

**Lawful Interception (LI);
Handover Interface and
Service-Specific Details (SSD) for IP delivery;
Part 5: Service-specific details for IP Multimedia Services**



Reference

RTS/LI-00072-5

Keywords

IMS, IP, Lawful Interception, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2010.
All rights reserved.

DECT[™], **PLUGTESTS**[™], **UMTS**[™], **TIPHON**[™], the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPP[™] is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

LTE[™] is a Trade Mark of ETSI currently being registered

for the benefit of its Members and of the 3GPP Organizational Partners.

GSM[®] and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	5
Foreword.....	5
Introduction	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	7
3 Definitions and abbreviations.....	7
3.1 Definitions	7
3.2 Abbreviations	8
4 General	9
4.1 Reference Model for Lawful Interception	9
4.2 Reference system model.....	10
4.2.1 Network layer Interception	10
4.2.2 Service layer Interception	11
4.3 General Requirements	12
5 Interception of IP Multimedia services	12
5.1 Identification of target of interception.....	12
5.1.1 SIP Target Identification.....	12
5.1.2 H.323 Target Identification.....	12
5.2 Interception of signalling.....	13
5.2.1 Provisioning of the SIP IRI IIF.....	13
5.2.2 Provisioning of the H.323 IRI IIF.....	13
5.3 Assigning a value to the Communication Identity Number	13
5.3.1 Assigning a CIN value to SIP related IRI.....	13
5.3.2 Assigning a CIN value to H.323 related IRI.....	14
5.4 Events and IRI record types	14
5.5 Interception of Content of Communication.....	15
6 Handover Interface	15
6.1 Intercepted Related Information.....	15
6.2 Correlation of IRI and CC	16
7 ASN.1 specification for IRI and CC.....	16
Annex A (informative): Interception using H.248	19
A.1 Purpose of this annex	19
A.2 Notes on interception using H.248	19
A.2.1 Target identification (see also clause 5.1)	19
A.2.2 Provisioning of the H.248 IRI IIF (see also clause 5.2)	20
A.3 Problems in H.248 interception.....	20
A.3.1 Missing information in H.248 signalling.....	20
A.3.2 Missing call content.....	21
Annex B (normative): Minimum set of functional attributes to be provided.....	22
B.1 General requirements	22
B.2 Result of interception	23
B.3 Location information.....	23
B.4 Time constraints	23

B.5	Technical handover interfaces and format requirements.....	24
Annex C (informative):	Change request history.....	25
History		26

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://webapp.etsi.org/IPR/home.asp>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Lawful Interception (LI).

The present document is part 5 of a multi-part deliverable. Full details of the entire series can be found in part 1 [2].

The ASN.1 module is also available as an electronic attachment to the original document from the ETSI site (see details in clause 7).

Introduction

The present document focuses on Lawful Interception of IP Multimedia Services. It is to be used in conjunction with TS 102 232-1 [2], in which the handling of the intercepted information is described.

1 Scope

The present document specifies interception of Internet Protocol (IP) Multimedia (MM) Services based on the Session Initiation Protocol (SIP) and Real Time Transport Protocol (RTP) and Message Session Relay Protocol (MSRP) and IP MM services as described by the ITU-T Recommendations H.323 [6] and H.248 [7].

The present document is consistent with the definition of the Handover Interface, as described in TS 102 232-1 [2].

The present document does not override or supersede any specifications or requirements in 3GPP TS 33.108 [9] and TS 101 671 [1].

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
 - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
 - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at <http://docbox.etsi.org/Reference>.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

- [1] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

NOTE: Periodically TS 101 671 is published as ES 201 671. A reference to the latest version of the TS as above reflects the latest stable content from ETSI/TC LI.

- [2] ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".
- [3] ITU-T Recommendation X.680: "Information Technology - Abstract Notation One (ASN.1): Specification of basic notation".
- [4] IETF RFC 3261: "SIP: Session Initiation Protocol".
- [5] IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications".
- [6] ITU-T Recommendation H.323: "Packet-based multimedia communications systems".

[7] ITU-T Recommendation H.248: "Gateway control protocol".

NOTE: H.248 was renumbered when revised on 2002-03-29. H.248 main body, Annexes A to E and Appendix I were included in H.248.1. Subsequent annexes were sequentially numbered in the series, e.g. H.248 Annex F became H.248.2.

[8] Void.

[9] ETSI TS 133 108: "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108)".

[10] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[11] ATIS-PP-1000678.2006: "Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunication Networks", Version 2 (Revision of ANS T1.678-2004).

[12] ITU-T Recommendation H.225.0: "Call signalling protocols and media stream packetization for packet-based multimedia communication systems".

[13] ITU-T Recommendation H.245: "Control protocol for multimedia communication".

[14] IETF RFC 4566: "SDP: Session Description Protocol".

[15] IETF RFC 4975: "The Message Session Relay Protocol (MSRP)".

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] ETSI TR 102 528: "Lawful Interception (LI); Interception domain Architecture for IP networks".

[i.2] ETSI TR 102 503: "Lawful Interception (LI); ASN.1 Object Identifiers in Lawful Interception and Retained data handling Specifications".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 101 671 [1], TS 102 232-1 [2] and the following apply:

context: logical collection of H.248 terminations

IP MultiMedia service: multimedia service that utilizes the Internet Protocol (IP) for the transport of data

MultiMedia (MM): use of computers to present text, graphics, video, animation, and sound in an integrated way

MultiMedia service: communication service that offers Multimedia communication to end-users

termination: entity in H.248 that acts as a source or sink of media. Terminations may be physical, such as a given channel on a TDM line, or ephemeral, such as an IP endpoint

TSAP identifier: piece of information used to multiplex several transport connections of the same type on a single H.323 entity with all transport connections sharing the same Network Address (e.g. the port number in a TCP/UDP/IP environment)

