

**Access, Terminals, Transmission and Multiplexing (ATTM);  
Lawful Interception (LI);  
Part 1: Interception of IP Telephony Service on Cable  
Operator's Broadband IP Network: Internal Network Interfaces**

---



---

Reference

DTS/ATTM-02007-1

---

Keywords

access, cable, lawful interception

**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](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 2009.  
All rights reserved.

**DECT**<sup>TM</sup>, **PLUGTESTS**<sup>TM</sup>, **UMTS**<sup>TM</sup>, **TIPHON**<sup>TM</sup>, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

**3GPP**<sup>TM</sup> is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

**LTE**<sup>TM</sup> is a Trade Mark of ETSI currently being registered

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

**GSM**<sup>®</sup> and the GSM logo are Trade Marks registered and owned by the GSM Association.

---

# Contents

Intellectual Property Rights .....	4
Foreword.....	4
Introduction .....	4
1 Scope .....	5
1.1 Requirements notation.....	5
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 Requirements.....	9
5 Overview .....	10
6 Internal Cable Network Interfaces.....	11
6.1 Introduction .....	11
6.2 IN1 .....	11
6.3 IN2a .....	12
6.4 IN3 - Call Content (CC) of Communication Interface .....	12
6.4.1 Call Content Connection Identifier.....	13
6.4.2 Original IP Header.....	14
6.4.3 Original UDP Header.....	14
6.4.4 Original RTP Header .....	14
6.4.5 Original Payload .....	14
6.5 SBCF (SNMP based Configuration Function) .....	14
7 LI Cable Broadband IP Network Architecture .....	15
7.1 Dimensioning and Capacity .....	16
7.2 Elements of Cable Broadband IP Network.....	16
7.3 Functional Description .....	16
7.3.1 LI Process: Interception of IP Telephony Signalling.....	17
7.3.2 LI Process: interception of on-net calls.....	18
7.3.3 LI Process: interception of off-net calls.....	21
7.3.4 Details: interception of hairpin calls .....	23
8 Security.....	24
<b>Annex A (informative): Requirements listed in Council Resolution of 17 January 1995 .....</b>	<b>25</b>
History .....	27

---

## 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 Access, Terminals, Transmission and Multiplexing (ATTM).

NOTE: An earlier specification to the current document referring to Lawful Interception within a Cable Network was produced by ETSI Access and Terminals, subgroup AT-D (Digital).

The present document is part 1 of a multi-part deliverable covering Data Over Cable Systems, as identified below:

- Part 1: "**Interception of IP Telephony Service on Cable Operator's Broadband IP Network: Internal Network Interfaces**";
- Part 2: "Interception of IP Data Service on Cable Operator's Broadband IP Network: Internal Network Interfaces";
- Part 3: "Interception of email Service on Cable Operator's Broadband IP Network: Internal Network Interfaces".

---

## Introduction

The cable industry in Europe and across other global regions have already deployed broadband cable television Hybrid Fibre/Coaxial (HFC) IP data and telephony networks running the Cable Modem Protocol. The cable industry is in the rapid stages of implementing interfaces that provide the capabilities for Lawful Interception (LI) of these services in accordance with requirements of Law Enforcement Agencies.

The cable industry has recognized the urgent need to develop ETSI Technical Specifications aimed at developing interoperable interface specifications and mechanisms for LI of IP telephony communications services.

The present document specifies the Lawful Interception (LI) and implementation of IP Telephony services within a Cable Operators Broadband IP Network for the purpose of providing such intercepted information to Law Enforcement Agencies (LEAs).

# 1 Scope

The present document specifies the internal network interfaces to enable the Lawful Interception (LI) of IP telephony services over cable operators broadband IP Networks. The current document describes the LI functional elements and interfaces for both the NCS based and SIP protocol signalling architectures within a PacketCable™ network architecture framework.

The present document provides the requirements for the internal cable network interfaces and their functions for those network elements within a Cable Operators network that are involved in the production of the interception of call content and call related information relating to the interception target of IP Telephony communication services.

The provision of a LI interface for a Cable Operators Broadband IP Network is a national option, however where it is provided it shall be provided as described in the present document.

The structure of LI in telecommunications is in two parts: The internal interface of a network that is built using a particular technology; and, the external interface (known as the Handover Interface) that links the LEA to the network. Between these two parts is described a LI Mediation Device (MD) whose functions cater for managing and provisioning the network elements for interception as well as national variances and delivery of the result of interception. The administration of LI is a function that is typically integrated within the manufacturer's MD but may also be a separate device. For the purpose of the current document the administration function is assumed as integrated within the MD.

The subject of the present document is the internal network LI interfaces that lies between the elements of a Cable Operators IP Broadband infrastructure and the functions of the MD.

The Handover Interface is out of scope of the present document. The current document assumes the delivery requirements specified by ETSI Technical Committee Lawful Intercept (TC LI), ES 201 671 [2], TS 101 671 [3] and TS 102 232 [4]. In addition the Handover Interface may be the subject of national regulation and therefore the function of the mediation device for delivery of the intercepted information to the LEA may also be a matter of national regulation.

Systems that use SIP based on Packet Cable™ 2.0 is out of scope of the present document.

## 1.1 Requirements notation

If the present document is implemented, the key words "MUST" and "SHALL" as well as "REQUIRED" are to be interpreted as indicating a mandatory aspect of the present document. The keywords indicating a certain level of significance of a particular requirement that are used throughout the present document are summarized below.

<b>MUST</b>	This word or the adjective "REQUIRED" means that the item is an absolute requirement of the present document.
<b>MUST NOT</b>	This phrase means that the item is an absolute prohibition of the present document.
<b>SHOULD</b>	This word or the adjective "RECOMMENDED" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
<b>SHOULD NOT</b>	This phrase means that there may exist valid reasons in particular circumstances when the listed behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
<b>MAY</b>	This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

---

## 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] Council Resolution of 17 January 1995 on the lawful interception of telecommunications.
- [2] ETSI ES 201 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".
- [3] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".
- [4] ETSI TS 102 232: "Lawful Interception (LI); Handover specification for IP delivery".
- [5] ETSI TS 101 909-4: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 4: Network Call Signalling Protocol [Partial Endorsement of ITU-T Recommendation J.162 (11/2005), modified]".
- [6] IETF RFC 3261: "SIP: Session Initiation Protocol".
- [7] CableLabs PKT-SP-EM1.5-I03-070412: "Event Messages", April 12 2007.
- [8] IETF RFC 768/STD0006 (August 1980): "User Datagram Protocol".
- [9] IETF RFC 1305: "Network Time Protocol (Version 3) Specification, Implementation and Analysis".
- [10] IETF RFC 2327 (April 1998): "SDP: Session Description Protocol".
- [11] IETF RFC 791/STD0005 (September 1981): "Internet Protocol".
- [12] IETF RFC 1889 (January 1996): "RTP: A Transport Protocol for Real-Time Applications".
- [13] IETF RFC 1890 (January 1996): "RTP Profile for Audio and Video Conferences with Minimal Control".
- [14] CableLabs PKT-SP-ES-INF-I04-080425: "Electronic Surveillance Intra-Network Specification, April 25, 2008".
- [15] Void.

- [16] ETSI ES 201 158: "Telecommunications security; Lawful Interception (LI); Requirements for network functions".
- [17] CableLabs PKT-SP-ESP1.5-IO2-070412: "Electronic Surveillance".
- [18] IETF RFC 3924: "Cisco Architecture for Lawful Intercept in IP Networks".

