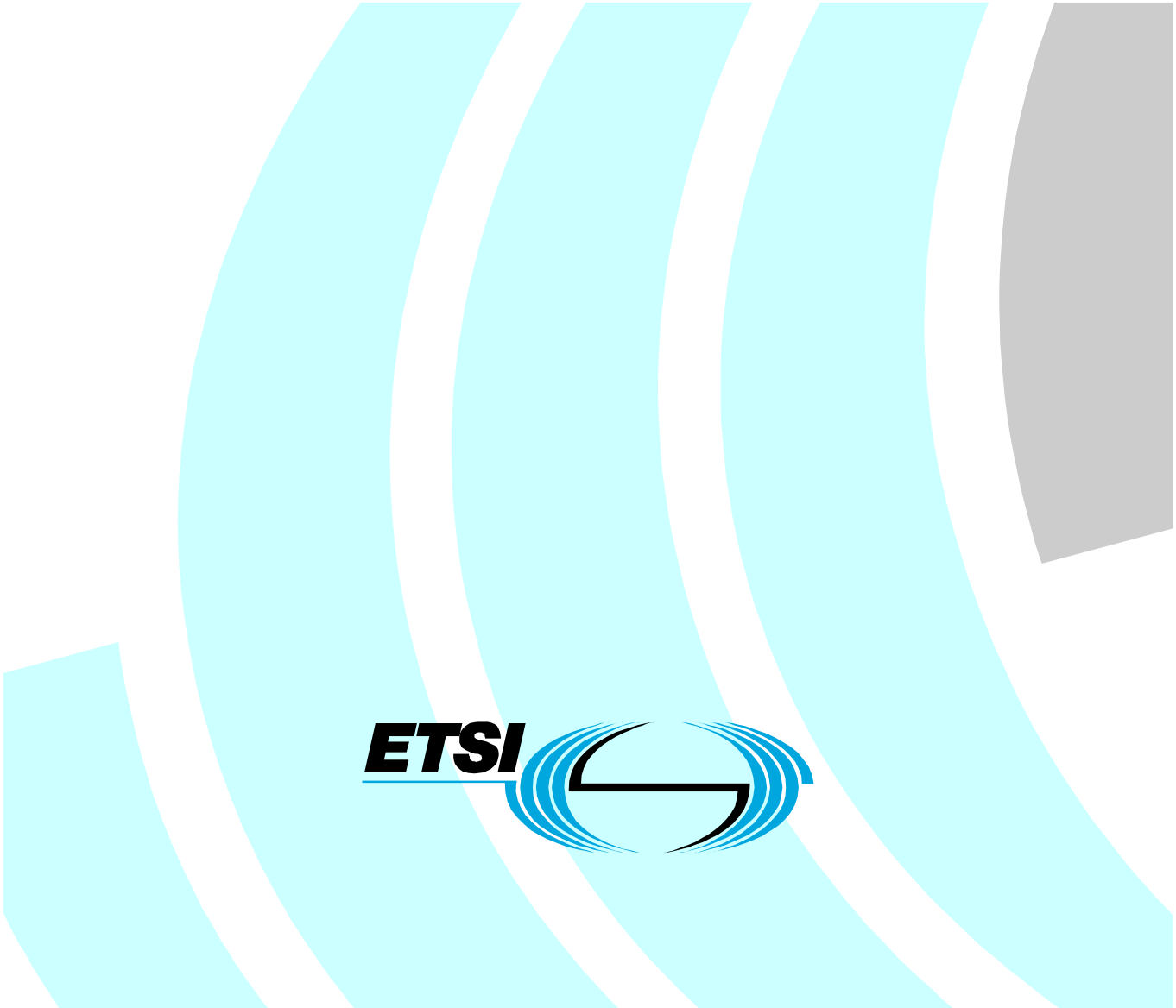
ETSI TS 101 909-20-1 V1.1.2 (2005-10)

Technical Specification

Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 1: CMS based Voice Telephony Services



Reference
DTS/AT-020020-20-01

Keywords
access, broadband, IP, IPCable, Lawful Interception, multimedia, PSTN, voice

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

Contents

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 and Terminals (AT).

The present document is part 20, sub-part 1, of a multi-part deliverable. Full details of the entire series can be found in part 1.

The present document is fully in line with initiative "eEurope 2002 - An Information Society For All", under "The contribution of European standardization to the eEurope Initiative, A rolling Action Plan" especially under key objectives:

1) A cheaper, faster and secure Internet
   a) Cheaper and faster Internet access
   b) Secure networks and smart cards
2) Stimulate the use of the Internet
   a) Accelerating e-commerce
   b) European digital content for global networks
   c) Intelligent transport systems

Introduction

The cable industry in Europe and across other Global regions has already deployed broadband cable television Hybrid Fibre/Coaxial (HFC) data networks running the Cable Modem Protocol. The cable industry is in the rapid stages of deploying IP Voice and other time critical multimedia services over these broadband cable television networks.

The cable industry has recognized the urgent need to develop ETSI Technical Specifications aimed at developing interoperable interface specifications and mechanisms for the delivery of end to end advanced real time IP multimedia time critical services over bi-directional broadband cable networks.

IPCablecom is a set of protocols and associated element functional requirements developed to deliver Quality of Service (QoS) enhanced secure IP multimedia time critical communications services using packetized data transmission technology to a consumer's home over the broadband cable television Hybrid Fibre/Coaxial (HFC) data network running the Cable Modem protocol. IPCablecom utilizes a network superstructure that overlays the two-way data-ready cable television network. While the initial service offerings in the IPCablecom product line are anticipated to be Packet Voice, the long-term project vision encompasses packet video and a large family of other packet-based services.

The Cable Industry is a global market and therefore the ETSI standards are developed to align with standards either already developed or under development in other regions. The ETSI Specifications are consistent with the CableLabs/ IPCablecom set of specifications as published by the SCTE. An agreement has been established between ETSI and SCTE in the US to ensure, where appropriate, that the release of IPCablecom and IPCablecom set of specifications are aligned and to avoid unnecessary duplication. The set of IPCablecom ETSI specifications also refers to ITU-SG9 draft and published recommendations relating to IP Cable Communication.

The whole set of multi-part ETSI deliverables to which the present document belongs specify a Cable Communication Service for the delivery of IP Multimedia Time Critical Services over a HFC Broadband Cable Network to the consumer's home cable telecom terminal. "IPCablecom" also refers to the ETSI working group program that shall define and develop these ETSI deliverables.

NOTE: The present document has been restructured to reflect the changes in the original work item.
Sub-part 1: IPCablecom CMS based architecture.

The present document contains updated and released information covering the intercept interfaces and consequently the corresponding ASN.1 coding specific to IPCablecom implementation of the ES 201 671 [8] HI specification. The restructuring of this document has been made possible as a result of parallel activity done under STF 261 on the development of TS 101 909-20-2, both documents have been aligned (as necessary) to ensure continuity. This part 20-1 has been renamed to more accurately reflect the scope, namely Lawful Interception of Voice Telephony within IPCablecom implementations based upon a CMS architecture.

1 Scope

The present document defines the interception of voice communications within the IPCablecom "NCS" architecture, using a CMS for call control, as identified by a unique address (number) e.g. IUT-T Recommendation E.164 [13]. The present set of documents specifies IPCablecom, a set of protocols and associated element functional requirements. These have been developed to deliver Quality of Service (QoS), enhanced secure IP multimedia time critical communication services, using packetized data transmission technology to a consumer's home over a cable television Hybrid Fiber/Coaxial (HFC) data network.

NOTE 1: IPCablecom set of documents utilize a network superstructure that overlays the two-way data-ready cable television network, e.g. as specified within ES 201 488 [12] and ES 200 800 (see bibliography).

While the initial service offerings in the IPCablecom product line are anticipated to be Packet Voice and Packet Video, the long-term project vision encompasses a large family of packet-based services. This may require in the future, not only careful maintenance control, but also an extension of the present set of documents.

NOTE 2: The present set of documents aims for global acceptance and applicability. It is therefore developed in alignment with standards either already existing or under development in other regions and in International Telecommunications Union (ITU).