NOTE: Transport layer Service Access Point (TSAP) identifiers may be (pre)assigned statically by some international authority or may be allocated dynamically during the setup of a call. Dynamically assigned TSAP identifiers are of transient nature, i.e. their values are only valid for the duration of a single call.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AF	Administration Function
ASN.1	Abstract Syntax Notation One
CC IIF	CC Internal Interception Function
CC	Content of Communication
CCCI	Content of Communication Control Interface
CCTF	Content of Communication Trigger Function
CCTI	Content of Communication Trigger Interface
CID	Communication IDentifier
CIN	Communication Identity Number
CLI	Calling Line Identity
CSP	Communications Service Provider (covers all AP/NWO/SvP)
DTMF	Dual Tone Multi Frequency
GW	GateWay
HI1	Handover Interface 1 (for Administrative Information)
HI2	Handover Interface 2 (for Intercept Related Information)
HI3	Handover Interface 3 (for Content of Communication)
IAP	Internet Access Provider
ID	Identity
IF	Interception Function
IIF	Internal Interception Function
INI	Internal Network Interface
IP	Internet Protocol
IRI IIF	IRI Internal Interception Function
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIAF	Lawful Interception Administration Function
LIID	Lawful Interception IDentifier
MF	Mediation Function
MG	Media Gateway
MGC	Media Gateway Controller
MM	MultiMedia
MSRP	Message Session Relay Protocol
PDU	Protocol Data Unit
RTCP	RTP Control Protocol
RTP	Realtime Transport Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SvP	Service Provider
TCP	Transmission Control Protocol
TDM	Time Division Multiplex
TSAP	Transport layer Service Access Point
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

4 General

4.1 Reference Model for Lawful Interception

The present document adopts the generic reference model for the interception domain from TR 102 528 [i.1], its internal intercept functions, Intercept Related Information Interception Function (IRI IIF), Content of Communication Trigger Function (CCTF), and Content of Communication Internal Interception Function (CC IIF), and the Internal Network Interfaces INI1, INI2, INI3, Content of Communication Trigger Interface (CCTI) and Content of Communication Control Interface (CCCI) as shown in figure 1.

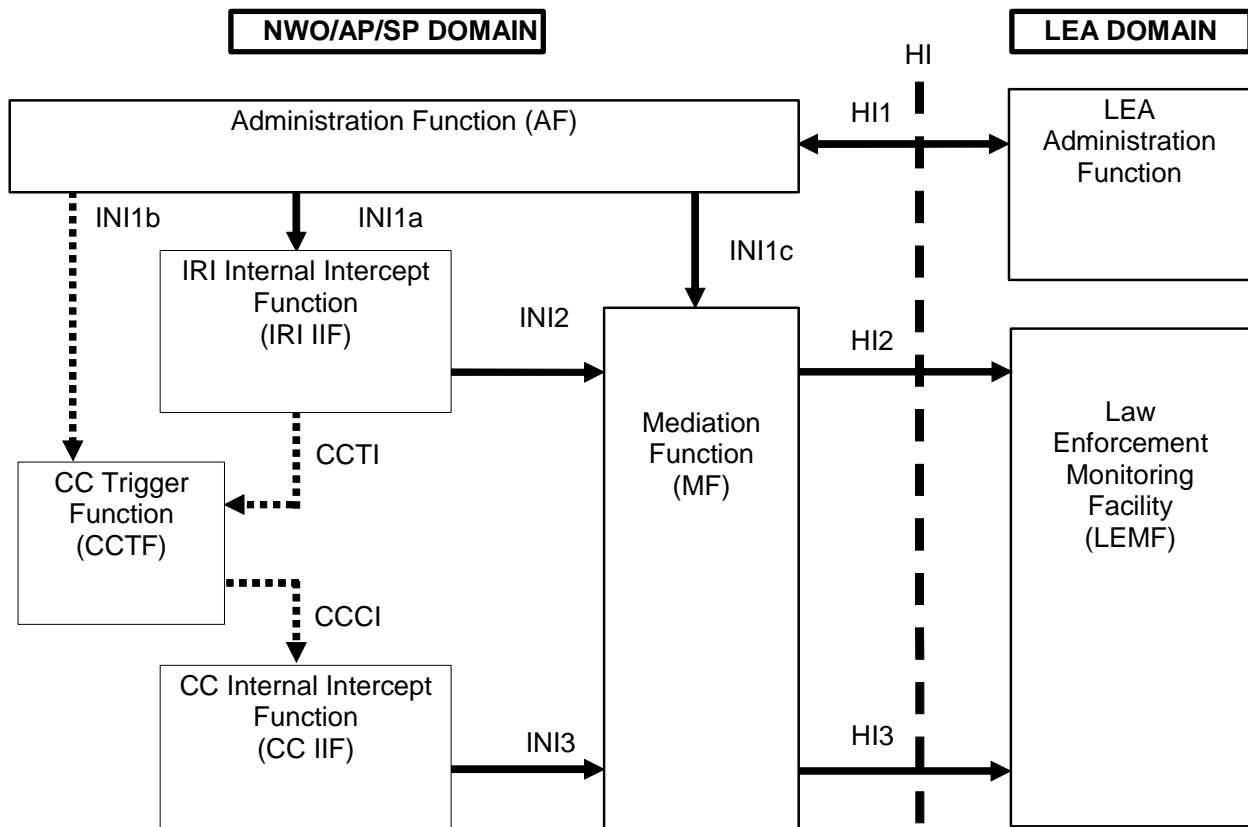


Figure 1: Reference Model for Lawful Interception

The reference model depicts the following functions and interfaces:

- INI1a provisions Intercept Related Information Internal Interception Function (IRI IIF).
- INI1b may (statically) provision Content of Communications Trigger Function (CCTF).
- INI1c provisions the Mediation Function (MF).
- Intercept Related Information Internal Interception Function (IRI IIF) generates IRI.
- Content of Communication Internal Interception Function (CC IIF) generates CC.
- Content of Communication Trigger Function (CCTF) controls CC IIF.
- Content of Communication Control Interface (CCCI) provisions CC IIF.
- Content of Communication Trigger Interface (CCTI) may trigger CCTF for provisioning of the CC IIF.
- Content of Communication Control Interface (CCCI) may dynamically provision the CC IIF.
- Internal interface INI1 carries provisioning information from LIAF to the Internal Intercept Functions (IIF).

- Internal interface INI2 carries Intercept Related Information (IRI) from IRI IIF to the MF.
- Internal interface INI3 carries Content of Communication (CC) information from CC IIF to the MF.

For an in-depth explanation of the functions and interface, is referred to clause 4 of TR 102 528 [i.1].