## 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] PacketCable 1.5 Security Specification, PKT-SP-SEC1.5-IO2-070412, April 12, 2007, Cable Television Laboratories, Inc.
- [i.2] PacketCable 1.5 Network-Based Call Signaling Protocol Specification, PKT-SP-NCS1.5-IO3-070412, April 12, 2007, Cable Television Laboratories, Inc.
- [i.3] PacketCable 1.5 Audio/Video Codecs Specification, PKT-SP-CODEC1.5-IO2-070412, April 12, 2007, Cable Television Laboratories, Inc.
- [i.4] ETSI TR 102 661: "Lawful Interception (LI); Security framework in Lawful Interception and Retained Data environment".
- [i.5] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

---

## 3 Definitions and abbreviations

### 3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

**cable modem:** layer two termination device that terminates the customer end of the J.112 connection

**hair-pin call:** call that is targeted to a customer on the cable network that has forwarding enabled to a line which is on a different network

**on-net call:** call that is initiated by a customer on the cable network targeted to and delivered to a customer on the same cable network

**off-net call:** call that is initiated by a customer on the cable network and targeted to a customer on another network, or call that is initiated by a customer on another network and targeted and terminated by a customer on the cable network

## 3.2 Abbreviations

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

AP	Access Provider
CC	Call Content
CCC	Communication Call Content
CMTS	Cable Modem Termination System
CRD	Call Related Details
DA	Destination Address
EM	Event Message
GW	Gateway
HFC	Hybrid Fiber Coax
HI	Handover Interface
IAP	Intercept Access Point
IETF	Internet Engineering Task Force
IIF	Internal Intercept Function
INI	Internal Network Interface
IP	Internet Protocol
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIID	LI Identity
LIMD	Lawful Intercept Mediation Device
MAC	Media Access Control
MD	Mediation Device
MF	Mediation Function
MG	Media Gateway
MGC	Media Gateway Controller
MIB	Management Information Base
NCS	Network-based Call Signalling
NWO	Network Operator
QoS	Quality of Service
RTP	Real Time Protocol
SBCF	SNMP Based Configuration Function
SD	Signalling Device
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SvP	Service Provider
TAP	Tapping
TDM	Time Division Multiplexing
USM	User-based Security Module
VACM	View-based Access Control Module



---

## 4 Requirements

European cable operators are required to have the capability of intercepting messages passed over their networks system in any form. This capability should be covert, not affect the operation of the system in any discernible way or be detectable by the end user. Therefore, a European implementation for a Cable Broadband IP network should include the following functionality:

- a) the network equipment needs to be capable of copying all Communication Call Content (CCC) being carried to and from specified target addresses to an additional delivery address specified by the network operator;
- b) in the short term, for practical reasons, identification of voice related calls (including fax and modem calls) may use E.164 addresses;
- c) where interception of both data and multi-media content is also required, the delivery address will be specified as an IP address in either the standard IPv4 or IPv6 formats; the target addresses may be either service addresses or IP addresses;
- d) the mechanism for lawful interception, where provided, in an IPCablecom system will ideally be capable of correct operation in networks where a customer's IP address is allocated dynamically, e.g. by a DHCP server, by relating the current IP address to the customer's equipment MAC address, or otherwise;
- e) it needs to be possible to provide both the Call Content and the Intercept Related Information (IRI) regarding the communication, including that added by the network operator to facilitate correct identification of the intercept to the law enforcement agencies;
- f) the mechanism for LI should correctly relate the 'Call Content' and the 'CRD';
- g) the capacity of the LI mechanism to provide multiple intercepts should be adequate; this requirement is subject of National Legislation.
- h) the LI facility should be capable of providing numerous simultaneous intercepts and be capable of providing several independent intercepts of the same target address; this requirement is subject of National Legislation.
- i) operation of the intercept should be invisible to any customer, even by the use of 'traceroute', 'ping' and similar utilities;
- j) any malfunction or mis-operation of the interception facility should not affect the customer's service;
- k) control of the facility needs to be segregated from normal operation of the system;
- l) it needs to be possible to address and control the interception facility remotely by secure means.

The above should be related to fundamental principles of country specific regulations. Their application in the voice, data and multi-media environments will differ depending on the cable operator's overall network strategy, for example, with legacy circuit switched network solutions or other intermediate network solutions that migrate towards a European DOCSIS<sup>©</sup> and PacketCable<sup>™</sup> network architecture.

**NOTE:** It is recognized that attempts at compliance with clause (d) may lead to specific difficulties; these should not be allowed to delay early implementation of systems, though it will be necessary to devise a solution in the longer term. This will need further detailed evaluation.

Additional information on LI Requirements as listed in council resolution of 17 January 1995 as given by [1] may also be found in annex B.

The following general requirements apply:

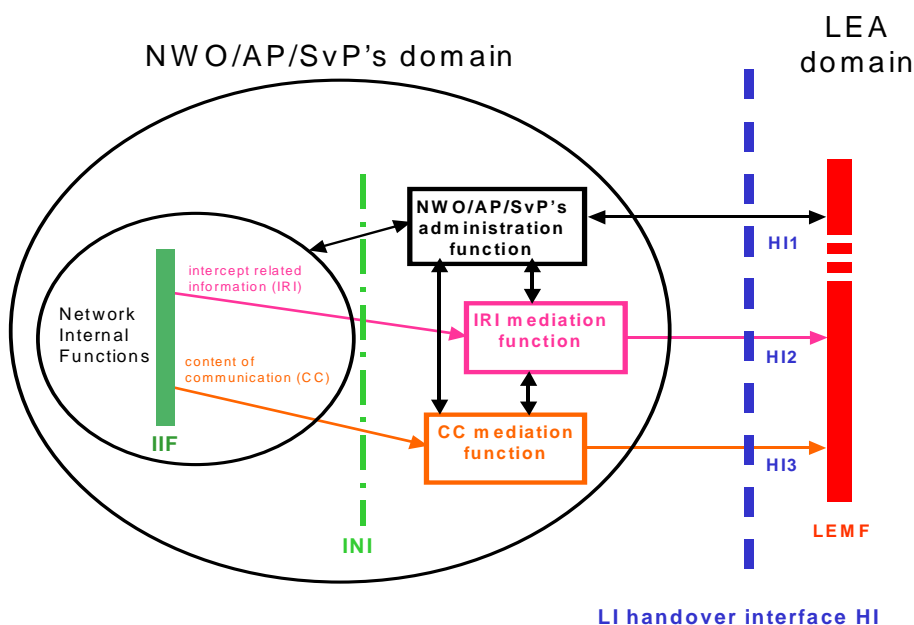
- The LI general requirements as given by TS 101 331 [i.5], including the requirements below apply:
  - Deliver content of communications for voice, fax.
  - Deliver intercept related information.
  - Interception of call features.
  - Real-time delivery.
  - Non-disclosure of information including interception methods and targets.
  - Protection of interception information and information transmission from unauthorized access.
- Solution must meet delivery requirements as given by the ETSI handover interface requirements as given by ETSI TC-LI standards [2], [3] and [4].

Optional requirements where applicable may be defined at a national level, for example:

- Multiple Subscriber Number, in the case of Basic Access services.
- Direct Dialling In number, in the case of Primary Access services.

## 5 Overview

The overall interception framework is extended from the model described in clause 5.2 of ES 201 158 as given by [16] and from the architecture identified in clause 5 of TS 101 671 as given by [3].



- IIF: internal interception function  
 INI: internal network interface  
 H11: administrative information  
 H12: intercept related information  
 H13: content of communication

**Figure 1: Functional block diagram showing Handover Interface HI (from ES 101 671 [2])**

The scope of the present document is the NWO/AP/SvP's domain as shown in figure 1 describing the internal interfaces INI1, INI2 and INI3.

The current solution adopts elements of the reference model for LI systems in IP networks defined in RFC 3924 [18], see figure 2 of the present document.

Automatic discovery of network topology is out-of-scope, i.e. it is assumed that the Mediation Device has its own means of knowing the network topology.

A mediation device might need to translate signalling on the IP-part of the network to signalling on a different interface type towards the LEA. The translation of this information is out-of-scope for the present document.

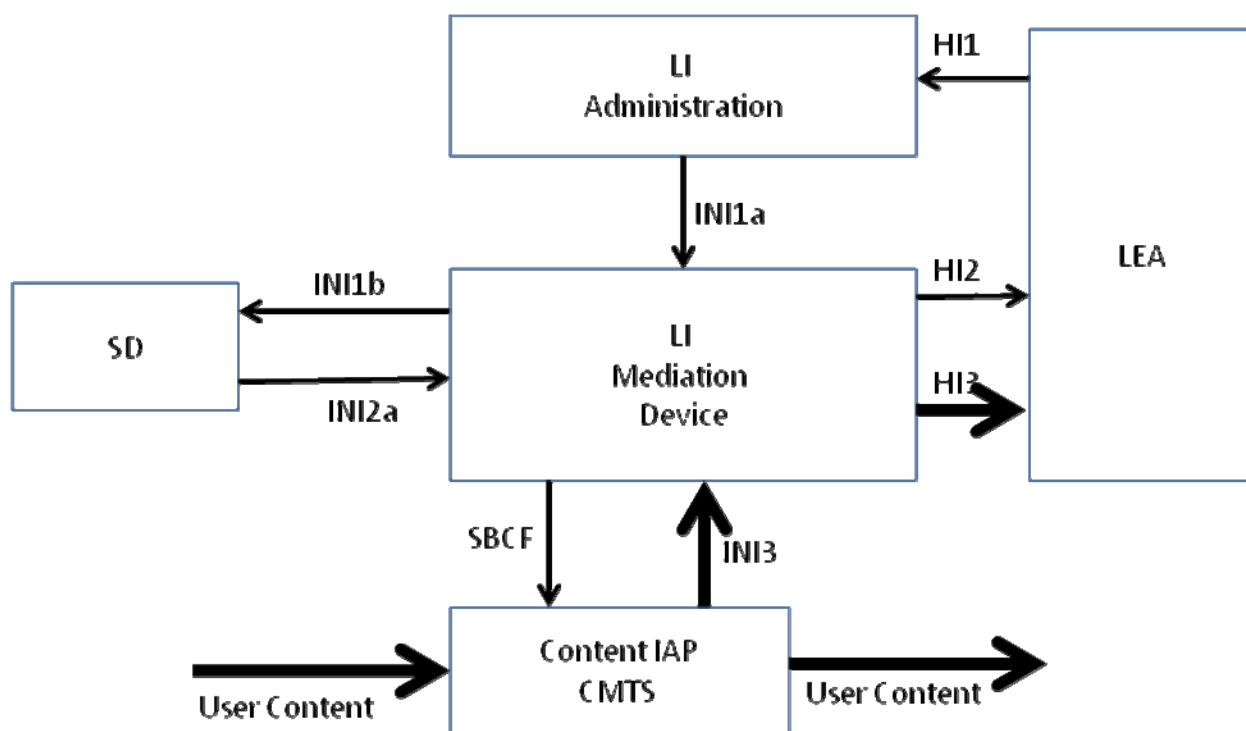
The description of the functional elements and interfaces at a generic level as given by RFC 3924, section 2.1 [18] are applied to Cable Networks as described within clause 6 of the present document.