To facilitate maintenance and future enhancements to support other real-time multimedia services the documents consist of multi-parts as detailed in part 1: General.

The present document is part 20 and describes a set of generic Lawful Interception (LI) mechanisms relating to IPCablecom. The objective of the present document is to define the implementation of Lawful Interception (LI) requirements within the current IP Core Network model adopted by IPCablecom. The specific deployments, where based on national variants or requirements (such as charging, applicability rules, privacy rules, etc.) or operation aspects based on vendor specific implementation (such as administration, bundling of functions into components, deployment concerns) are outside the scope of this generic document.

NOTE 3: The present document neither defines the events nor the information to be provided to the handover interface, this will be included in the next edition.

Lawful Interception in the Line Control Signalling (LCS) Architecture (TS 101 909-23 [4]), which uses V 5.2 to Local Exchange (LE) is entirely handled by the LE and has no impact.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- 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.
- For a non-specific reference, the latest version applies.

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

[1] ETSI TS 101 909-11 (V.1.2.1): "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 11: Security".

[2] ETSI TS 101 909-18: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 18: Embedded Media Terminal Adapter (e-MTA) offering an interface to analogue terminals and Cable Modem".

[3] ETSI TS 101 909-20-2: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 2: Streamed multimedia services".

[4] ETSI TS 101 909-23: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 23: Internet Protocol Access Terminal - Line Control Signalling (IPAT - LCS)".

[5] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector; (OJ L 1998/24, 30.01.1998, page 1)

NOTE: http://europa.eu.int/ISPO/infosoc/telecompolicy/en/9766en.pdf

[6] Directive 95/46/EC of the European Parliament of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; (OJ L281 of 23.11.1995)

NOTE: http://www.icm2006.org/imgs/congresos/Directive%2095%2046%20EC.pdf

[7] Commission Directive 90/388/EEC of 28 June 1990 on competition in the markets for telecommunications services.

[8] ETSI ES 201 671: "Telecommunications Security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

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

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

[11] ITU-T Recommendation J.112: "Transmission systems for interactive cable television services".

[12] ETSI ES 201 488: "Data-Over-Cable Service Interface Specifications; Radio Frequency Interface Specification".

[13] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[14] ITU-T Recommendation X.680: "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[15] ITU-T Recommendation X.690: "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

[16] ETSI TR 101 963: "Access and Terminals (AT); Report on the Requirements of European Cable Industry for Implementation of IPCablecom Technologies; Identification of high level requirements and establishment of priorities".

[17] IETF RFC 2327 April 1998: M. Handley and V. Jacobson; "SDP: Session Description Protocol".

[18] Directive 2002/22/EC [Universal Service Directive] of the European Parliament and of the Council on Universal service and users' rights relating to electronic communications networks and services. [OJ L 108, 24.4.2002].

[19] PacketCable™ Electronic Surveillance Specification PKT-SP-ESP-I04-040723 (Cable Television Laboratories, Inc.).

3 Definitions and abbreviations

3.1 Definitions

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

Access Node (AN): as used in TS 101 909-20-1 an Access Node is a layer two termination device that terminates the network end of the ITU-T Recommendation J.112 [11] connection. It is technology specific. In ITU_T Recommendation J.112 [11] annex A it is called the INA while in annex B it is the CMTS. In this document CMTS will be the preferred term.

(to) buffer: temporary storing of information in case the necessary telecommunication connection to transport information to the Law Enforcement Monitoring Facility (LEMF) is temporarily unavailable

Cable Modem: layer two termination device that terminates the customer end of the ITU-T Recommendation J.112 [11] (HFC Access Network) connection

call: any connection (fixed or temporary) capable of transferring information between two or more users of a telecommunications system

CMS: IPCablecom element that performs telecommunications-specific functions in the establishment of a call, such as address translation, call routing, directory services, usage recording, and authorization of QoS

content of communication: information exchanged between two or more users of a telecommunications service, excluding intercept related information. This includes information, which may, as part of some telecommunications service, be stored by one user for subsequent retrieval by another. This is also called call content.

Controlling Party: party invoking a feature

handover interface: physical and logical interface across which the interception measures are requested from an AP/NWO/SvP, and the results of interception are delivered from an AP/NWO/SvP to an LEMF

identity: technical label which may represent the origin or destination of any telecommunications traffic, as a rule clearly identified by a physical telecommunications identity number (such as a telephone number) or the logical or virtual telecommunications identity number (such as a personal number) which the subscriber can assign to a physical access on a case-by-case basis

Information Service:

(A) the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunication; and

(B) includes:

- (i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities;
- (ii) electronic publishing; and
- (iii) electronic messaging services; but

(C) does not include any capability for a telecommunications carrier's internal management, control, or operation of its telecommunications network. See also Telecommunication Carrier and TSP

intercept related information: collection of information or data associated with telecommunication services involving the target identity, specifically call associated information or data (e.g. unsuccessful call attempts), service associated information or data (e.g. service profile management by subscriber) and location information. This is also called call identifying information in TS 101 909-20-1

interception (lawful interception): action (based on the law), performed by an AP/NWO/SvP, of making available certain information and providing that information to an LEMF

interception interface: physical and logical locations within the network operator's/service provider's telecommunications facilities where access to the content of communication and intercept related information is provided. The interception interface is not necessarily a single, fixed point. In the IPCablecom network, the ***interception interface*** of a ***interception subject*** is the AN serving the subject, and the CMS designated by the IPCC/TSP which processes calls for the subject

interception measure: technical measure which facilitates the interception of telecommunications traffic pursuant to the relevant national laws and regulations

interception subject: person or persons, specified in a lawful authorization, whose telecommunications are to be intercepted

IPCablecom: architecture and a series of specifications that enable the delivery of real time services (such as telephony) over the cable television networks using cable modems

IPCC/TSP: IPCablecom Telecommunications Service Provider. As used in TS 101 909-20-1, an IPCC/TSP is an entity, typically a cable operator, that has:

(a) taken the steps necessary to be a "telecommunications carrier" for purposes of LI, and

(b) provides its telecommunications services using IPCablecom capabilities. The fact that an entity may use IPCablecom, including the use of IPCablecom for voice telephony applications, does not mean that the entity is a "telecommunications carrier" for purposes of LI or any other regulatory purpose. This is also called an operator in TS 101 909-20-1.

Law Enforcement Administrative Function (LEAF): is responsible for controlling the LEA Collection Function and maintenance of HI1. This function is under the responsibility of the LEMF

Law Enforcement Agency (LEA): organization authorized by a lawful authorization based on a national law to request interception measures and to receive the results of telecommunications interceptions

Law Enforcement Monitoring Facility (LEMF): law enforcement facility designated as the transmission destination for the results of interception relating to a particular interception subject. This is also called a collection function in TS 101 909-20-1

lawful authorization: permission granted to an LEA under certain conditions to intercept specified telecommunications and requiring co-operation from a network operator /access provider/service provider. Typically, this refers to a warrant or order issued by a lawfully authorized body

location information: information relating to the geographic, physical or logical location of an identity relating to an interception subject

network operator: operator of a public telecommunications infrastructure which permits the conveyance of signals between defined network termination points by wire, by microwave, by optical means or by other electromagnetic means

origin: number of the party initiating a call (e.g. calling party). See Call-Identifying Information

Publicly Available Telephone Service (PATS): means a service available to the public for originating and receiving national and international calls and access to emergency services through a number or numbers in a national or international telephone numbering plan, and in addition may, where relevant, include one or more of the following services: the provision of operator assistance, directory enquiry services, directories, provision of public pay phones, provision of service under special terms, provision of special facilities for customers with disabilities or with special social needs and/or the provision of non-geographic services (Universal Service Directive 2002/22/EC [18])

redirected call: call that is transferred (see Transferred call), or redirected as a service provided to a terminating subscriber, such as unconditionally, or when the terminating subscriber's line is busy, or when the terminating subscriber does not answer

Quality of Service (QoS): collective effect of service performance which determines the degree of satisfaction of a user of the service (taken from ITU-T Recommendation E.800)

reliability: probability that a system or service will perform in a satisfactory manner for a given period of time when used under specific operating conditions

result of interception: information relating to a target service, including the content of communication and intercept related information, which is passed by a network operator or service provider to a law enforcement agency. Intercept related information shall be provided whether or not call activity is taking place.

service provider: natural or legal person providing one or more public telecommunications services whose provision consists wholly or partly in the transmission and routing of signals on a telecommunications network. A service provider need not necessarily run his own network

Service Provider Administration Function: logically part of the OSS, but may be implemented according to operator preferences or national requirements

target identity: identity associated with a target service used by the interception subject

target service: telecommunications service associated with an interception subject and usually specified in a lawful authorization for interception

telecommunications: any transfer of signs, signals, writing images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photo-optical system

termination: number of the party ultimately receiving a call (e.g. answering party). See Call-Identifying Information

transferred call: call that changes either the originating party or terminating party, based on action taken by one of the parties in the call

transmission: See Telecommunications.