4.2 Reference system model

The reference system model applied in the present document, as depicted in figure 2, provides a simplified model of a technology independent, IP MultiMedia (MM) service platform, access by multiple different access networks. The access networks may provide different forms of network access, using different technologies; they all have in common that they provide IP connectivity among end-users and between end-users and the IP MM services provided by the IP MM service platform.

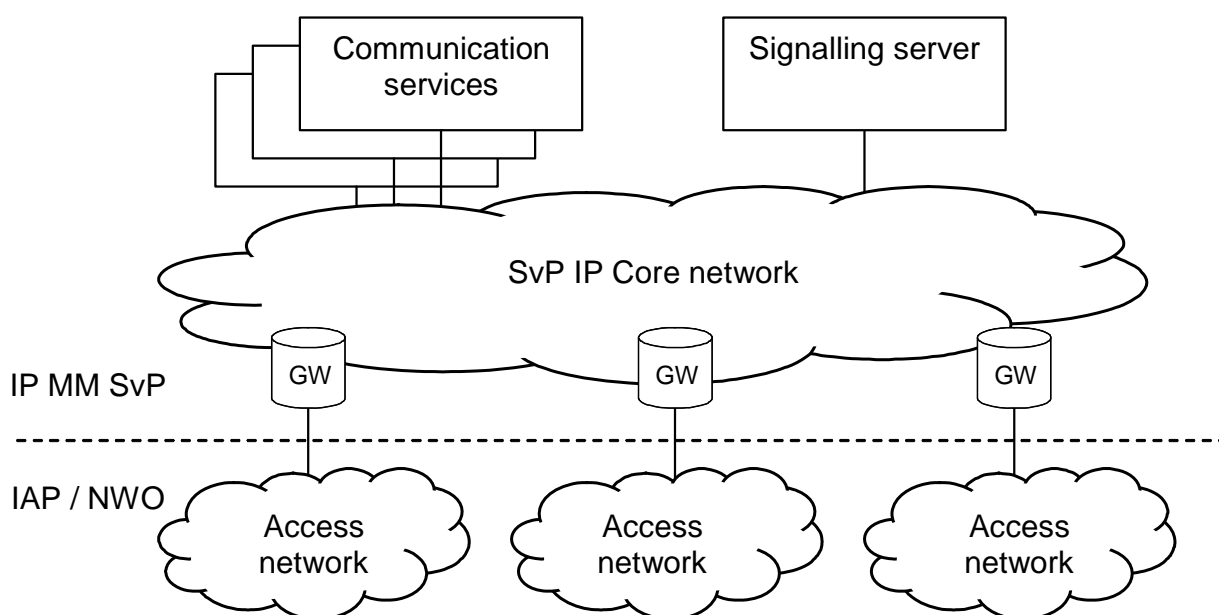


Figure 2: Reference System Model

Access from the access networks into the IP Core network of the IP MM service provider is assumed to be protected by some gateway device (e.g. a session border controller, border gateway controller or a firewall/router combination).

The IP MM Service platform contains a signalling server that provides session initiation functionality (e.g. a SIP call manager or an H.323 gatekeeper) among end-users and between end-users and communication services (e.g. unified messaging, audio or video conference servers).

4.2.1 Network layer Interception

Network Layer interception requires a copy of all signalling information as well as call content exchanged in the platform to be available at a central point in the infrastructure.

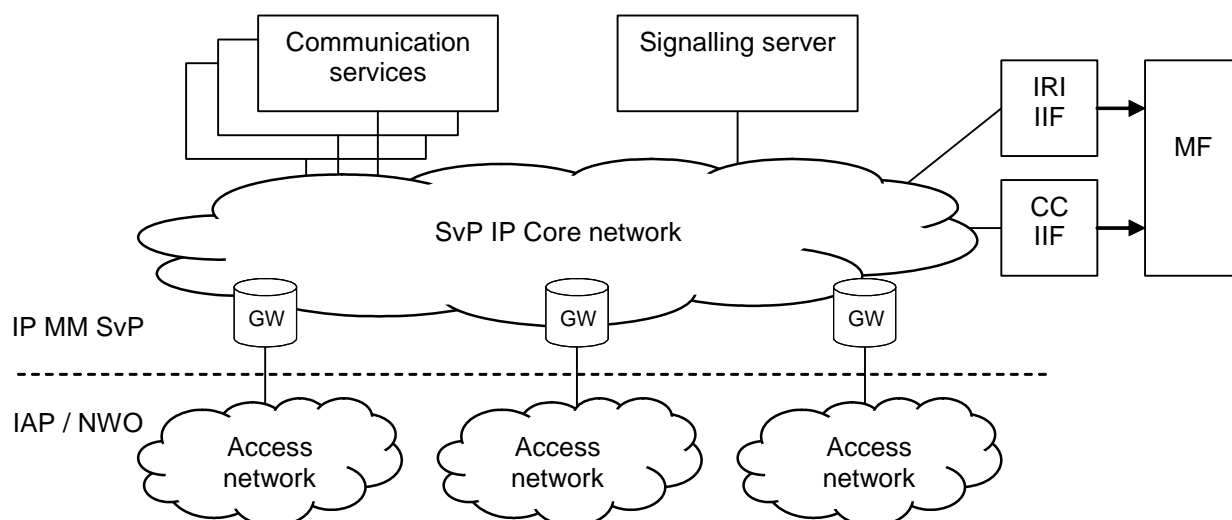


Figure 3: Network layer Interception Model

This can be achieved by means of span-ports in the layer 2 switching backbone or by means of passive splitters (either copper or fibre) at strategic points in the SvP's core network. Either way, due to the bandwidth of copied network traffic, some form of filtering will most likely be required (e.g. by means of a layer 3 switch).

4.2.2 Service layer Interception

Service Layer interception requires LI interfaces and functionality to be available in both the signalling server and the gateways.

