet oriented data services such as GPRS, if Lawful Interception (LI) is being activated during an already established PDP context or similar, an IRI-BEGIN record will mark the start of the interception. If LI is being deactivated during an established PDP context or similar, no IRI-END record will be transmitted. The end of interception can be communicated to the LEA by other means Handover Interface Port 1 (for Administrative Information)(HI1) (whereas Handover Interface Port 2 (HT2) transports IRI information and Handover Interface Port 3 (HT3) transports Content of Communication information).

Typical information found in an IRI record

- Record type (Start, Continue, End, Report)
- LIID
- CIN (communication identity number)
- Operator identifier
- Direction (target is originating, or terminating)
- Call state (idle, setup, connected)
- Duration of ring and conversation states
- Calling / called party numbers
- Release reason
- CC link state (setup, active, released, lack of resources)
- CC link release reason

IRI records generating

- IRI records are generated at various states of the interception
- They provide information on the interception, and call state
- In a call, each call leg can be an interception target
- When a leg is an interception target, it's intercepted:
 - Audio from; this leg is forked to a new outgoing call toward the agency
 - Audio to; this leg is forked to a new outgoing call toward the agency
 - IRI records are generated for this interception
- Both legs may be independently and simultaneously intercepted
 - 2 pairs of forked audio outgoing calls
 - 2 sets of IRI records

IRI records encoding

- IRI records are encoded in ASN.1 (a binary encoding standard that is used by IRI records) format and using the basic encoding rules (BER).
- ASN.1 IDs and objects hierarchy for encoding IRI records is provided by ETSI specifications

IRI records values and files specification

- IRI records values can be
 - Mandatory in each record
 - In one record only for the whole call
 - optional (in some records only, or none at all)
- IRI record files can
 - Contain only one IRI record (one file per record)
 - Contain multiple IRI records (grouped)

IRI records uploading to the agency

- As files, using the FTP protocol
- Telcobridges also supports SFTP as file transfer method

Configuring Lawful Interception

- Configure Lawful Agencies
 - Summary of information required
 - NAP to use for CC links
 - FTP (or SFTP) server info (IP, port, user, password, folder)
 - IRI upload mode (per record, grouped)
 - Multiple agencies can be configured
 - Note: SFTP requires password-less login to be configured (through exchange of keys between servers)
 - Provide the list of intercepted targets
 - The list of intercepted targets is provided as a CSV file
 - Uploaded in the <<File DB>> section of the Web Portal
 - Required columns:
 - liid
 - number
 - Optional columns
 - start
 - end
 - Example


```
liid,number,start,end John Smith,555-0001,2012-10-24T00:00:00-05:00,2012-10-24T23:59:59-05:00
```

Joe Dalton,333-3007,2012-01-01T00:00:00-05:00,2012-12-31T23:59:59-05:00 Ben
Laden,022-44-66-33-11 Ben Yi,450-621-1990 </pre> <a
href=„https://docs.telcobridges.com/tbwiki/Toolpack:Enable_Lawful_Interception_in_Routing_Script_B“
title=„Toolpack:Enable Lawful Interception in Routing Script B“>Enable Lawful Interception in a
Routing Scripts (<a
href=„https://docs.telcobridges.com/tbwiki/Toolpack:Enable_Lawful_Interception_in_Routing_Script_A“
title=„Toolpack:Enable Lawful Interception in Routing Script A“>For Toolpack 2.7) The
<<lawful interception>> routing script filter is provided with toolpack Users only
need to <<include>> it in their current routing script
 <pre>
require 'lawful_intercept' (...)

```
include LawfulIntercept
```

(...)

```
after_filter :method =&gt; :enable_lawful_intercept
```

</pre> For more information on Routing Scripts, please see <a
href=„https://docs.telcobridges.com/tbwiki/Routing_script_tutorial:Mini_Development_Guide“
title=„Routing script tutorial:Mini Development Guide“>mini development guide
<h2>Lawful Interception Statistics</h2> Live statistics and statistics history
The Web Portal provides Lawful Interception statistics Global Per
agency Available statistics are Total / current intercepted calls
Total IRI records generated Total IRI records dropped Total failed
interceptions IRI records upload queue length and state ... and a few more
 <h2>IRI records decoding</h2> <p>As IRI record is encoded in ASN.1
format, some online ASN.1 decoders are also available to check the IRI record. Upload a
message/PDU/record file, and the decoded data can be downloaded as a text file in the ASN.1 Value
Notation format.</p><h2>References</h2> <a rel=„nofollow“ class=„external text“
href=„http://en.wikipedia.org/wiki/Lawful_interception“>Wikipedia lawful intercept article
<a rel=„nofollow“ class=„external text“ href=„<http://cryptome.org/espy/ES201-671-v211.pdf>“>ETSI ES 201 671 V2.1.1 (2001-09) - Cryptome <a rel=„nofollow“
class=„external text“ href=„<http://asn1-playground.oss.com/>“>ASN.1 Playground - learn, play,
test <a rel=„nofollow“ class=„external text“
href=„<https://www.marben-products.com/asn.1/services/decoder-asn1-security.html>“>Free Online
Security ASN.1 Messages Decoder <a rel=„nofollow“ class=„external text“
href=„<https://holtstrom.com/michael/tools/asn1decoder.php>“>ASN.1 decoder
</html>

From:
<https://schnipsl.qgelm.de/> - Qgelm

Permanent link:
<https://schnipsl.qgelm.de/doku.php?id=wallabag:lawful-interception---tbwiki>

Last update: **2021/12/06 15:24**