3.2 Abbreviations

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

AN	Access Node (See also CMTS)
AP	Access Provider
ASN.1	Abstract Syntax Notation version 1
BER	Basic Encoding Rules
CC	Content of Communication
CCIF	Content of Communication Interception Function
CID	Communication IDentifier
CM	Cable Modem
CMS	Call Management Server
CMS	Cryptographic Message Syntax
CMTS	Cable Modem Termination System (See also Access Node)
COPS	Common Open Policy Service protocol
DER	Distinguished Encoding Rules
DF	Delivery Function
DSS1	Digital Subscriber Signalling system No.1
ESP	IPSec Encapsulation Security
FTP	File Transfer Protocol
HFC	Hybrid Fibre/Coaxial [cable]
HI	Handover Interface
HI1	Handover Interface Port 1 (for Administrative Information)
HI2	Handover Interface Port 2 (for Intercept Related Information)
HI3	Handover Interface Port 3 (for Content of Communication)
HOLD	call HOLD supplementary service
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
INI	Internal Network Interface
IP	Internet Protocol
IPCC/TSP	IPCableCom Telecommunications Service Provider
IPSec	Internet Protocol Security
IRI	Intercept Related Information
IRIIF	IRI Intercept InterFace
ISDN	Integrated Services Digital Network
LCS	Line Control Signalling

LE	Local Exchange
LEA	Law Enforcement Agency
LEAF	Law Enforcement Administrative Function
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIAF	Lawful Intercept Administration Function
LIID	Lawful Interception IDentifier
LIMF	Lawful Intercept Mediation Function
MAC	Media Access Control
MAC	Message Authentication Code
MG	Media Gateway
MGC	Media Gateway Controller
MIB	Management Information Base
MTA	Media Terminal Adapter
NCS	Network-based Call Signalling
NWO	NetWork Operator
OSS	Operation System Support
PATS	Publicly Available Telephone Service
PCESP	Packet Cable Electronic Surveillance SPecification
PHY	PHYsical
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFC	Request For Comments
ROSE	Remote Operation Service Element
RSVP	Resource reSerVation Protocol
RTP	Real Time Protocol
SAP	Service Access Point
SCN	Switched Circuit Network
SCTE	Society of Cable Telecommunication Engineers
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SS	Supplementary Service
SvP	Service Provider
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

4 Lawful Interception overview

4.1 Lawful Interception principles

Although national surveillance regulations may not apply to any particular cable operator, in general, they require certain telecommunications carriers to ensure that their equipment, facilities, or services have the capability to:

a) Expeditiously isolate and enable the LEA to access reasonably available call identifying information.

b) Expeditiously isolate and enable the LEA to intercept all communications carried by a carrier within a service area to or from the equipment, facilities or services of a subscriber, concurrently with the communications' transmission.

c) Make intercepted communications and call identifying information available to the LEA in a format available to the carrier so they may be transmitted over packet or circuit switched (transit) networks by the LEA to a location away from the carrier's premises.

d) Meet these requirements with a minimum of interference with the subscriber's services and in such a way that protects the privacy of communications and call identifying information that are not authorized to be intercepted, and that maintains the confidentiality of the LEA's electronic surveillance.

The EU Data Protection Directives 95/46 [6] and 90/388 [7] and more particularly article 5 (see note) of the Telecommunications Data Protection Directive 97/66 [5] oblige Member States to ensure the confidentiality in public telecommunications networks, as well as publicly available telecommunication services. In addition, and in order to put article 5 into practice, under article 4 of the same Directive providers of public services and networks are required to take appropriate technical and organizational measures to safeguard the security of their services. In further accordance with the article, these measures must ensure a level of security that is appropriate to the risk presented, in view of the state of the art and the cost of their implementation. This means all network operators have a legal obligation to protect communications against unlawful interception.

NOTE: "Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunication network and publicly available telecommunication services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorized, in accordance with article 14 (1)"

4.2 Lawful Interception requirements

A complete list of LEA requirements are provided in TR 101 331 [10], however, this clause gives an overview of the expected operation for lawful interception that apply to an IPCablecom system. Reference should be made to TR 101 963 [16] which reflects the European Cable Network Operators' obligations for IPCablecom Lawful Interception.

4.2.1 Intercept administration requirements

A secure means of administrating the service by the IPCC/TSP and intercept requesting entity is necessary. This mechanism shall provide means to activate, deactivate, show, or list targets in the IPCablecom system as quickly as possible. The function shall be policed by appropriate authentication and audit procedures.

4.2.1.1 Activation of LI

As a result of the activation (of a warrant) it shall be possible to request for the specified target, either IRI, or both the IRI and the CC and designate the LEA destination addresses for the delivery of the CC and IRI if required. These shall be selectable on an IPCablecom system basis according to national options.

4.2.1.2 Deactivation of LI

As a result of deactivation it shall be possible to stop all, or a part of, interception activities for the specified target.

4.2.1.3 Security of processes

The intercept function shall only be accessible by authorized personnel. It should have authentication procedures to guard against unauthorized access, and all transmissions should be secured.

To be effective, interception shall take place without the knowledge of either party to the communication.

No indication shall be given to any person except authorized personnel that the intercept function has been activated on a target. Authentication, encryption, audits, log files and other mechanisms may be used to maintain security in the system. Audit procedures should be capable of keeping accurate logs of administration commands.

4.2.2 Intercept invocation

4.2.2.1 Invocation events for lawful interception

In general, Lawful Interception (LI) should be invoked when the transmission of information or an event takes place that involves the target. Examples of when Lawful Interception (LI) could be invoked are when:

- a voice telephony call is requested and either originated from, terminated to, or redirected by the target;
- the target selects a specified feature relating to a voice telephony call - e.g. CALL HOLD;

- the target activates, or deactivates, a particular network supported feature relating to the voice telephony service - e.g. CALL DIVERT.

4.2.2.2 Invocation and removal of interception regarding services

The invocation of lawful interception shall not alter the operation of a target's services or provide indication to any party involved in communication with the target. Lawful interception shall not alter the standard function of the IPCablecom network elements.

If lawful interception is activated during a voice telephony call, the currently active voice call is not required to be intercepted. If lawful interception is deactivated during a voice telephony call, all ongoing intercepted activities may continue until they are completed.

4.2.2.3 Correlation of information and product

When both IRI and CC are invoked, an unambiguous correlation shall be established between the two. The IRI and CC shall be delivered in as near real time as possible.

NOTE: Clarification about correlation limitations during interdomain (IPCablecom) call or session handovers is for further study.

4.2.2.4 Services subject to interception

The target service specifically addressed in the present document is the voice telephony service that is identifiable by a unique address (number) within a single IPCablecom domain.

NOTE: There may be more than one target service associated with a single interception subject.

4.3 Exceptional procedures

If a connection failure towards the LEA occurs, calls within the IPCablecom system shall operate normally, thus ensuring the target receives full capabilities of the voice service.

A national option may be that when failure occurs while trying to provide the IRI it shall be temporarily stored in the IPCablecom system and some further attempts shall be made to deliver it if available.

4.4 Interworking considerations

The IPCC/TSP shall not be responsible to interpret the protocol used by the target, or to remove user level compression or encryption. The IPCC/TSP is responsible for delivering the RTP media stream and service related information to the Lawful Intercept Mediation Function (LIMF).