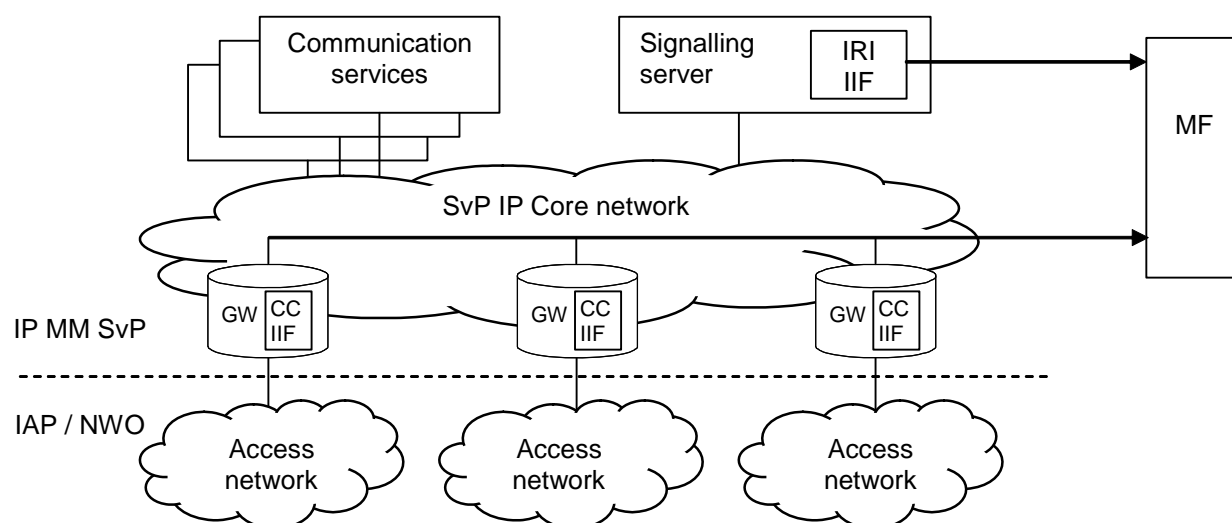


Figure 4: Service layer Interception Model

Typically the IRI IIF in the signalling server is provisioned with the target ID. At detection of a session setup for a target, the IRI IIF will provide the IRI for the intercepted session and may provide session information to be used for ad-hoc provisioning of the gateway devices. In some implementations, the gateway devices are also provisioned with the target ID beforehand and are capable of detecting sessions independent from the signalling server.

4.3 General Requirements

The following requirements regarding the interception of signalling shall apply:

- 1) Annex B provides the functional description of the minimal set of information that is to be provided to Law Enforcement for each intercepted communication.
- 2) The present document supports the interception of communication services defined in the following IETF/ITU-T standards and recommendations:
 - RFC 3261 [4] (SIP);
 - RFC 3550 [5] (RTP);
 - RFC 4975 [15] (MSRP);
 - RFC 4566 [14] (SDP);
 - ITU-T Recommendation H.323 [6];
 - ITU-T Recommendation H.225.0 [12];
 - ITU-T Recommendation H.245 [13].
- 3) Any deviation from the supported IETF and ITU-T specifications identified in item 2, e.g. vendor specific parameters, shall be agreed in advance between the Communications Service Provider (CSP) and Law Enforcement Agency (LEA).
- 4) The present document specifies the handover of intercepted signalling containing all information required in TS 101 331 [10] by encapsulating that intercepted signalling.
- 5) IRI that is not part of intercepted signalling shall also be delivered. The format of such information on the handover interface shall be agreed in advance between the CSP and LEA.
- 6) As a national option, mapping of the IRI information onto specific messages at the handover interface may be mandated, e.g. according to the ANS T1.678 [11] specification.

5 Interception of IP Multimedia services

5.1 Identification of target of interception

5.1.1 SIP Target Identification

The target identity is not a network layer or transport layer address. The target identity shall be an address type that uniquely identifies the target in the CSP's network and by means of which sessions among users can be established, such as:

- TEL URI;
- SIP URI;
- E.164 Number.

5.1.2 H.323 Target Identification

The target identity is not a network layer or transport layer address. The target identity shall be an address type that uniquely identifies the target in the CSP's network and by means of which sessions among users can be established, such as:

- H.323 URL;

- H.323 ID;
- E.164 Number.

5.2 Interception of signalling

5.2.1 Provisioning of the SIP IRI IIF

SIP messaging RFC 3261 [4] is reported as Intercept Related Information (IRI) for the interception of multi-media service. All SIP messages executed on behalf of a target subscriber are subject to interception at the IRI Internal Interception Function (IIF). Based upon network configuration, the Administration Function (AF) shall provision IRI IIF with SIP Uniform Resource Identifier (URI) or TEL Uniform Resource Locator (URL) target identifiers. These resulting intercepted SIP messages shall be sent to the Mediation Function (MF) over the INI2 interface for mediation prior to transmittal across the HI2 interface.

5.2.2 Provisioning of the H.323 IRI IIF

H.323 call signalling, call control and subscriber controlled input messages are reported as Intercepted Related Information (IRI) for the interception of multi-media services. H.323 call signalling and control messages refer to the basic call signalling (H.225.0), call control (H.245) and those messages required for the signalling of supplementary services (i.e.: H.450.x). Subscriber controlled input messages refer to those messages generated as a result of user procedures for the control of Supplementary Services (activation/deactivation/interrogation).

All H.323 call signalling, call control and subscriber controlled input messages that are transmitted on behalf of the target subscriber are subject to intercept at the IRI IIF. Based upon the network configuration, the AF shall provision IRI IIF with either a H.323 Unique Resource Locator (H.323-URL), or a H.323 Identity (H.323-ID), or a public E.164 telephone number.

If available events related to the Registration, Administration and Status (i.e. H.323 RAS) of the target subscriber's terminal equipment are also subject to intercept at the IRI IIF.

5.3 Assigning a value to the Communication Identity Number

In order to produce useful IRI records from events, the IRI and CC records of a communication session must be correlated with a single value for the Communication Identity Number (CIN) field. The CIN should be assigned upon first IRI or CC message.

5.3.1 Assigning a CIN value to SIP related IRI

All IRI events resulting from SIP messages in a single call signalling leg (i.e. with an identical value for the SIP field "Call-ID") will be assigned the same value for the CIN. A call may consist of two or more call signalling legs (e.g. when communicating via a SIP proxy). The various related call signalling legs are matched using the O field in the RFC 4566 [14] SDP part of the SIP messages; call legs with an identical O field will be assigned the CIN value of the active session from which they are spawned.