## 6 Internal Cable Network Interfaces

### 6.1 Introduction

The Cable Network IP Telephony services is based on the PacketCable™ reference architecture and deploys signalling based on the NCS architecture described by TS 101 909-4 [5] and SIP architecture as given by RFC 3261 [6].

Figure 2 illustrates the reference model as specified for a Cable Network.



**Figure 2: Cable Network Reference model for Lawful Interception**

In this model, a Mediation System interacts with LEA and with the cable service provider's network: an LI Administration Function of the Mediation System serves staff at service provider or LEA to manage and provision intercepts; an LI Mediation Function gathers interception information from a diversity of Cable elements Intercept Access Points (IAPs) across the cable service provider's network, and delivers it to one or more LEAs through handover interfaces as defined by ETSI as given by [2], [3] and [4].

### 6.2 INI1

The protocol used for INI1a is not specified and dependant on the MD equipment. The INI1a between the LI Administration and LI MD is assumed to be integrated within the Mediation Device.

The administrative information relating to the target to be intercepted is exchanged between the internal elements of the LI Administration function and LI MD. This information is delivered to the SD over INI1b. The interface function and protocol used for INI1b is not specified and dependant on the MD and SD equipment.

INI1b provides at least the following functionality:

- Install new intercept.
- Remove intercept.
- Query intercepts.
- Alter an intercept.
- Each intercept must be assigned a unique LIID (Lawful intercept ID).
- The target identifier is specified for each intercept.

Specification of the interface INI1b is out-of-scope.

## 6.3 INI2a

The SD sends all events related to a communication session that is under intercept to the MD.

Internal interface INI2a carries Intercept Related Information (IRI) from the SD relating to the communication session that is under intercept to the MD.

Based on the IRI the MD will invoke the SBCF to trigger delivery of the CC.

Where the IN1a does not specify intercept of CC then the MD will not invoke the SBCF.

The IRI information is forwarded over HI2.

The INI2a interface **MUST** support PC1.5 EM [7] for SIP and NCS.

The SD **MUST** send the appropriate PC1.5 EM to the MD over the INI2a interface when a call feature is activated or deactivated.

## 6.4 INI3 - Call Content (CC) of Communication Interface

Timestamp is an option for the CMTS, the MD must be able to be configured for both with and without timestamp. Clarify behaviour of MD in case of the two options.

Internal interface INI3 carries Call Content (CC) of Communication information related to the intercept from the CMTS or MG to the mediation function, consistent with PacketCable™ PC ESP [17], section 5.

This clause describes the mechanism for delivery of call content, via (CC) Connections from the cable operators network LI mediation device (MD) to the Law Enforcement's Mediation Function (LEMF).

Call Content **MUST** be delivered as a stream of UDP/IP datagrams, as defined in [8] and [11] sent to the port number at the LEMF as provided during provisioning of the interception. The UDP/IP payload **MUST** adhere to the following format:

The CCC datagrams **MAY** contain a timestamp that allows the MD to identify the time at which the corresponding information was detected by the IAP. This timestamp **MUST** have an accuracy of at least 200 milliseconds. The Timestamp **MUST** adhere to the NTP time format as defined in [9] a 64-bit unsigned fixed-point number, in seconds relative to 0000 on 1 January 1900. The integer (whole seconds) part is in the first 32 bits and the fractional part (fractional seconds) is in the last 32 bits. The timestamp **MUST** be accurate to within 200 milliseconds.

The timestamp is optional on the CCC interface, a CMTS has the option to include or not include this timestamp. A MD must be configurable to receive packets over INI3 with or without the timestamp. If the timestamp is provided on INI3 the MD must forward the timestamp as received over INI3 to the LEA over HI3. If the timestamp is not provided and the LEA requires a timestamp in the packet on HI3, the MD MUST insert a timestamp in the packet delivered over HI3 to the LEA.

**Table 1: Payload of Call Content Connection Datagrams**

CCC Identifier (4 bytes)
Timestamp (8 bytes) (optional)
Intercepted Information (arbitrary length)
-----
-----
-----
-----

Intercepted RTP information will be of the following format:

**Table 2: Intercepted Information**

Original IP Header (20 bytes for IPv4, typically 40 bytes for IPv6)
-----
-----
-----
-----
Original UDP Header (8 bytes)
-----
Original RTP Header (variable length, 12 - 72 bytes)
-----
-----
-----
Original Payload (arbitrary length)
-----
-----

NOTE: Protocols other than RTP may be intercepted, such as for T.38 fax relay.

### 6.4.1 Call Content Connection Identifier

The CCC-Identifier is a 32-bit quantity, and is used to identify the intercept order to the Law Enforcement Agency.

A conversation in the PacketCable network typically consists of two separate packet streams, each corresponding to a direction of the communication. Both are delivered to the demarcation point with the same CCC-Identifier. The party listening to the communication is identified by the combination of Destination Address (from Original IP Header) and Destination Port (from Original UDP Header). The Destination Address and Destination Port for both parties involved in the communication are provided in the Session Description (SDP) [10] information provided to the MD as part of the Media\_Report message.

The MD MUST generate a CCC-Identifier that is different from all other CCC-Identifiers in use between that MD and a particular LEA. That is, two streams of content delivered to a single LEA must have different CCC-Identifiers, but a single stream of content delivered to multiple LEAs may use a single CCC-Identifier, so long as no other stream being delivered to one of the LEAs is using the same CCC-Identifier.

## 6.4.2 Original IP Header

This is the IP header [11] as sent by the endpoint. Contained in this IP header is the IP Source Address (SA) and IP Destination Address (DA), that identify the internet addresses of the source and destination of the packet.

## 6.4.3 Original UDP Header

This is the User Datagram Protocol (UDP) header [8] as sent by the endpoint. Contained in this UDP header is the Source Port and Destination Port, both of which are 16-bit quantities that identify the connection to the two endpoints.

## 6.4.4 Original RTP Header

This is the Real-Time Transport Protocol (RTP) header [12], as sent by the endpoint identified in the Source Address and Source Port. This header contains the packet formation timestamp, packet sequence number, and payload type value, as generated by the source endpoint.

The payload type value is defined by [13] and is referenced in the Session Description (SDP) [10].

## 6.4.5 Original Payload

The payload field is the bit-sequence as sent by the endpoint identified in the Source Address and Source Port. The payload typically contains the voice samples, as encoded and encrypted by the sending endpoint.

Encryption of the payload is by use of a stream cipher, or other method as described in [i.1] Keying material is contained in the Session Description (SDP) [i.2] and the algorithm to generate the actual key is described in [i.1].

Encoding of the voice may be done through use of one of the IETF's defined CODEC algorithms (as defined in [i.3]) or through a dynamic payload type defined in the Session Description (SDP) [10]. Definition of CODEC algorithms is contained in [i.3].