The essential requirement is to deliver to the LIMF exactly what the operator receives from the subscriber, without attempting to interpret the stream i.e. provide a bit exact copy of the Content of Communication (CC).

4.5 Charging aspects

This clause does not refer to the subscriber charging, but to the charges applied by the operator to the LEA for services related to the intercept. The IPCC/TSP may charge for intercept service subject to national laws and regulations. Thus details of this clause are outside the scope of the present document.

Charging mechanisms may include the following:

- use of network resources;
- activation and deactivation of the target;
- every intercept invocation.

The IPCablecom system should be capable of producing intercept-charging data. It should be possible to produce this data in such a way that access by non-authorized personnel or the target is precluded. Charging data files shall be generated by the various components of the IPCablecom Architecture. Based upon the national laws and regulations the charging data files may be processed and used as the basis for accounting.

4.6 Minimum service requirements

Quality of service, capacity and reliability are the subject of bilateral agreement between the relevant authorities and the IPCC/TSP. The QoS towards the delivery function provided by the network shall be equivalent to that provided by the network to the target.

5 Functional architecture

5.1 Overview

Figure 1 contains the reference configuration for the lawful interception. The intercept function is viewed as five broad categories: access, delivery, mediation, service provider administration, and law enforcement administration. These functions are discussed functionally in this clause, without regard to their implementation. The various entities and interfaces are described in more detail in the succeeding clauses.

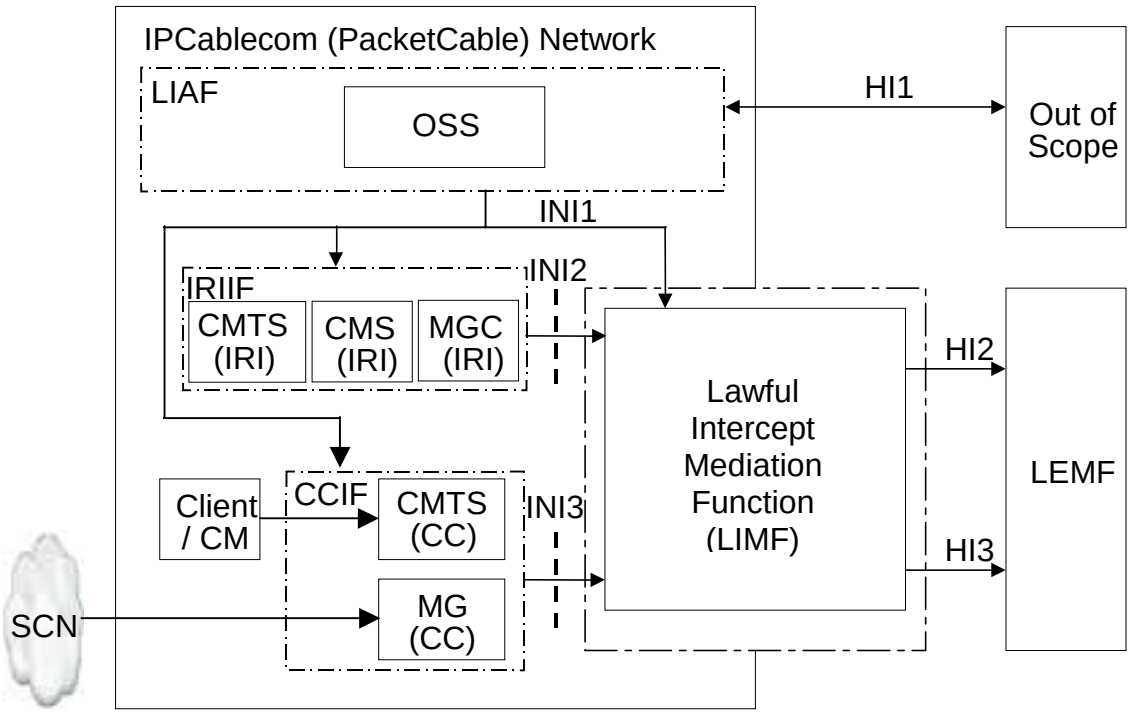


Figure 1: Intercept Architecture in IPCablecom

The reference configuration is only a logical representation of the entities involved in lawful interception and does not mandate separate physical entities. The operator's network may contain other elements beyond the scope of the present document relating to Lawful Interception (LI), but that the IPCablecom System itself defines a set of functions and interfaces supporting the Lawful interception requirements. The IPCablecom architecture makes no assumption or places any requirements on the bundling or unbundling of the functions; this is considered an operator determined implementation option. While the IPCablecom network operator is responsible according to TS 101 331 [10] for all the functions described, IPCablecom only covers the descriptions of the OSS, Intercept Functions (CMS, MGC, MG, CMTS) and Delivery/Mediation Function (LIMF) and; it does not cover the definition of the Law Enforcement Mediation Function (LEMF) or the handover interfaces (HI1, HI2 and HI3).

In addition, the service provider administration function (LIAF) is provided by a lawfully authorized order and administered by the operator using the Operational Support System (OSS), INI1 is considered an internal system interface and an example of the information flows are described in clause 7.

The internal intercept interface (INI2), as shown in figure 1, represents the point at which the Intercept Related Information (IRI) (i.e. call identifying information) is passed to the IPCablecom Lawful Intercept Mediation Function (LIMF). Similarly, internal intercept interface (INI3), as shown in figure 1, represents the point at which the Content of Communication (CC) (i.e. call content) is passed to the IPCablecom Lawful Intercept Mediation Function (LIMF).

The HI2 and HI3-interfaces represent the interfaces between the LEA LEMF and the IPCablecom LI Mediation Function (LIMF) and are defined by ES 201 671 [8] and TS 101 671 [9]. The LIMF is required to:

- distribute the Intercept Related Information (IRI) (i.e. call identifying information) to the relevant LEA(s) via HI2; this is received by the LIMF over an INI2 connection from the IRIIF. If the INI2 is delivered using Distinguished Encoding Rules (DER) ITU-T Recommendation X.690 [15] then the LIMF will need to decode and re-encode using Basic Encoding Rules (BER) ITU-T Recommendation X.690 [15].

- distribute the Content of Communication (CC) (i.e. call content) to the relevant LEA(s) via HI3; this is received by the LIMF over an INI3 connection from the CCIF. If the INI3 is delivered to the LIMF with network encryption, then it is the responsibility of the LIMF to remove the encryption (refer to clause 4.4).

The delivery may be IP or switched circuit based, subject to national requirements.

5.2 Functional Components

5.2.1 Subscriber functions in the E-MTA/CM

The core of providing all IPCablecom services, including any telecommunications services that a provider might offer, is the broadband access network. This network is characterized as a DOCSIS 1.1 [12] or later [DOCSIS] access network, but may be provided over access networks supporting other standards. The access network consists of the cable modem, the cable modem termination system, and the Media Access Control (MAC) and Physical (PHY) access layers.

The subscriber equipment includes those elements of the access network that are located in the customer's home. This includes the Cable Modem (CM) and the Multi-media Terminal Adapter (MTA).

The CM is an IPCablecom network element as defined by the DOCSIS [12] specification. The CM plays a key role in handling the media stream. Services which may be provided by the CM include classification of traffic into service flows according to classification filters, rate shaping, and prioritized queuing.

An MTA is a single hardware device that incorporates audio and optionally video IP telephony. An MTA may optionally incorporate a DOCSIS cable modem (an Embedded MTA) or may connect through external means to a DOCSIS cable modem (a Standalone MTA).

An MTA supports the following functionality:

- Provides one or more analogue PSTN interfaces to analogue terminals.
- Performs call signalling with the CMS to originate and terminate calls.
- Supports QoS signalling with the CMS and the CMTS.
- Supports security signalling with the CMS and other MTA devices.
- Supports provisioning signalling with the Provisioning server(s).
- Performs encoding/decoding of audio streams.
- Provides multiple audio indicators to phones, such as ringing tones, call waiting tones, stutter dial tone, dial tone, etc.
- Provides standard PSTN analogue line signalling for audio tones, voice transport, caller-id signalling, and message waiting indications.