This is depicted in figure 5, where *all* resulting IRI-Event are assigned the same CIN.

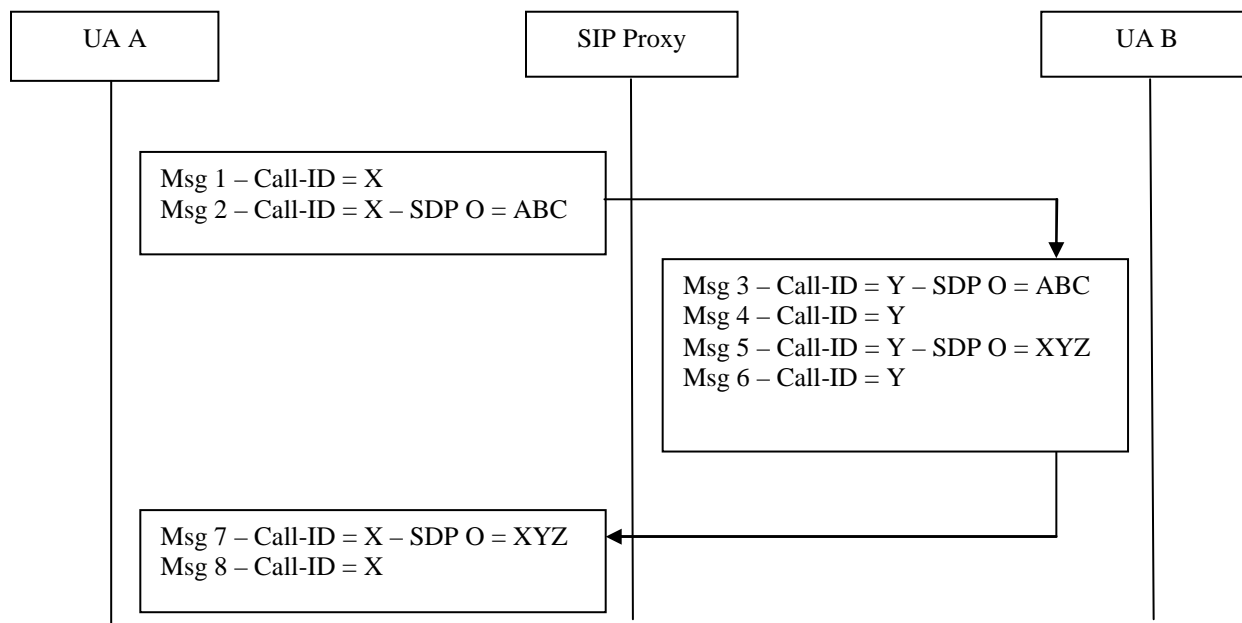


Figure 5: Relation between call signalling legs

5.3.2 Assigning a CIN value to H.323 related IRI

All IRI events resulting from messages within a single H.323 call will be assigned the same value for the CIN. Messages within a H.323 call can be identified as those messages containing, or associated with the same unique H.225.0 Call ID. The term H.323 Call is defined in the ITU-T Recommendation H.323 [6]. The term Call ID also referred to as H.225.0 Call ID and is described in the ITU-T Recommendations H.323 [6] and H.225.0 [12].

5.4 Events and IRI record types

The following requirements need to be met:

- All multimedia signalling and control messages to or from a targeted subscriber, and all multimedia signalling and control messages executed on behalf of or related to a targeted subscriber are intercepted by the IRI IIF and sent to the MF over the INI2 interface as IRI records.
- IRI records for all events related to a single communication session, which may consist of multiple media streams, that are being exchanged among the possibly more than two users, will be assigned the same CIN value.
- In addition, information on non-transmission related actions of a target constitute IRI is assigned CIN and is sent via HI2 (e.g. information on subscriber controlled input).

NOTE: This includes events related to the target service handled internally by network functions (e.g. communications among GWs, Signalling Servers and Communication Services). The format of such information on the handover interface should be agreed in advance between the CSP and LEA.

For each event, a record is sent to the LEMF. A new value for the CIN field is assigned if an event is detected that is not related to an already existing communication session. This event is reported as an IRI-REPORT or IRI-BEGIN record. Every subsequent record related to this communication session is reported as an IRI-REPORT or IRI-CONTINUE record. At the detection of the event that denotes the end of a session an IRI-REPORT or IRI-END record is sent.

In case of implementation issues, operational flaws or problems, events may need to be reported for a communication session for which the IRI-END record already has been sent. These events are reported as an IRI-REPORT with the proper value for the CIN.

Table 1 summarizes the mapping between event type and record type sent to the LEMF.

Table 1: Mapping between IP MM Events and IRI Records Type

Event	IRI Record Type
At assignment of a new CIN value	BEGIN/REPORT
All intermediate signalling, other than the last event	CONTINUE
The last event related to a communication session	END
Delayed IRI events related to an already ended session	REPORT
Events that are not mapped	REPORT
NOTE: Not mapped events could for example be encapsulated SIP messages.	

5.5 Interception of Content of Communication

The Content of Communication (CC) provided is a copy of the multimedia stream sent through the SvP's network that is addressed to, sent from or related to the targeted subscriber as described in the intercepted call signalling and call control information.

Multimedia stream consists in:

- every RFC 3550 [5] RTP and RTCP packet for real time multimedia services (e.g. VoIP),
- every RFC 4975 [15] MSRP packet for MSRP based multimedia services (e.g. instant messaging, file sharing, ...).

The RTP CC shall also contain the RTP header, UDP header and IP header, except by agreement between CSP and LEA (for example these headers may not be available at the point of interception).

The MSRP CC shall contain the TCP header.

The frameType field indicates which headers are present in a given CC stream.

In the case where the RTP header is unavailable, one may be inserted by the mediation function, subject to agreement between LEA and CSP. The addition of an inserted RTP header may aid processing the audio stream at the receiver.

IP and UDP or TCP headers shall not be inserted to the intercepted material by the mediation function if they are unavailable.

In addition to IRI messages, all RTP/RTCP or MSRP packets identified to be associated with a specific intercepted call or session shall be assigned the same CIN.