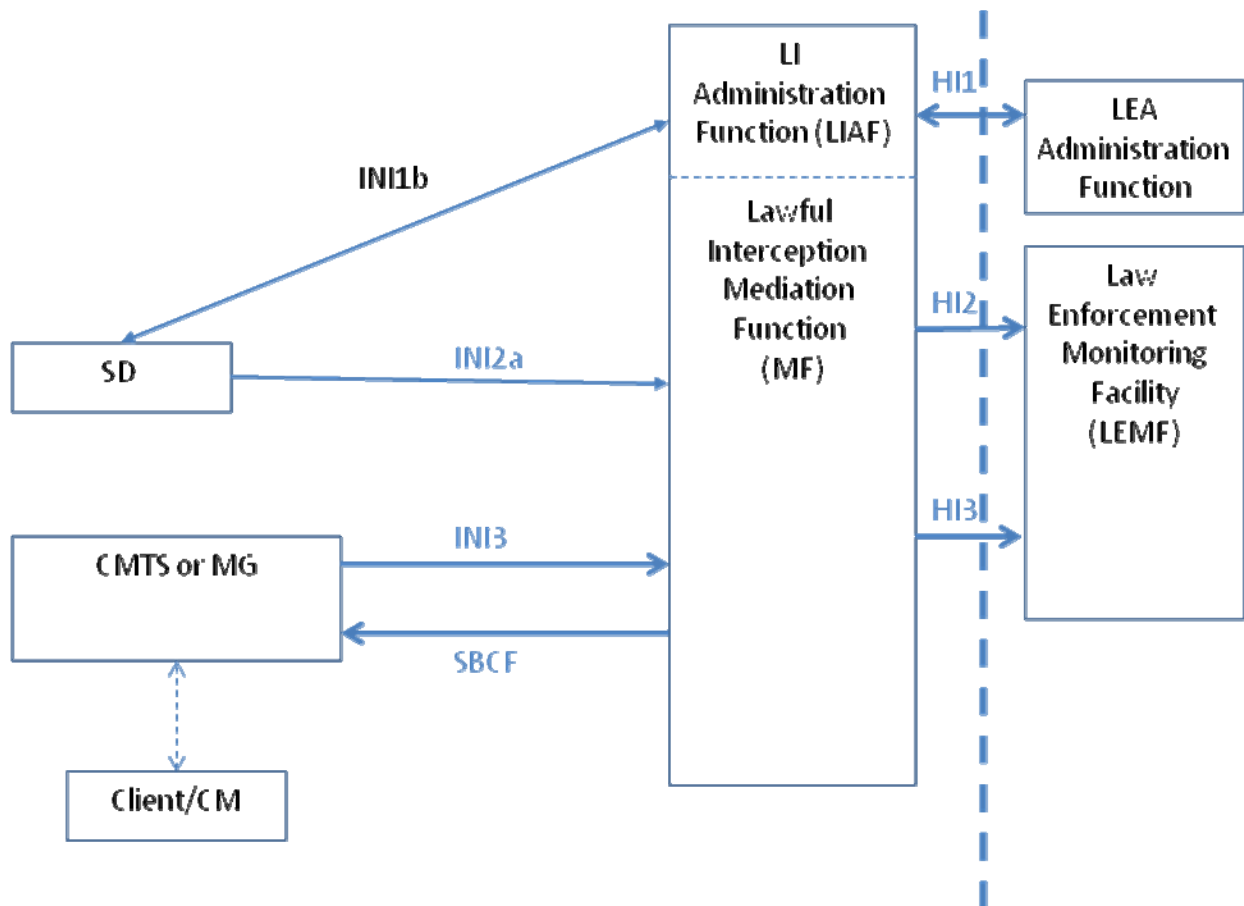
## 6.5 SBCF (SNMP based Configuration Function)

Based on SNMPv3, with the use of the IP intercept and IP TAP MIB. An example of this MIB can be found in Annex B of CableLabs Electronic Surveillance Intra-Network Specification as given by [14].

An intercept and tap mib specifies mibs for tapping content at IP Layer and configuring the delivery of the content to the MD.

## 7 LI Cable Broadband IP Network Architecture

The cable broadband IP network architecture given by PacketCable™ maps to the LI reference model as given by figure 3.



**Figure 3: Cable Network Architecture for LI**

The SD provides the IRI. In an actual implementation of there may be more than one elements of SD and MDs within a Cable Network Architecture.

The SD provides IRI information to the LIMD, including session information, session status information (start, stop, etc.), and security information.

IRI information is delivered to the LIMD by the SD over INI2a and includes:

- Events like session start/stop/redirection.
- Session information including SDPs, QoS parameters, security information where necessary e.g. where the information is encrypted.

The CMTS and MG provides the CC over INI3.

The interception function within the CMTS or MG provides the CC information to the MD as follows:

- Duplication of complete traffic belonging to a specific flow of IP packets based on IP-filter criteria (IP-addresses, port numbers, etc.)

## 7.1 Dimensioning and Capacity

The LI solution shall be scaled to accommodate the level of interception service that's proportionate with the subscriber base with minimum requirements defined by national legislation, e.g. number of LEA's supported by the network provider with delivery to a number of LEMF's and a number of simultaneous interception orders for a single target.

## 7.2 Elements of Cable Broadband IP Network

**LI Monitoring / LEMD Function:** The LI Monitoring / Law Enforcement Monitoring function is the system used by the LEA for the receiving of the HI-2 and/or HI-3 information streams. This system requirements are out of scope of the current document and assumed to be already available.

**LI Administration:** The LI administration function may be provided by the mediation device and may be located, operated and maintained at the Cable Operators premises by for example Cable Operator's personnel as authorised by the LEA or as described by national legislation.

**LI Mediation:** The LI Mediation function is to be provided by one or more Mediation Devices (and associated devices, for purposes of the present document "Mediation Device" may refer to one or more of these devices at the same time). This device is typically located and maintained at the Cable Operators premises, and managed by the Cable Operator through the LI Administration function.

**SD/MGC:** These elements refer to the Cable Network softswitch devices. These devices are typically located, maintained and operated at the Cable Operators premises. These devices provide signalling and control information, as well as all LI provisioning functions.

**CONTENT-IAP:** These elements refer to the Cable Network intercept access point. The IAP would reside on devices that carry the content of the traffic i.e. call content (CC). Such devices are, for example but not limited to, CMTS, Routers, MG, etc.

## 7.3 Functional Description

The reference model RFC 3924 [18] is assumed as given in clause 5 with the elements of an LI Mediation Device (MD) and an LI Administrative Function located at the Cable Operators premises.

The SD must support the LI INI1b and INI2a as described by the present document.

The SD receives over INI1b information relating to the target to be intercepted.

INI2 provides call data/event interception/notification, which in turn will enable the Mediation Device to activate the interception of the Communications Content at the appropriate network elements.

The following are functionalities of a MD:

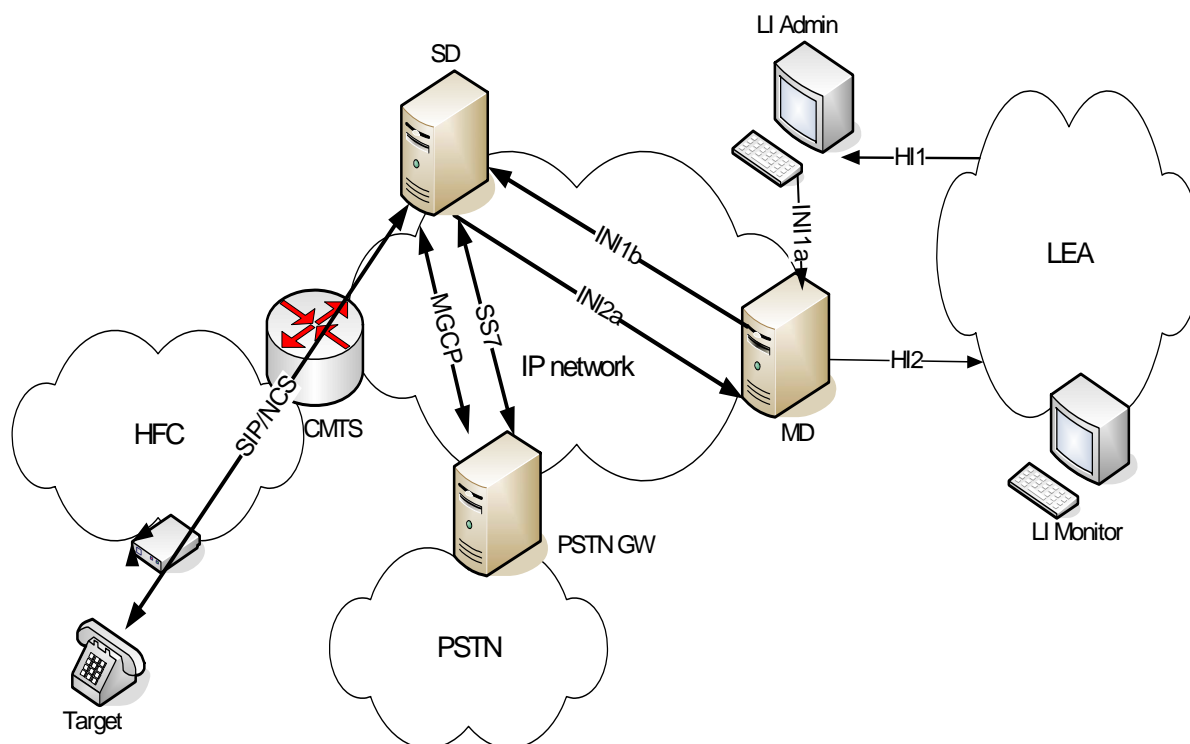
- LI Administration function: LI administration typically might be performed by authorized Cable Operator staff, typically based on applicable warrants received from the LEA(s) or as prescribed by National Legislation.
- LI provisioning (SD): IRI provisioning over INI1b must be implemented by the MD through the secure interface to each SD.
- LI provisioning (network): CCC provisioning will be done by the MD. The MD acts on information received over INI2s i.e. IRI. If specified by LEA the MD shall invoke its SBCF to configure the IAP at the CMTS or MG to copy the CC.
- IRI IAP (SD): The SD intercepts call data/events, this data will be provided to the MD according to the PacketCable™ Event Message specification, then mediated into the appropriate HI-2 messages by the MD and delivered to LEMF.