NOTE: The IPCablecom system design places much of the session control intelligence at the endpoints, where it can easily scale with technology and provide new and innovative services. While this "future-proofing" is a goal of the design, it is recognized that it leaves open a wide range of fraud possibilities. The basic assumption is that the E-MTA is not immune to customer tampering, and that the significant incentive for free service will lead to some very sophisticated attempts to thwart any network controls placed on the E-MTA. Under these circumstances, it is important to realize that an MTA under customer control will likely not cooperate with LI, and methods are therefore described here that do not depend in any way on cooperation with the MTA.

5.2.2 Intercept functions in IPCablecom system

The intercept functions as shown in figure 1 isolate communication (CC) to and from a target or reasonably available call-identifying information unobtrusively. The Intercept Functions are responsible for the collection of Content of Communication (CC) and reasonably available call-identifying information. The IRI information is sent to the Lawful Intercept Mediation Function (LIMF) to be delivered to the LEMF over interface HI2.

In an IPCablecom network, four components are designated as Intercept Functions:

- The Cable Modem Termination System (CMTS) controls the set of cable modems attached to the shared medium of the DOCSIS [12] network and shall have the capability for intercepting the Content of Communication (CC).
- The Call Management System (CMS) provides service to the subscriber and shall have the capability for intercepting the Call-Identifying information (IRI).
- The Media Gateway (MG) shall have the capability, as an Content of Communication Intercept Function (CCIF), for purposes of intercepting Content of Communication (CC) (e.g. for redirected calls to the PSTN).
- The Media Gateway Controller (MGC) shall have the capability, as an Intercept Function (IRIIF), for purposes of intercepting the Call-identifying information (IRI) (e.g. for redirected calls to the PSTN).

The IPCC/TSP shall have the capability to intercept both ON-NET to ON-NET and ON-NET to OFF-NET, as well as OFF-NET to ON-NET redirected calls back to OFF-NET. Where this requires the cooperation of both the CMTS and MG for Content of Communication (CC) and the collaboration of all IAPs (CMTS, CMS, MG and MGC) for call-identifying information.

5.2.3 Content of Communication Interception Function (CCIF)

The Content of Communication Interception Function (CCIF) shall cause the Content of Communication (CC) to be duplicated and passed to the Lawful Interception Mediation Function (LIMF). The content may be duplicated within the media layer or within the transport layer and this may be achieved by any means such that the sender and recipient(s) are unaware of the copying process and cannot take steps that will reveal the copying process is taking place.

The content of communication is sent to the Lawful Interception Mediation Function (LIMF) and it is formatted in accordance with later clauses for delivery to the LEMF over interface HI3.

5.2.4 Lawful Interception Mediation Function (LIMF)

Within each administrative domain shall be an additional functional entity - the Lawful Interception Mediation Function (LIMF). This entity receives information from the IRIIF(s) within the administrative domain and formats them to be passed on to the Law Enforcement Mediation Function (LEMF) using the interface design specified in the Handover specification ES 201 671 [8]. If there is more than one Lawful Interception (LI) function within an administrative domain the Lawful Interception Mediation Function (LIMF) shall manage the reporting state of the call so that information is sent to the LEMF as if it were from a single Lawful Interception (LI) function. In this case the LIMF shall ensure that the reported information elements represent a consistent and single view of the intercept.

The Lawful Interception Mediation Function (LIMF) includes the ability to:

a) collect and deliver Content of Communication (CC) and available call-identifying information for each target to the LEMF;

b) protect (i.e. prevent unauthorized access to, or manipulation and disclosure of) intercept controls, intercepted call content, and call-identifying information, through methods that are consistent with the normal security policies of the affected IPCC/TSP;

c) ensure that delivery of LI information is only available for the period and in the jurisdictions stated in the lawful authorization;

d) deliver Content of Communication (CC) and available call-identifying information.

Enabling and disabling the LIMF is managed via the LIAF.

NOTE 1: Call-identifying information, Content of Communication (CC), or both, associated with a particular subject may need to be delivered to more than one LEMF simultaneously. This will occur when different LEAs are conducting independent investigations on the same target. In this instance the LIAF will establish separate instances of interception of the target.

NOTE 2: ES 201 671 [8] requires delivery of CC in "stereo mode"; that is to say the media channels shall not be summed, separate" virtual" channels are required for the CC in each direction.

5.2.5 Lawful Intercept Administration Function (LIAF)

In each administrative domain there exists a Lawful Interception Administration Function (LIAF) to manage requests for interception. This function ensures that the request from an LEA to send IRI and or CC information to an LEMF is acted upon. This function is not the subject of the present document and it is listed here for completeness.

The information available at the LIAF includes:

NOTE: This list is adapted from clause 7.1 of TS 101 671 [9].

- Identification of the interception subject (target identity).
- The agreed Lawful Interception IDentifier (LIID).
- Start and end, or start and duration, of the interception.
- Kind of interception information, i.e. IRI, CC or both.
- Destination address of the LEMF to which IRI information should be sent i.e. the HI2 destination address (if applicable).
- Destination address of the LEMF to which CC information should be sent i.e. the HI3 destination address (if applicable).
- Other details related to the intercept such as the value of options.
- A reference for authorization of the interception.
- Other information as required.

This information is placed in the Lawful Interception (LI) Function, Lawful Interception Mediation Function (LIMF) and Content of Communications Interception Function (CCIF) as necessary by means that are not described in the present document.

The LIAF sets the policies to protect (i.e. prevent unauthorized access to, or manipulation of, or disclosure of) intercept controls, intercepted call content (CC), and call-identifying information (IRI), consistent with the normal security policies of the affected IPCC/TSP.

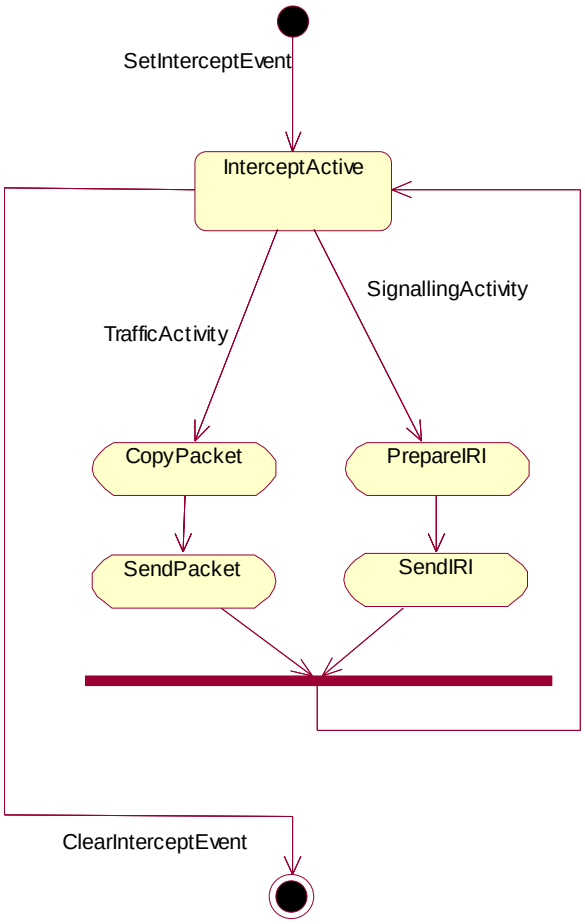


Figure 2: Simplified interception activity diagram

5.2.6 Law Enforcement Mediation Function (LEMF)

The definition of the LEMF is outside the scope of the present document.

NOTE: The LEMF is responsible for collecting intercepted communication (CC) and call-identifying information (IRI) via the handover point. The LEMF is the responsibility of the LEA. Enabling and disabling the activation of the LEA-provided interface is the responsibility of the LEA Administrative Function and is beyond the scope of the present document.

6 IPCablecom internal intercept interfaces

The internal intercept interfaces (see figure 1 reference point INI) are defined as part of the IPCablecom architecture, the requirements for these interfaces are defined within clause 7.

7 LI activation, deactivation and interrogation

This clause describes the requirements for interface INI1. It introduces the required information flows as well as the required data for the IRIIF.

It is not the intention of this clause to define a protocol for INI1. It rather aims to show which kind of information is necessary to be contained in the communication between LIAF and IRIIF. The means of transport may be UDP, TCP or embedded in an application protocol.