In case where some headers are not reported within the CC (because not available at the point of interception) there may be a need to identify the media streams inside the CC, typically in situations where the SIP communication consists in multiple media streams of same type. The streamIdentifier field identifies the media stream unambiguously (it may contain the corresponding SDP 'c=' and 'm=' lines for instance).

NOTE 1: The ASN.1 definition for CC is presented as the iPMultimediaPDU in clause 7.

NOTE 2: The CC also contains the target media streams that are not transferred via RTP or RTCP or MSRP (for example, those streams handled by a GW and not passing the core network). The format of such information on the handover interface should be agreed in advance between the CSP and LEA.

6 Handover Interface

6.1 Intercepted Related Information

The Communication Identity Number (CIN) is used to uniquely identify a communication session (as described in TS 102 232-1 [2] and TS 101 671 [1]). Applied to IP MM Services, a communication session refers to a single self contained transaction or a series of protocol data units that together form a self-contained communication such as a SIP or H.323 Session.

6.2 Correlation of IRI and CC

To assure correlation between the independently transmitted Content of Communication and the Intercepted Related Information (IRI) of an intercepted call the following parameters are used:

- Lawful Interception Identifier (LIID);
- Communication Identifier (CID).

NOTE: The target identifier may not necessarily be found in both communication content and interception related information.

In situations where the SIP communication consists of multiple media streams the streamIdentifier field of CC may be used to correlate each media stream of CC with the corresponding SDP media description of IRI.

7 ASN.1 specification for IRI and CC

The ASN.1 (ITU-T Recommendation X.680 [3]) module that represents the information in the present document and meets all stated requirements is shown below. TR 102 503 [i.2] gives an overview of the relevant Object Identifiers (OID) used in ASN.1 modules of the Lawful Intercept specifications and points to the specification where the modules can be found.

The ASN.1 definitions are in .txt file "IPMultimediaPRU, ver4.txt", contained in archive ts_10223205v020401p0.zip which accompanies the present document.

```
-- =====
-- Description of the IP Multimedia PDU
-- =====
```

IPMultimediaPDU

```
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) li-ps(5)
iPMultimedia(5) version4(4)}
```

```
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

```
IMPORTS
  -- from TS 101 671 [1]
  IPAddress
  FROM HI2Operations
  {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
version10(10)};
```

```
-- =====
-- Object Identifier Definition
-- =====
```

```
iPMIRIObjId RELATIVE-OID ::= {li-ps(5) iPMultimedia(5) version4(4) iRI(1)}
iPMCCObjId RELATIVE-OID ::= {li-ps(5) iPMultimedia(5) version4(4) cC(2)}
  -- both definitions relative to:
  -- {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2)}
```



```
-- =====
-- IP Multimedia Communications Contents
-- =====
```

```
IPMMCC ::= SEQUENCE
{
  iPMCCObjId          [0] RELATIVE-OID,
  mMCCContents       [1] OCTET STRING,
  -- Copy of the multimediasream, i.e. all related RTP/RTCP or MSRP packets
  -- Protocol of the multimedia packets is indicated by means of mMCCprotocol parameter
  -- mMCCContents was called rTPCCContents in earlier versions until v2.3.2.
  ...,
  frameType          [2] FrameType OPTIONAL,
  -- The availability of header information shall be signalled with the frameType parameter
  -- The module is defined as OPTIONAL because of backwards compatibility reasons
  -- For new implementations the module is MANDATORY to be used as defined in clause 5.5
  streamIdentifier   [3] OCTET STRING OPTIONAL,
  -- Used to identify the media stream within the current CIN, typically in case of
  -- multiple media streams communications
  -- May be used to correlate each media stream with the relevant SDP media description of IRI
  -- May contain c= and m= lines extracts for instance
  mMCCprotocol       [4] MMCCprotocol OPTIONAL
  -- Used to identify the protocol of packets sent in MMCCContent (RTP, MSRP, etc.)
  -- Absence means mMCCContents contains RTP/RTCP packets
}
```

```
FrameType ::= ENUMERATED
{
  ipFrame(0),
  -- All headers are present
  udpFrame(1),
  -- IP header is missing
  rtpFrame(2),
  -- UDP and IP headers are missing
  audioFrame(3),
  -- All headers are missing
  ...,
  tcpFrame(4)
  -- IP header is missing
}
```

```
MMCCprotocol ::= ENUMERATED
{
  rTP(0),
  -- mMCCContents parameter contains RTP/RTCP packets
  mSRP(1),
  -- mMCCContents parameter contains MSRP packets
  ...
}
```

```
-- =====
-- Intercept-related information for IP Multimedia sessions
-- =====
```

```
IPMMIRI ::= SEQUENCE
{
  iPMIRIObjId        [0] RELATIVE-OID,
  iPMIRIContents     [1] IPIRISContents,
  ...
}
```

```
IPIRISContents ::= CHOICE
{
  originalIPMMMessage [0] OCTET STRING,
  -- Copy of the IP MM signalling packet including the original IP and UDP/TCP headers
  sIPMessage          [1] SIPMessage,
  -- Copy of the SIP content and the source and destination IP address
  h323Message         [2] H323Message,
  -- Copy of the H.323 content and the source and destination IP address
  ...
}
```

```
SIPMessage ::= SEQUENCE
{
  iPSourceAddress      [0] IPAddress,
  iPDestinationAddress [1] IPAddress,
  sIPContent           [2] OCTET STRING,
  ...
}
```

```
H323Message ::= SEQUENCE
{
  iPSourceAddress      [0] IPAddress,
  iPDestinationAddress [1] IPAddress,
  h323Content          [2] H323MessageContent,
  ...
}
```