- Content IAP (CMTS/MG): On-Net and Off-Net intercepted calls will be intercepted by the IAP at the CMTS or MG. The Content IAP will duplicate the required data to MD without disturbing the normal traffic flow from target to destination and vice versa.
- Timestamp: Where the LEA requires identify the time at which the corresponding information was detected by the MD, a timestamp of call content datagrams delivered between the MD and LEMF shall be supported by the MD.

### 7.3.1 LI Process: Interception of IP Telephony Signalling

The functional model for interception of IP Telephony Signalling is given by figure 4.



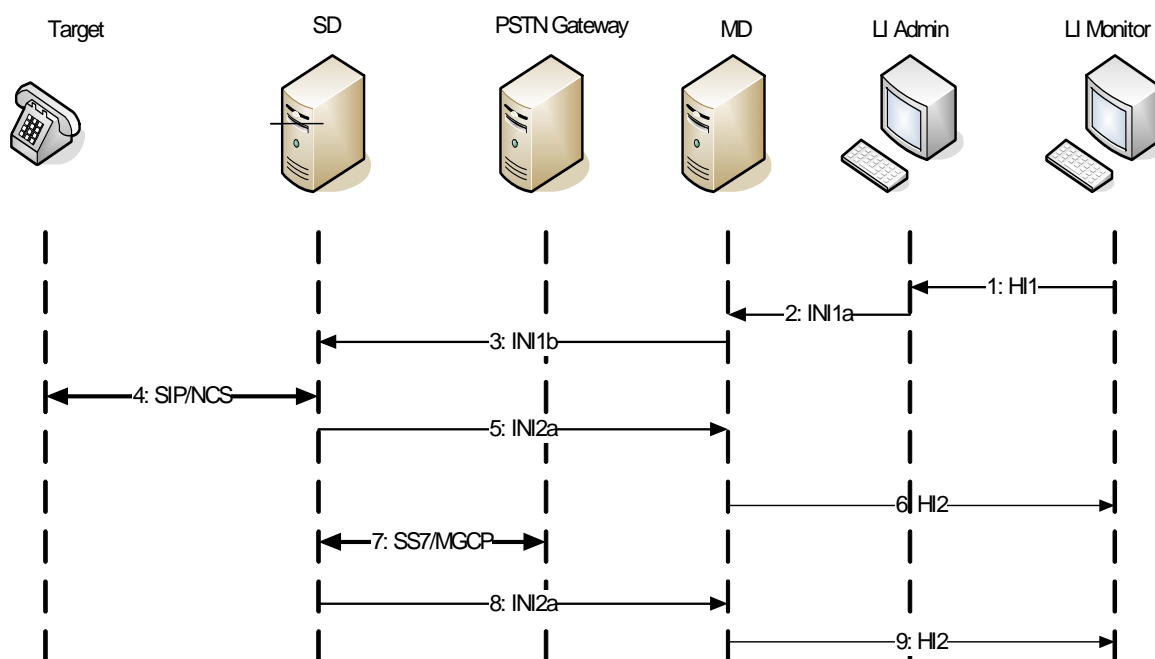
**Figure 4: Interception of IP Telephony signalling**

All signalling will be intercepted at the SD/PSTN GW device, concentrated and delivered by MD as given by figure 4.

Interception would take place according to the following sequence:

- 1) LI warrant is provided by LEA to Cable Operator.
- 2) The Cable Operator provisions interception on the Mediation Device.
- 3) Mediation Device provisions SD to intercept all events in relation to the target of interception.
- 4) No interception is done until target registers activity.
- 5) Signaling activity takes place via the IP or TDM network.
- 6) All signalling is captured by the SD/PSTN GW.
- 7) SD/PSTN GW delivers event records to Mediation Device.
- 8) Mediation Device delivers HI-2 records to LEMF.

## Sequence diagram



**Figure 5: Sequence diagram for interception of Telephony signalling**

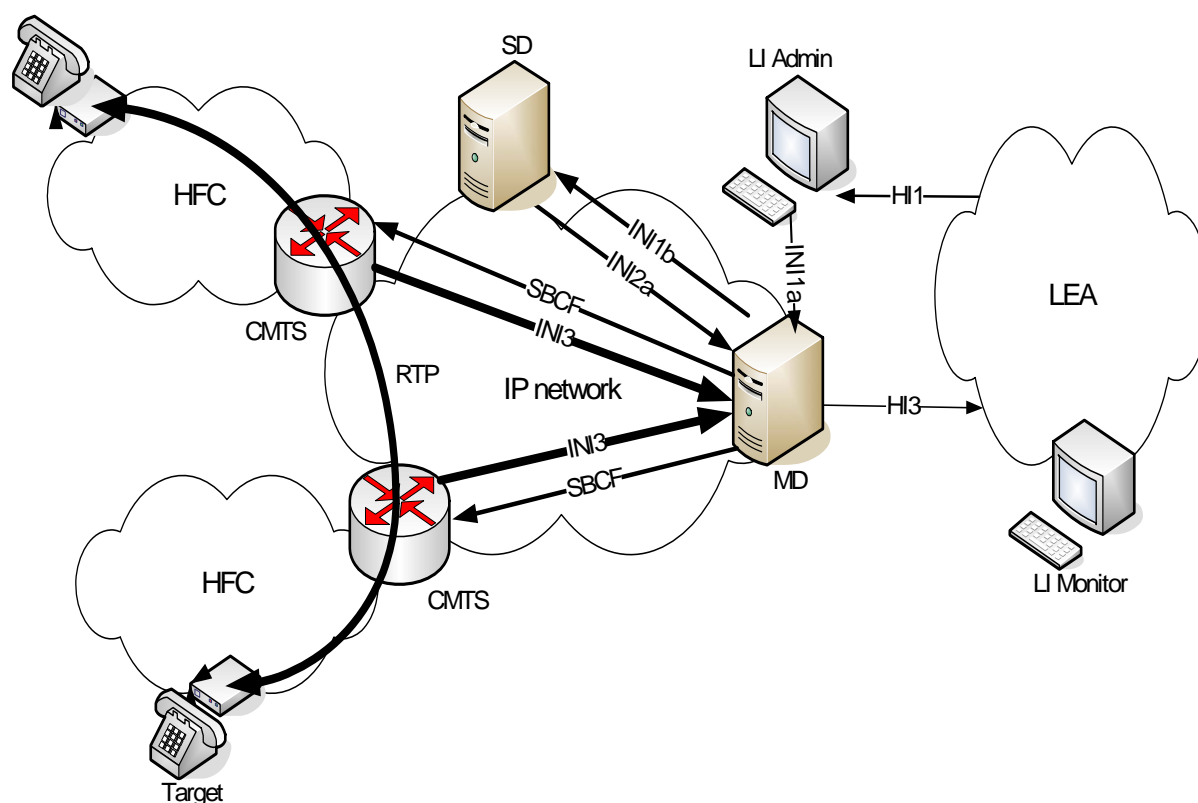
Figure 5 shows the process for the interception of IRI for Telephony. The following steps are done:

- 1) Cable operator staff receives a warrant over HI1.
- 2) LI admin provisions Mediation Devices over INI1a (internal interface).
- 3) MD provisions SD to send all events related to target to MD.
- 4) Target participates in call (as callee, caller or feature invocation).
- 5) SD forwards all signalling information to MD.
- 6) MD forwards all signalling over HI2 to LEA.
- 7) Call may invoke signalling on the PSTN network, SD participates in that signalling.
- 8) SD forwards all signalling related to PSTN also to MD.
- 9) MD forwards all PSTN signalling to LEA over HI2.