The information flows in the following clauses consist of request/response type messages. The request messages request a certain action. The responses confirm that the message was received and some means of status that allows the LIAF to know whether the request could be completed successfully or not.

7.1 Activation of LI

Clause 5.2.5 shows a list of data available at the LIAF. This information has to be conveyed to the IRIIF for the activation of the LI.

The information passed from the LIAF to the IRIIF for the purpose of the activation of LI shall include at least:

- LIID.
- Identities to intercept.
- Start, stop time, respectively the duration of the interception.
- Destination address of the DF for IRI.
- Credentials to fulfil the security service requirements for the delivery to the DF.

Figure 3 illustrates the information flow for the activation of LI. The number of concurrent LI activations in one message is an implementation issue. However, the activation of an entered LI at the HI1 shall be forwarded to the IRIIF immediately on reception.

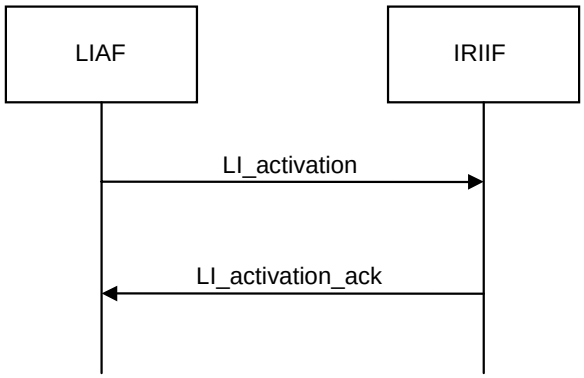


Figure 3: Information flow for the activation of LI

7.2 Modification of LI

This information flow is used to update a LI activity, e.g. to change the interception period or the communication identity used by the target.

Important information that shall be conveyed includes:

- LIID.
- Parameters to be changed.

The information flow is depicted in figure 4. The message to acknowledge the request contains the positive or negative result of the processed request.

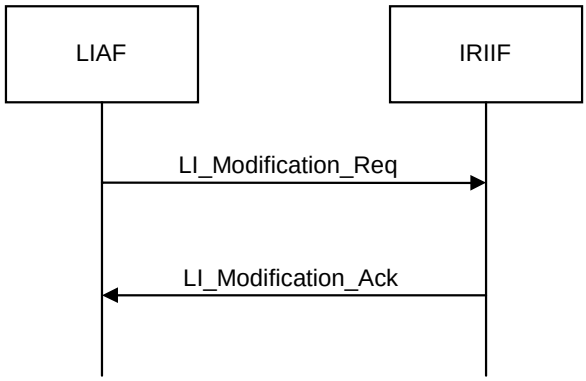


Figure 4: Information flow for the modification of an LI activity

7.3 Deactivation of LI

This flow is used to deactivate the LI of an LIID's identity or of all LIID related interceptions, as implemented. The required fields are:

- LIID.
- CID.

This request may be used to stop an ongoing interception for a certain communication identity before the interception period is finished. Reasons for such requests may include that the interception of a certain communication service is no longer required. The information flow is shown in figure 5.

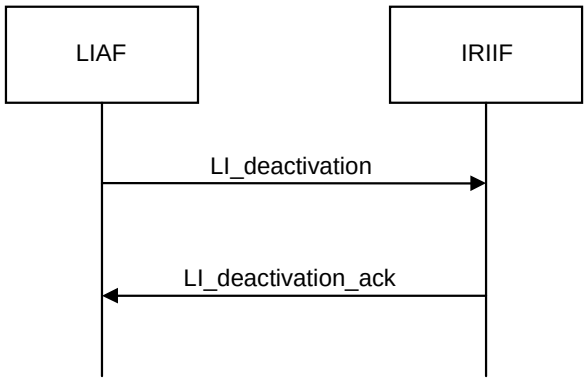


Figure 5: Information flow for the deactivation of an LI activity

7.4 Interrogation of LI

This information flow allows for requesting status information about certain LI activities at the IRIIF. The following fields shall be included:

- LIID.
- Relevant CID.
- Type of requested information.

Figure 6 demonstrates the corresponding message exchange.

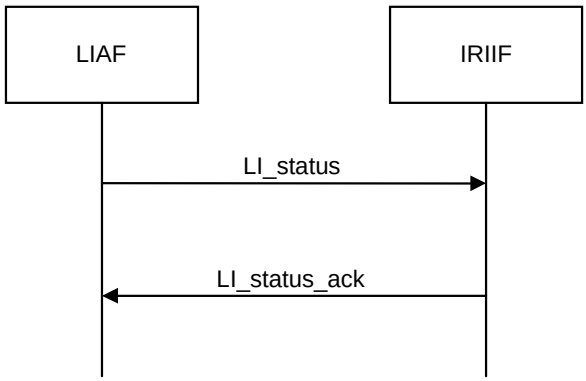
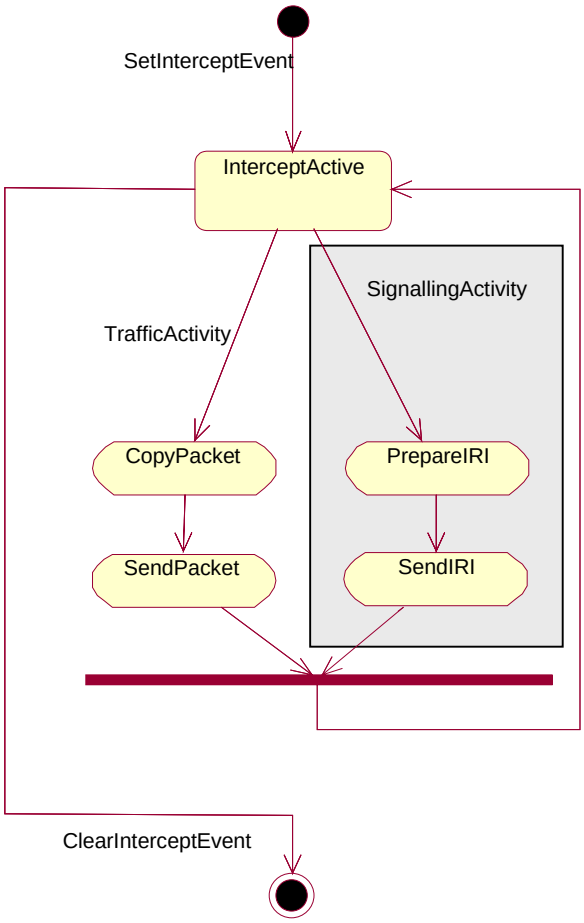


Figure 6: Information flow for requesting status about an LI activity

8 Interception of user signalling

Figure 7 illustrates the required interception activities. This clause covers the interception of user signalling whereas the interception of CC is described in clause 9.



NOTE: The figure shows both traffic and signalling interception for completeness, the shaded area shows the scope of this clause.

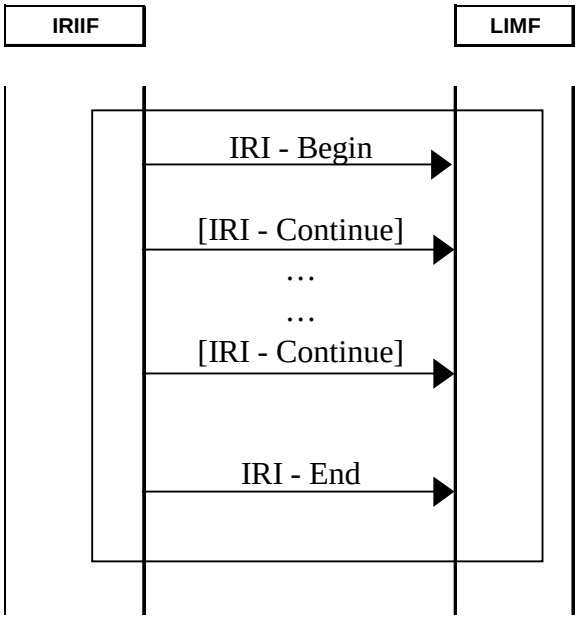
Figure 7: Simplified interception activity diagram

8.1 Interception protocol at interface INI2

There are four kinds of record type used across INI2, which are:

- Begin-record.
- Continue-record.
- End-record.
- Report-record.