```
H323MessageContent ::= CHOICE
{
  h225CSMessageContent [0] OCTET STRING,
  h225RASMessageContent [1] OCTET STRING,
  h245MessageContent   [2] OCTET STRING,
  genericMessageContent [3] OCTET STRING,
  ...
}
```

END -- end of IP Multimedia PDU

Annex A (informative): Interception using H.248

A.1 Purpose of this annex

There are a number of problems with extracting useful IRI from H.248 signalling. These problems are largely due to the fact that H.248 is a gateway control protocol, not an end-to-end call initiation protocol like SIP or H.323. Often, useful information may be more easily extracted from other signalling links such as SIP, or from on-switch interception solutions. However, in certain circumstances it may be necessary to use the H.248 link. For example, for security or architecture reasons, it may be that the simpler options are not possible or acceptable. This annex provides some notes on how LI could be performed on a H.248 link (see clause A.2) and describes some of the problems and issues that arise (see clause A.3). It is not intended to be a complete or comprehensive description and solutions to the problems and issues are not presented.

A.2 Notes on interception using H.248

A.2.1 Target identification (see also clause 5.1)

H.248 messages typically do not contain authoritative target identifiers, such as E.164 phone numbers. Instead, they will typically contain termination and context identifiers. Hence, a probe provisioned with a list of target identifiers, and sniffing an H.248 link, will not be able to discriminate between target and non-target H.248 messages.

A possible solution would be to provide a mapping between authoritative identifiers such as E.164 numbers, and H.248 identifiers such as termination IDs. The MGC would provide the IF or MF with a list of the termination IDs in each MG it controls, and the corresponding authoritative identifier for each termination. This list of correspondences, along with the target list held by the IF or MF, would allow the IF to target H.248 transactions based on termination ID.

Information such as the IP endpoint for the RTP stream will be sent to a different termination. However, it will be in the same context as the target termination. Hence, it will be necessary for the probe to extract the relevant Context ID from any messages it intercepts by Termination ID, and intercept subsequent messages by this Context ID.

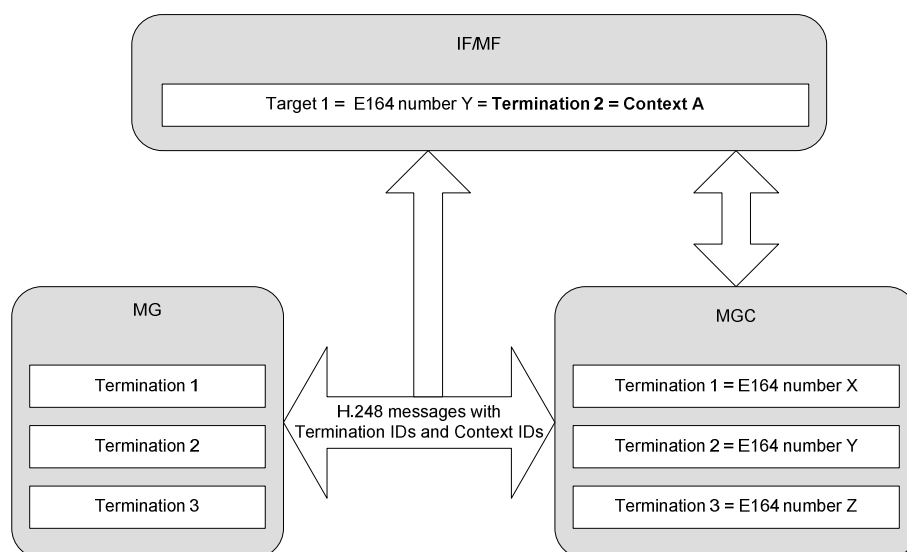


Figure A.1: Mapping of Authoritative Identifiers to Termination and Context Identifiers

There is still a problem with this method. There is no guarantee that the first termination to be added to a context will be the target physical termination. For example, the MGC may choose to add an ephemeral IP termination first, followed by the target termination. The IF will only intercept signalling after the target termination is added. Information contained in the first Add message is missed. This message may contain the IP endpoints and codec for the media stream, and so missing it means that the call content cannot be intercepted.

It is worth noting that typically, there is no advantage to adding the ephemeral termination first, and so H.248 implementations tend to add the physical termination at the same time as, or before, the ephemeral one.

The recommendation is therefore that:

- The IF will intercept H.248 signalling using a physical termination ID as an identifier.
- The IF will subsequently intercept any H.248 signalling to the same context as the physical termination.
- The MGC provides a mapping of authoritative identifiers to physical termination IDs.

The problems with this approach are:

- Any signalling to a context sent before a target termination is added to that context may be missed. This may mean important information such as details of the call content media stream are missed.

Other methods of identifying target H.248 transactions (for example, examining some other signalling link) are also possible.

A.2.2 Provisioning of the H.248 IRI IIF (see also clause 5.2)

For H.248, the IRI IIF is provisioned with a mapping between H.248 target identifiers and physical termination IDs. All H.248 signalling to and from a targeted termination is subject to interception. In addition, to retrieve information about the subsequent media path, any signalling sent to or from the same context as a targeted termination is also subject to interception.

A.3 Problems in H.248 interception

A.3.1 Missing information in H.248 signalling

In some circumstances, target H.248 messages may not contain all of the information an end user might expect. The following list shows what information may be missing:

- If a non-target calls a target, the non-target's number may be unavailable. A CLI signal may be used to discover the caller's number, but if there is no CLI package in place, or the user withholds their number, the calling number is unavailable.
- A failed attempt to call the target (because, for example, the target was busy) may not generate any target signalling, as the MGC will determine that the call cannot be made.
- If a target is called, the H.248 signalling gives no indication whether the call was made directly, or if the call was, for example, diverted or transferred to the target. If the call was diverted, there is no way of obtaining the original number (unless it is provided in some kind of package).
- Similarly, when a call is torn down, unless the target hung up, there is no indication of why the call ended.
- In some implementations, features such as call-holding or conference calling may be dealt with by a separate dedicated server (not the MGC). For example, a user may flash-hook, and be automatically redirected to a dedicated conferencing server, which would subsequently listen for the DTMF digits of the person the user wants to conference with. In this case, the digits the user dials are carried over the media stream to the conferencing server, rather than over H.248 signalling to the MGC. This number would only be found by analysing the call content afterwards.

A.3.2 Missing call content

Local call turnaround creates a problem in capturing the call media. If the call is turned around locally at a Media Gateway, then the RTP media stream is never presented to the IP network. Therefore no interception function in the IP network will be able to intercept the call media.

Annex B (normative): Minimum set of functional attributes to be provided

This annex provides the functional description of the minimal set of information that is to be provided to Law Enforcement for each intercepted communication.

The full law enforcement requirements are in TS 101 331 [10].

The present annex describes the requirements from a Law Enforcement Agency's (LEA's) point of view.

Not all requirements necessarily apply in one individual nation.

These requirements shall be used to derive specific network requirements and furthermore to standardize handover interfaces.

B.1 General requirements

- a) The obligation of the CSP as to which telecommunications traffic shall be intercepted is subject to national laws.
- b) In accordance with the relevant lawful authorization a CSP shall ensure that:
 - b.1) the entire content of communication associated with a target identity being intercepted can be intercepted during the entire period of the lawful authorization;
 - b.2) any content of communication associated with a target identity being intercepted which is routed to technical storage facilities or is retrieved from such storage facilities can be intercepted during the entire period of the lawful authorization;
 - b.3) the delivery of the intercept related information is reliable. If the intercept related information cannot be delivered immediately to the relevant LEMF, then the intercept related information shall be buffered until they can be delivered;
 - b.4) the delivery of the content of communication is reliable. If the content of communication cannot be delivered immediately to the relevant LEMF, then the content of communication shall be buffered if this is required by national laws;
 - b.5) the CSP shall not monitor or permanently record the results of interception.
- c) The ability to intercept telecommunications shall be provided relating to the interception subjects operating permanently within a telecommunications system (e.g. a subscriber or account).
- d) The ability to intercept telecommunications shall be provided relating to the interception subjects operating temporarily within a telecommunications system (e.g. a visiting mobile subscriber or a visiting subscriber using an access network to a home service).
- e) The results of interception relating to a target service shall be provided by the CSP in such a way that any telecommunications that do not fall within the scope of the lawful authorization shall be excluded by the CSP.

NOTE 1: It is assumed that the intercepting system exercises best effort to exclude non-authorized interception patterns (e.g. transferred communication).

- f) All results of interception provided at the handover interface shall be given a unique identification relating to lawful authorization.

NOTE 2: Information used for the IRI is expected to be part of standard network signalling procedures. No additional signalling is expected for the IRI.

B.2 Result of interception

The CSP shall, in relation to each target service:

- a) Provide the content of communication.
- b) Remove any service coding or encryption which has been applied to the content of communication (i.e. encipher) and the intercept related information at the instigation of the CSP.
- c) Provide the LEA with any other decryption keys whose uses include encryption of the content of communication, where such keys are available for CSP.
- d) Intercept related information shall be provided:
 - d.1) when communication is attempted;
 - d.2) when communication is established;
 - d.3) when no successful communication is established;
 - d.4) on change of status (e.g. in the access network);
 - d.5) on change of service or service parameter;
 - d.6) on change of location (this can be related or unrelated to the communication or at all times when the apparatus is switched on).
- e) Intercept related information shall contain:
 - e.1) the identities that have attempted telecommunications with the target identity, successful or not;
 - e.2) identities used by or associated with the target identity;
 - e.3) details of services used and their associated parameters;
 - e.4) information relating to status;
 - e.5) time stamps.
- f) The conditions mentioned above also apply to multi-party or multi-way telecommunication if and as long as the target identity participates.

B.3 Location information

An LEA may request location information relating to locations, in a number of forms: the current geographic, physical or logical location of the target identity. This information is expected to be made available from normal network operation.

B.4 Time constraints

- a) A CSP shall make the necessary arrangements to fulfil his obligation to enable the interception and delivery of the result of interception from the point in time when the telecommunication installation commences commercial service.
- b) The above requirement applies accordingly to the introduction of modifications to the telecommunication installation or to new operational features for existing telecommunications services to the extent of their impact on existing interception capabilities.
- c) When a lawful authorization is presented a CSP provider shall co-operate immediately.

- d) After a lawful authorization has been issued, provision of the results of interception of a target identity shall proceed on a real-time basis.

B.5 Technical handover interfaces and format requirements

- a) The configuration of the handover interface shall ensure that the quality of service of the telecommunications traffic provided at the handover interface is not inferior to that offered to the target service for each particular call.
- b) Each interception target shall be uniquely associated with a single instance of the handover interface. This could be achieved by separate channels or the use of identifiers.
- c) The correlation between the content of communication and intercept related information shall be unique.

Annex C (informative): Change request history

Status of present document: TS 102 232-5 Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Service; Handover specification for IP delivery		
Date	Version	Remarks
January 2007	2.1.1	First publication of the TS after approval by ETSI/TC LI#14 (30 January - 1 February 2007, Puerto de la Cruz). Version 2.1.1 prepared by Johan Bakker (KPN) (rapporteur V2.1.1)
October 2007	2.2.1	Included Change Requests: TS102232-05CR001 (cat D) IRI Record type TS102232-05CR002r2 (cat B) Clarification of use of RTP/UDP/IP headers These CRs were approved TC LI#16, 2-4 October 2007; Berlin version 2.2.1 prepared by Peter van der Arend (KPN) (chairman TC LI)
December 2007	2.2.2	Figure 5 was updated.
January 2008	2.3.1	Included Change Request: TS102232-05CR003r1 (cat B) on Media stream identification for correlation in case of multiple media streams communications This CR was approved TC LI#17, 22-24 January 2008, Como version 2.3.1 prepared by Peter van der Arend (KPN) (chairman TC LI)
July 2009	2.3.2	Included Change Request: TS102232-05CR004r2 (cat D) Clarification about CIN assignment This CR was approved by TC LI#21, 29 June – 1 July 2009, Sophia Antipolis; The ASN.1 definitions are contained in an .asn file (TS 102 232-5, IPMultimediaPRU, ver3.asn) which accompanies the present document. version 2.3.2 prepared by Peter van der Arend (Vodafone) (chairman TC LI)
February 2010	2.4.1	Included Change Request: TS102232-05CR005r1 (cat B) update to handle non-RTP bearers (MSRP) for new IMS services This CR was approved by TC LI#23, 9-11 February 2010, Rome. The ASN.1 definitions are contained in a .txt file (TS 102 232-5, IPMultimediaPRU, ver4.txt) which accompanies the present document. version 2.4.1 prepared by Peter van der Arend (Vodafone) (chairman TC LI)
Rapporteur of the present document is Mark Lastdrager (Pine Digital Security)		

History

Document history		
V2.1.1	February 2007	Publication
V2.2.1	November 2007	Publication
V2.2.2	December 2007	Publication
V2.3.1	April 2008	Publication
V2.3.2	October 2009	Publication
V2.4.1	April 2010	Publication