Note that steps 4 and 7 typically over a longer time in multiple messages that are typically not sequential. The diagrams illustrates that all events related to signalling are sent to MD, and that MD delivers the information to the LEA. The diagram does not intend to specify a certain call flow.

### 7.3.2 LI Process: interception of on-net calls

The functional model for interception of IP Telephony on-net calls is given by figure 6.



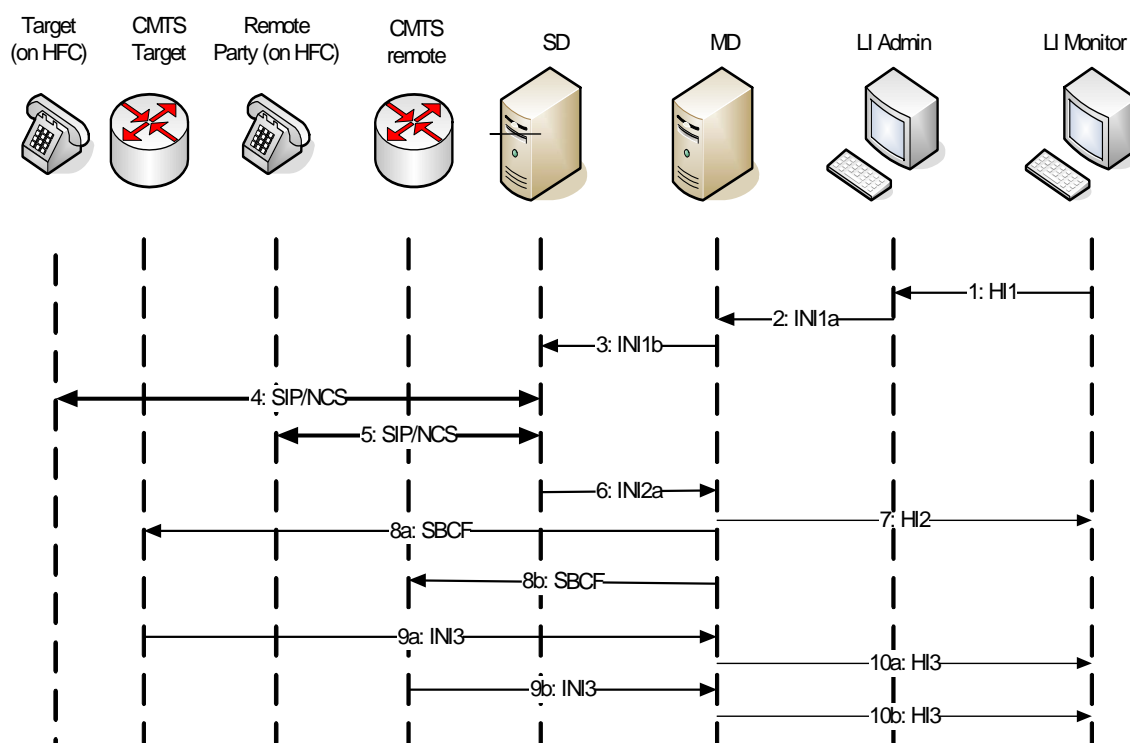
**Figure 6: Interception of on-net voice calls**

Interception shall be at the IAP of SD and CMTS as given by figure 6. Call content traffic to and from the interception target will be duplicated at the IAP of CMTS and sent to the Mediation Device, where it will be delivered to LEMF.

The interception shall be according to the sequence described below:

- 1) LI warrant is provided by LEA to Cable Operator.
- 2) The Cable operator provisions interception on the Mediation Device.
- 3) Mediation Device provisions SD to intercept all events in relation to the target of interception.
- 4) No interception is done until target registers activity.
- 5) Call by interception target is initiated via IP.
- 6) SD sets up call path; delivers INI2a to MD, triggering the content tap.
- 7) MD sets up interception of content via its SBCF on the IAP of CMTS.
- 8) IAP of CMTS duplicates call content and sends duplicated Call Content to Mediation Device.
- 9) Mediation Device delivers HI-2 and HI-3 to the LEMF.

## Sequence diagram



**Figure 7: Sequence diagram: content intercept for on-net calls**

The sequence diagram in figure 7 show the process for the interception of call content for Telephony for an on-net call. The following steps are done:

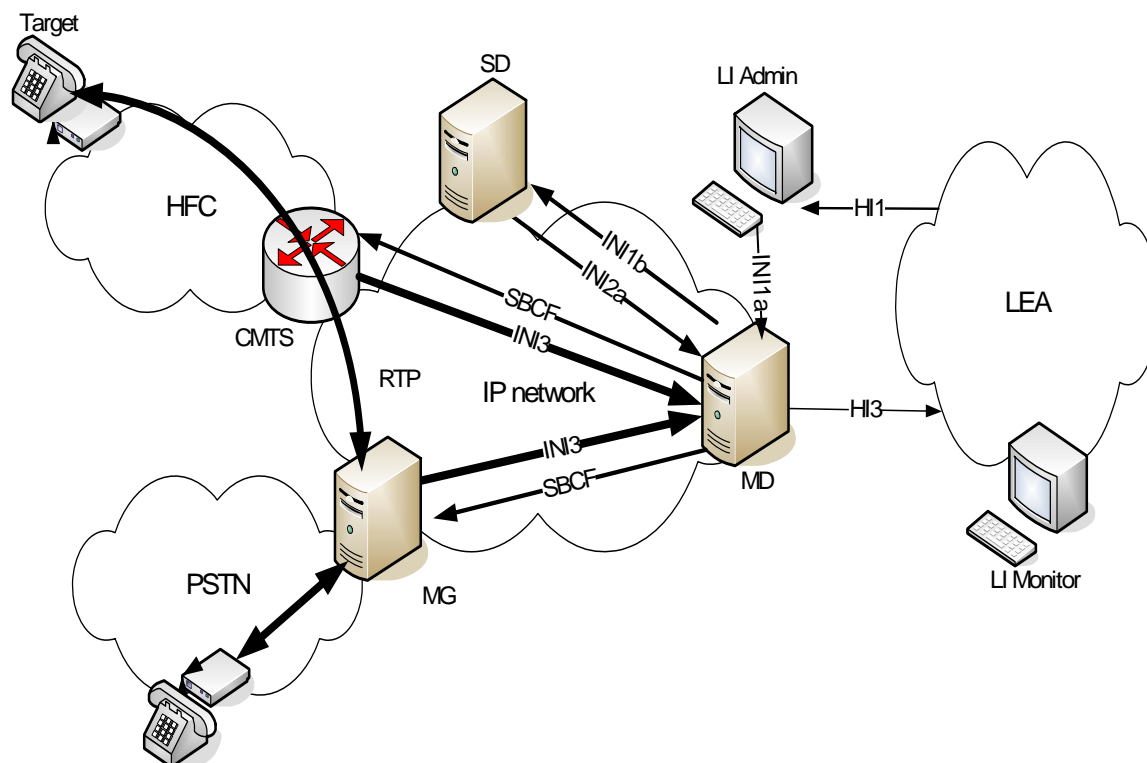
- 1) Cable operator staff receives a warrant over HI1.
- 2) LI admin provisions Mediation Devices over INI1a (internal interface).
- 3) MD provisions SD to send all events related to target to MD.
- 4) Target participates in call (as callee, caller or feature invocation). Signaling consists of signalling to target (step 4a) and signalling to other party (step 4b).
- 5) SD forwards all call event information (both derived from 4a and 4b) to MD.
- 6) MD forwards all call information over HI2 to LEA (step 6 and 7 may be in a different order).
- 7) MD installs taps over SBCF on CMTS of target (step 7a) and/or CMTS of other party (step 7b).
- 8) CMTS(s) forward call content based on installed tap over INI3 to MD.
- 9) MD delivers call content over HI3 to LEA.

Interception at both the target CMTS and remote CMTS might be needed, interception on one of the CMTSs might be sufficient.

In the case that the call involves subscribers on two different SDs, the signalling with the remote party will be with a second SD. The SD of the target provides all necessary information to the MD over INI2a. The MD has a full view of the network topology and can install the TAP on the remote CMTS.

### 7.3.3 LI Process: interception of off-net calls

The functional model for interception of IP Telephony off-net calls is given by figure 8.