The first three of these record types form an IRI-transaction.



NOTE: The bordered area of the chart indicates an IRI-transaction.

Figure 8: IRI protocol sequence chart

The use of each IRI record types is defined by table 1.

Table 1: Use of IRI Record Types

Record Type	When record type is used
Begin	First event of a communication attempt, opening the IRI transaction
Continue	Any time during a communication or communication attempt within the IRI transaction
End	The end of a communication or communication attempt, closing the IRI transaction
Report	Used in general for non-communication related events

8.1.1 Content of IRI Record

The IRI Record (the result of interception) shall contain:

1) the identities that have attempted communication with the target, successful or not;
2) the identities that the target has attempted communication with, successful or not;
3) identities used by or associated with the target;
4) details of services used and their associated parameters;
5) those signals emitted by the target invoking additional or modified services;

6) time-stamps for identifying the beginning, end and duration of the connection;

7) actual destination and intermediate directory numbers if call has been diverted;

in addition the IRI record should contain:

8) location information.

The result of interception shall apply to all call types if, and as long as, to the best knowledge of the network operator/service provider, the target is a participant.

8.2 Signal sets and interception

All signals in an IPCablecom environment can be classified using set theory as below (see also figure 9):

$$anySignal \in \{AllSignals\}$$
$$\{TransactionSignals\} \subset \{AllSignals\}$$
$$\{BeginSignals\} \subset \{TransactionSignals\}$$
$$\{EndSignals\} \subset \{TransactionSignals\}$$
$$\{ContinueSignals\} \subset \{TransactionSignals\}$$

The sets {*BeginSignals*}, {*EndSignals*} and {*ContinueSignals*} in general should have no intersections, i.e. *anySignal* should only be a member of one of these sets.

NOTE: In some protocols, e.g. SIP, the set of message types is very small and the same message type may belong to more than one set. In such cases the content of the message determines to which set the message belongs. In other protocols, e.g. ISDN (DSS1), the message type itself determines to which set the message belongs.

The logical processing model of interception is shown below:

IF $AnySignal \in \{BeginSignals\}$ THEN "prepare IRI-Begin record"

IF $AnySignal \in \{EndSignals\}$ THEN " prepare IRI-End record"

IF $AnySignal \in \{ContinueSignals\}$ THEN " prepare IRI-Continue record"

IF $AnySignal \notin \{TransactionSignals\}$ THEN " prepare IRI-Report record"

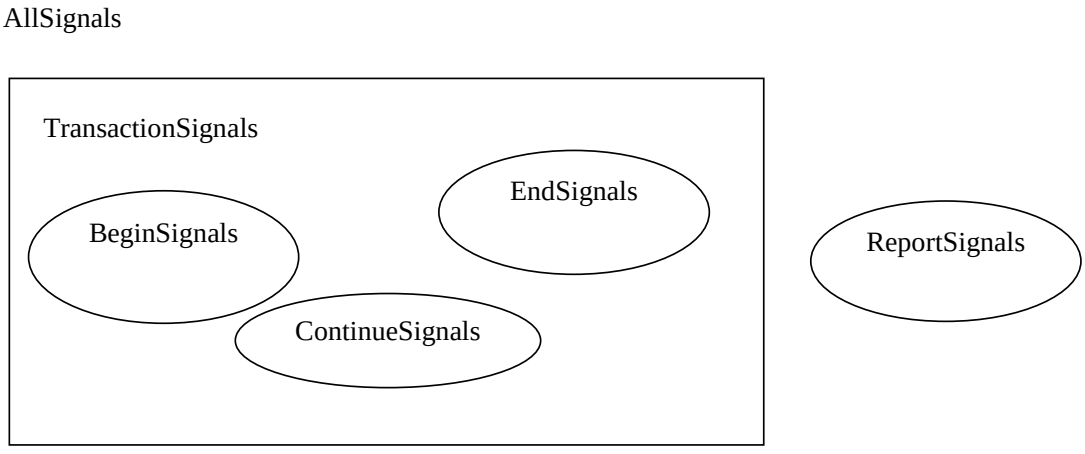


Figure 9: Venn diagram showing signal sets

8.3 Location of LI functions

The IRIIF function can be located within more than one IPCablecom functional entity:

- The Call Management Server (CMS);
- Media Gateway Controller (MGC);
- Media Gateway (MG);
- Cable Modem Termination System (CMTS).

The CCIF function is always located within the CMTS and MG functional entities.

8.4 Interception of specific signalling

The generic information flow that describes INI2 intercepted packets is defined below in the "target activity monitor" information.

8.4.1 IRI protocol service model

The IRI protocol model offers a single Service Access Point (SAP) as shown in figure 10 with the following requirements placed on the transfer protocol:

- Integrity: The intercepted data should be protected against data manipulation whilst in transit.
- Confidentiality: The intercepted data, if itself intercepted in transit, should not be able to reveal any information to the interceptor.
- Reliability and transmission requirement: There shall be no retransmission constraint placed on the IRI protocol itself.

NOTE: Where the network is physically reliable UDP may satisfy the latter requirement.

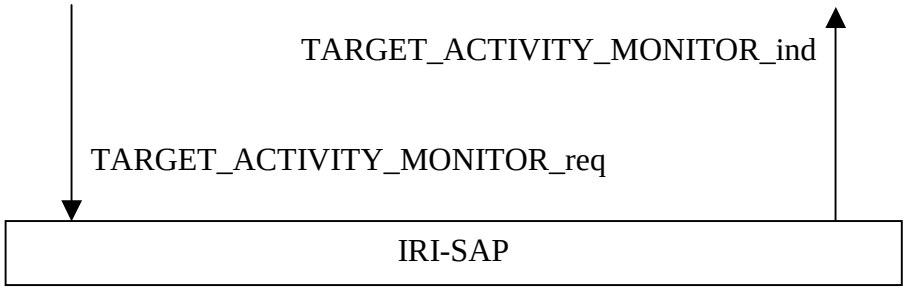


Figure 10: IRI protocol service model

The transmission protocol should employ the security mechanism defined in TS 101 909-11 [1] as pkt-s21 (and/or pkt-s23) as modified by clause 8 of TS 101 909-20-2 [3].

8.4.2 Target activity monitor

This information flow shall provide the activity of the target on the IPCablecom network to the LIMF. It has a header section indicating who, when and where, with a body section indicating the what of the target activity.

The IRI-Record shall by default be of type IRI-Report and the user-signal shall be sent as a bit exact copy of the signal, i.e. no interpretation shall be attempted.

```
TARGETACTIVITYMONITOR ::= SEQUENCE
{
    version                     INTEGER DEFAULT 2,          -- header, version -
    -- this module has version 2 because 'iRIMessage' is new
    lIInstanceid                LIIDType,                   -- header, who -
    timestamp                   UTCTime,                    -- header, when -
    targetLocation              LocationType,               -- header, where -
    direction                   DirectionType,
    iRITransaction              IRITransactionType DEFAULT iRIreport,
    iRITransactionNumber        INTEGER,
    userSignal                  UserSignalType,             -- Either copy or interpreted signalling
    cryptoCheckSum              BIT STRING              OPTIONAL,
    iRIMessageBER       IRIMessage     OPTIONAL,
    -- This parameter can only be used when the IRIMessage from the module IPCableComIRI
    -- is encoded using BER
    iRIMessageDER       OCTET STRING       OPTIONAL
    -- This Octet String contains the DER encoded parameters 'IRIMessage' from the
    -- module 'IPCableComIRI'
    -- parameter added in version 2
}
```

Protocol constraints:

Response to = None

Response expected = None

All parameter definitions are contained in a single ASN.1 module in annex A.

8.4.2.1 Data provision and encoding

8.4.2.1.1 Version

The version field identifies the version of the present document that the data structure is defined in. By default for this, the first version of the present document, the value of this field is 1.

8.4.2.1.2 Lawful Interception instance identity

The result of interception provided at the LEMF side of the LI interface shall be given a unique tag that shall allow identification of the LEA, the target, network operator/service provider and the warrant reference. This tag shall be first returned by the management activation flow (see annex B) and form part of the subsequent header data in TARGETACTIVITYMONITOR and TTRAFFIC/CTTRAFFIC information flows, as well as being used by the management information flows.