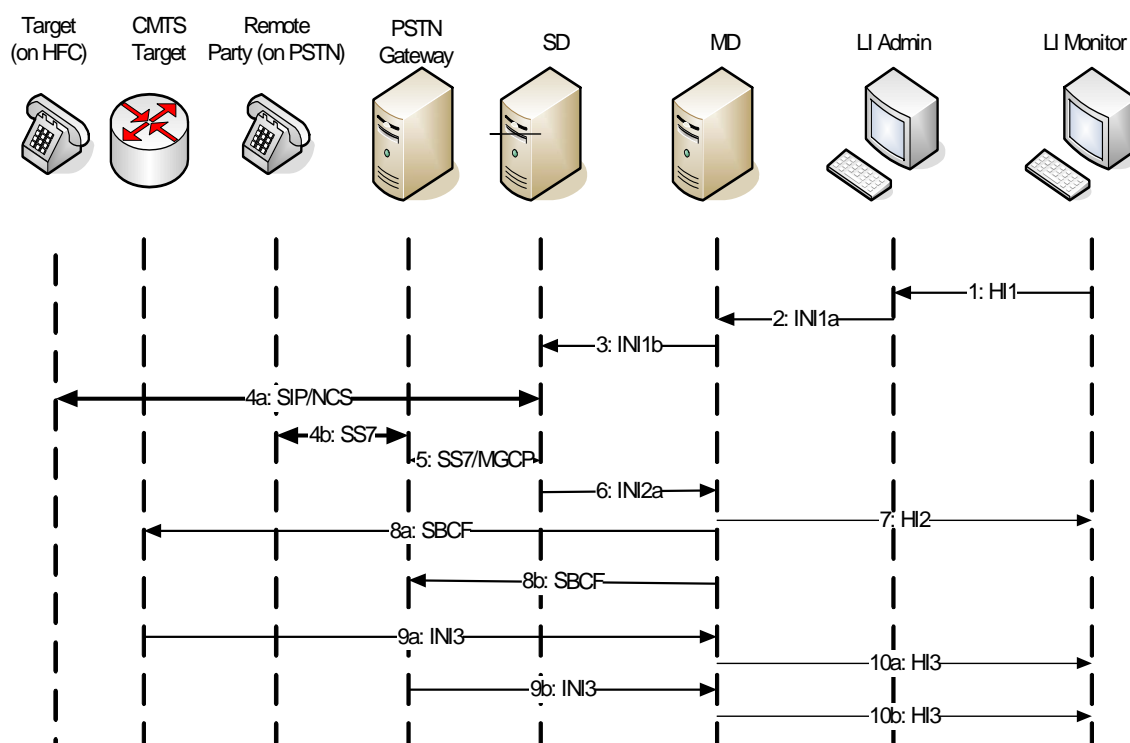
**Figure 8: Interception of off-net voice calls**

Interception shall be at the IAP of the CMTS or MG, in the same way as on-net calls as given by figure 8. Call content traffic to and from the interception target will be duplicated at the IAP of CMTS or MG and sent to the Mediation Device, where it will be delivered to LEMF.

The interception shall be according to the sequence described below:

- 1) LI warrant is provided by LEA to Cable Operator.
- 2) The Cable Operator provisions interception on the Mediation Device.
- 3) Mediation Device provisions SD to intercept all events in relation to the target of interception.
- 4) No interception is done until target registers activity.
- 5) Call by interception target is initiated via IP or TDM.
- 6) SD sets up call path; delivers IRI over INI2a to MD, triggering the content tap.
- 7) MD sets up interception of content via its SBCF on the IAP of CMTS.
- 8) IAP of CMTS duplicates call content and sends duplicated Call Content to Mediation Device.
- 9) Mediation Device delivers HI-2 and HI-3 to LEMF.

## Sequence diagram



**Figure 9: Sequence diagram for off-net content intercept**

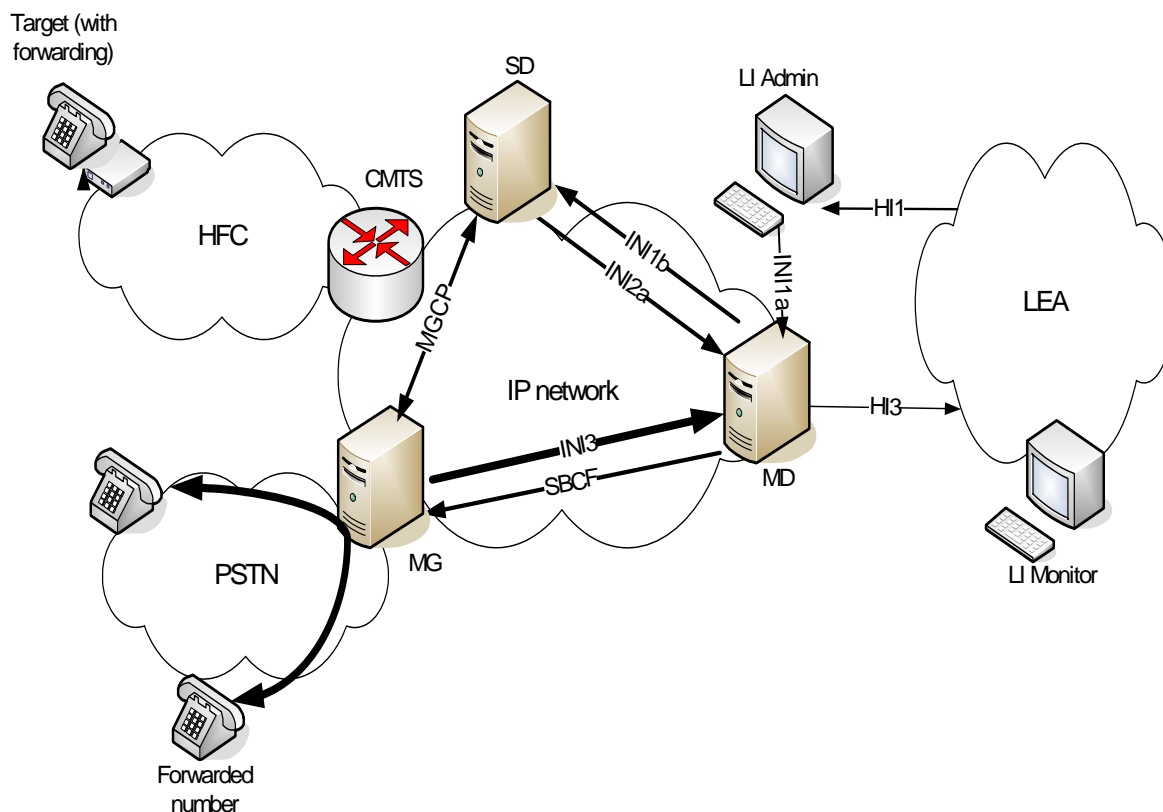
The sequence diagram in figure 9 show the process for the interception of call content for telephony for an off-net call. The following steps are done:

- 1) Cable operator staff receives a warrant over HI1.
- 2) LI admin provisions Mediation Devices over INI1a (internal interface).
- 3) MD provisions SD to send all events related to target to MD.
- 4) Target participates in call (as callee, caller or feature invocation). Signaling consists of signalling to target (step 4a) and signalling to other party (step 4b). Signaling to other party.
- 5) Signaling and from remote party on PSTN network is sent to SD.
- 6) SD forwards all call event information (both derived from 4a and 5) to MD.
- 7) MD forwards all call information over HI2 to LEA (step 7 and 8 may be in a different order).
- 8) MD installs taps over SBCF on CMTS of target (step 8a) and/or PSTN gateway of other party (step 8b).
- 9) CMTS and/or PSTN gateway forward call content based on installed tap over INI3 to MD.
- 10) MD delivers call content over HI3 to LEA.

Interception at both the CMTS and MG might be needed, interception on the CMTS or MG might be sufficient.

### 7.3.4 Details: interception of hairpin calls

The functional model for interception of IP Telephony hairpin calls is given in figure 10.



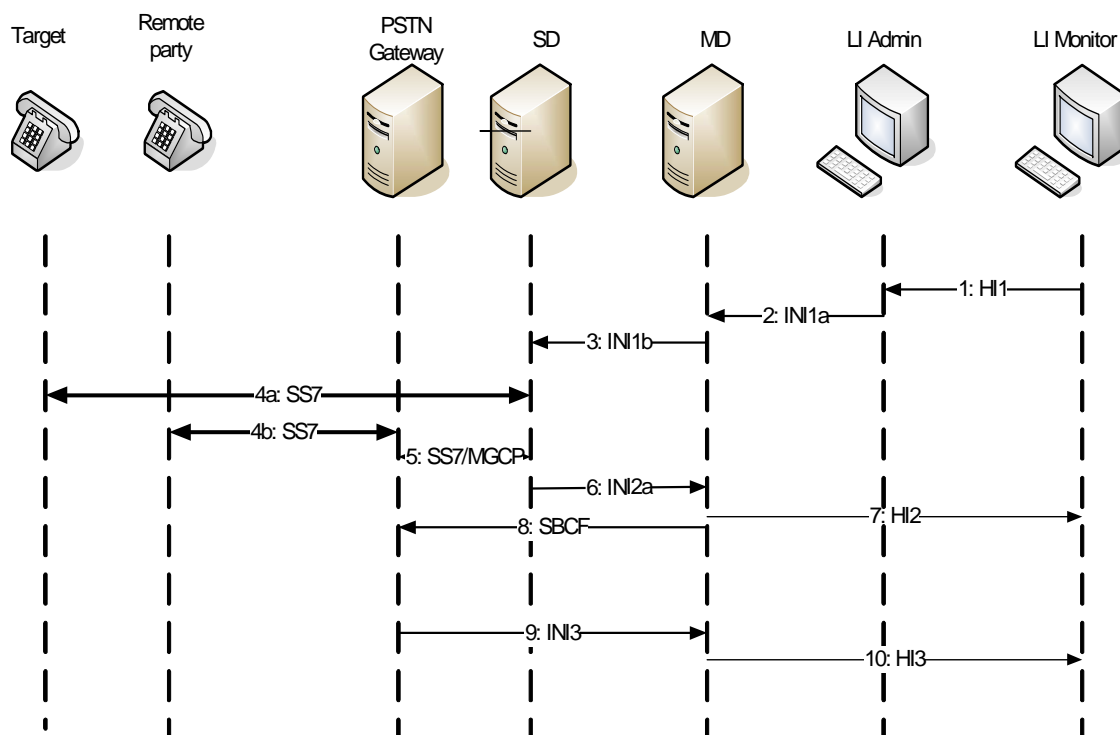
**Figure 10: Interception of hairpin voice calls**

Interception shall be at the IAP of the MG as given by figure 10. Call content traffic to and from the interception target will be duplicated at the IAP of the MG and sent to the MD, where it will be delivered to LEMF.

The interception shall be according to the sequence described below:

- 1) LI warrant is provided by LEA to authorized Cable Operator personnel.
- 2) Authorized Cable Operator personnel provisions interception at Mediation Device.
- 3) Mediation Device provisions SD to report all activity to target of interception.
- 4) No interception is done until target registers activity.
- 5) Call is initiated via SS7 to the interception target.
- 6) SD sets up call path forwarding to forwarded called party; delivers INI2 to MD, triggering the content tap, note that the media path is setup in such a way that the MG converts the TDM to RTP, sends the RTP to itself (internal), and convert the RTP back to TDM.
- 7) MD sets up interception of content via its SBCF on the IAP of the MG.
- 8) IAP of MG duplicates call content and sends duplicated Call Content to Mediation Device.
- 9) Mediation Device delivers Call Content to LEMF.

## Sequence diagram



**Figure 11: Sequence diagram for interception of content for hairpin calls**

The sequence diagram in figure 11 show the process for the interception of call content for telephony for a hairpin call. The following steps are done:

- 1) Cable operator staff receives a warrant over HI1.
- 2) LI admin provisions Mediation Devices over INI1a (internal interface).
- 3) MD provisions SD to report all activity to MD.
- 4) Signaling happens on the PSTN networks.
- 5) PSTN gateway performs signalling with SD.

NOTE: Steps 4 and 5 happen in interaction.

- 6) SD forwards signalling information to MD.
- 7) MD forwards signalling information to LEA.
- 8) MD installs tap on PSTN gateway based on information received in step 6 from SD.
- 9) PSTN gateway delivers call content over INI3 to MD.
- 10) MD forwards call content over HI3 to LEA.

## 8 Security

The SNMP3 (VACM and USM MIBs) configuration must be such that only authorised personal can modify and view the MIBs used for LI.

Security requirements for LI are given by TR 102 661 [i.4].



---

## Annex A (informative): Requirements listed in Council Resolution of 17 January 1995

The following requirements for Telecommunications Network operators to provide assistance to Law Enforcement agencies in the Member States are listed in the European Council Resolution of 17 January 1995 [1] and are included here for information.

Law enforcement agencies require access to the entire telecommunications transmitted, or caused to be transmitted, to and from the number or other identifier of the target service used by the interception subject. Law enforcement agencies also require access to the call-associated data that are generated to process the call.

Law enforcement agencies require access to all interception subjects operating temporarily or permanently within a telecommunications system.

Law enforcement agencies require access in cases where the interception subject may be using features to divert calls to other telecommunications services or terminal equipment, including calls that traverse more than one network or are processed by more than one network operator/service provider before completing.

Law enforcement agencies require that the telecommunications to and from a target service be provided to the exclusion of any telecommunications that do not fall within the scope of the interception authorization.

Law enforcement agencies require access to call associated data such as:

- signalling of access ready status;
- called party number for outgoing connections even if there is no successful connection established;
- calling party number for incoming connections even if there is no successful connection established;
- all signals emitted by the target, including post-connection dialled signals emitted to activate features such as conference calling and call transfer;
- beginning, end and duration of the connection;
- actual destination and intermediate directory numbers if call has been diverted.

Law enforcement agencies require information on the most accurate geographical location known to the network for mobile subscribers.

Law enforcement agencies require data on the specific services used by the interception subject and the technical parameters for those types of communication.

Law enforcement agencies require a real-time, fulltime monitoring capability for the interception of telecommunications. Call associated data should also be provided in real-time. If call associated data cannot be made available in real time, law enforcement agencies require the data to be available as soon as possible upon call termination.

Law enforcement agencies require network operators/service providers to provide one or several interfaces from which the intercepted communications can be transmitted to the law enforcement monitoring facility. These interfaces have to be commonly agreed on by the interception authorities and the network operators/service providers. Other issues associated with these interfaces will be handled according to accepted practices in individual countries.

Law enforcement agencies require network operators/service providers to provide call associated data and Call Content from the target service in a way that allows for the accurate correlation of call associated data with Call Content.

Law enforcement agencies require that the format for transmitting the intercepted communications to the monitoring facility be a generally available format. This format will be agreed upon on an individual country basis.

If network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law enforcement agencies require the network operators/service providers to provide intercepted communications *en clair*.

Law enforcement agencies require network operators/service providers to be able to transmit the intercepted communications to the law enforcement monitoring facility via fixed or switched connections.

Law enforcement agencies require that the transmission of the intercepted communications to the monitoring facility meet applicable security requirements.

Law enforcement agencies require interceptions to be implemented so that neither the interception target nor any other unauthorized person is aware of any changes made to fulfil the interception order. In particular, the operation of the target service should appear unchanged to the interception subject.

Law enforcement agencies require the interception to be designed and implemented to preclude unauthorized or improper use and to safeguard the information related to the interception.

Law enforcement agencies require network operators/service providers to protect information on which and how many interceptions are being or have been performed, and not disclose information on how interceptions are carried out.

Law enforcement agencies require network operators/service providers to ensure that intercepted communications are only transmitted to the monitoring agency specified in the interception authorization.

According to national regulations, network operators and service providers could be obliged to maintain an adequately protected record of the activation of interceptions.

Based on a lawful inquiry and before implementation of the interception, law enforcement agencies require:

- the interception subject's identity, service number or other distinctive identifier;
- information on the services and features of the telecommunications system used by the interception subject and delivered by network operators/service providers; and
- information on the technical parameters of the transmission to the law enforcement monitoring facility.

During the interception, law enforcement agencies may require information and/or assistance from the network operators/service providers to ensure that the communications acquired at the interception interface are those communications associated with the target service. The type of information and/or assistance required will vary according to the accepted practices in individual countries.

Law enforcement agencies require network operators/service providers to make provisions for implementing a number of simultaneous intercepts. Multiple interceptions may be required for a single target service to allow monitoring by more than one law enforcement agency. In this case, network operators/service providers should take precautions to safeguard the identities of the monitoring agencies and ensure the confidentiality of the investigations. The maximum number of simultaneous interceptions for a given subscriber population will be in accordance with national requirements.

Law enforcement agencies require network operators/service providers to implement interceptions as quickly as possible (in urgent cases within a few hours or minutes). The response requirements of law enforcement agencies will vary by country and by the type of target service to be intercepted.

For the duration of the interception, law enforcement agencies require that the reliability of the services supporting the interception at least equals the reliability of the target services provided to the interception subject. Law enforcement agencies require the quality of service of the intercepted transmissions forwarded to the monitoring facility to comply with the performance standards of the network operators/service providers.

---

## History

<b>Document history</b>		
V1.1.1	November 2009	Publication