LIIdType ::= INTEGER(0 .. 65535) -- 16 bits -

8.4.2.1.3 Timestamp

Each IRI Record shall contain a timestamp indicating when the interception was made. The header of TARGETACTIVITYMONITOR information flow shall contain a mandatory timestamp information element. This element shall be of the type defined below:

```
UTCTime
```

NOTE: UTCTime is derived from the coordinated universal time system (see clause 3.1).

8.4.2.1.4 Target location

A network operator shall provide to the best of their knowledge any location information that may be requested by the LEA and addressed within the initiating warrant. Such data should be within the normal operating parameters of the network.

The location information should be delivered at one or more of the following times:

1) with registration;

2) with result of interception;

Location information relating to the target should be provided in the header of every TARGETACTIVITYMONITOR information flow. The header element shall contain either a nameAddress field (for static provision where the target location is known to the service provider and can be offered as a standard name and address field (as used when addressing the customer bill)) or as geodetic data giving the spatial coordinates of the target (e.g. GPS coordinates).

The location data shall be provided using the following data construct:

```
LocationType ::= CHOICE
{
        geodeticData        BIT STRING,
        nameAddress         PrintableString (SIZE (1..100))
}
```

8.4.2.1.5 Direction

The network operator shall provide, to the best of their knowledge, an indication of the direction of any signal, i.e. to or from the target.

The direction data shall be provided using the following data construct:

```
DirectionType ::= ENUMERATED
{
   toTarget,
   fromTarget,
   unknown
}
```

8.4.2.1.6 IRI transaction type

The result of interception shall indicate explicitly if the IRI-Record belongs to an IRI-Transaction, and if so of which type within the transaction.

The transaction type shall be provided using the following data construct:

```
IRITransactionType ::= ENUMERATED
{
        iRIbegin,
        iRIcontinue,
        iRIend,
        iRIreport
}
```

8.4.2.1.7 IRI transaction number

Along with the Lawful Interception (LI) instance identity this uniquely identifies an IRI Transaction. Where IRI transaction type is "iRIreport" this field shall be set to zero and should be ignored by the receiving entity. In all other instances IRIBegin shall increment the value of the IRI transaction number and this value shall be kept constant for all IRIcontinue and the final IRIend records.

8.4.2.1.8 User signal

The exact transaction of the user shall be provided, encoded as below.

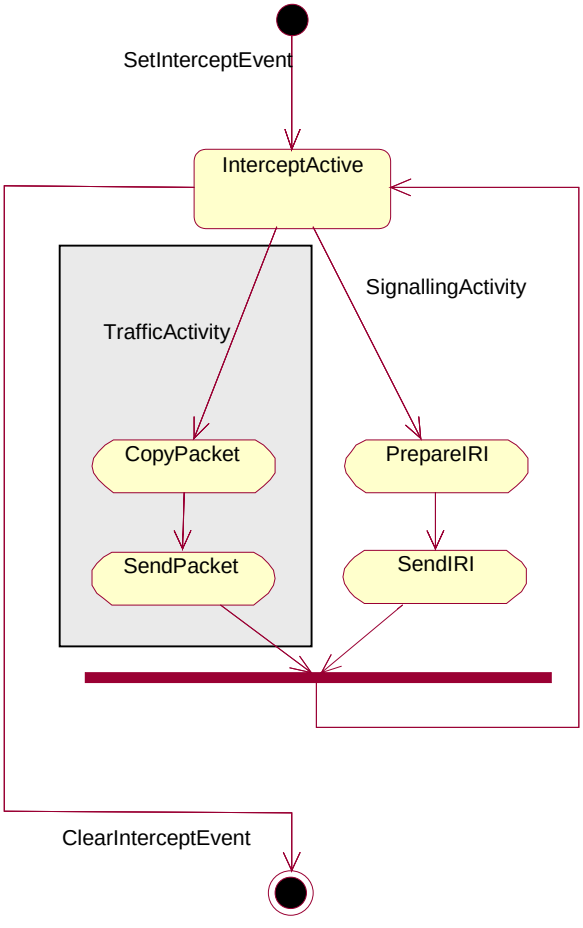
```
UserSignalType ::= CHOICE
{
    copySignal        BIT STRING,
    interpretedSignal INTEGER
}
```

8.4.2.1.9 Crypto check sum

The network operator may choose to assure himself of the integrity of the data intercepted by providing an cryptographic check sum to the main content of the interception record. The mechanism used should align with the overall security policy of the network operator.

9 Interception of Content of Communication (CC)

Figure 11 illustrates the required interception activities. This clause covers the interception of the Content of Communication (CC) whereas the interception of signalling is described in clause 8.



NOTE: The figure shows both traffic and signalling interception for completeness, the shaded area shows the scope of this clause.

Figure 11: Simplified interception activity diagram

9.1 Internal delivery of Content of Communication (CC) across interface INI3

NOTE: The interception methods described here apply only when IP is used for streaming media.

9.1.1 General model

The general model employed for delivery of content of communication over INI3 is to encapsulate the target and co-target traffic using the data structures T-Traffic and CT-Traffic defined in this clause. In addition this clause specifies the rules to be followed for embedding the intercepted traffic packet into the "TrafficPacket" element of the T-Traffic and CT-Traffic data structures.

The result of interception shall contain:

- the content of all calls originated by the target;
- the content of all calls to the target;
- the content of multi-party calls in which to the best knowledge of the network operator/service provider the target is participating;
- the content of broadcast calls to a user population of which to the best knowledge of the network operator/service provider the target is a member.

9.1.2 CC protocol service model

The CC protocol model offers a single Service Access Point (SAP) as shown in figure 12 with the following requirements placed on the transfer protocol:

- Integrity: The intercepted data should be protected against data manipulation whilst in transit.
- Confidentiality: The intercepted data, if itself intercepted in transit, should not be able to reveal any information to the interceptor.
- Reliability and transmission requirement: There shall be no retransmission constraint placed on the CC protocol itself.

NOTE: Where the network is physically reliable UDP may satisfy the latter requirement.

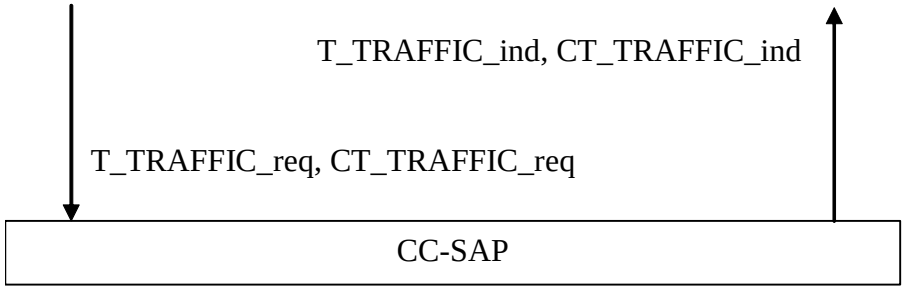


Figure 12: CC protocol service model

The transmission protocol should employ the security mechanism defined in TS 101 909-11 [1] as pkt-s22 or as modified by clause 8 of TS 101 909-20-2 [3].

9.1.2.1 T_TRAFFIC_req_ind

This information flow carries a traffic packet of the target to the DF.

```
TTRAFFIC ::= SEQUENCE
{
        version                 INTEGER DEFAULT 1,      -- header, version -
        lIInstanceid            LIIdType,
        iRITransactionNumber    INTEGER,
        trafficPacket           BIT STRING,
        cryptoChecksum          BIT STRING    OPTIONAL
}
```

Protocol constraints:

Response to = None

Response expected = None

9.1.2.2 CT_TRAFFIC_req_ind

This information flow carries a traffic packet of the co-target to the DF. Each successive correspondent shall be identified by incrementing the "correspondentCount" element of the information element.

```
CTTRAFFIC ::= SEQUENCE
{
        version                 INTEGER DEFAULT 1,      -- header, version -
        lIInstanceid            LIIdType,
        correspondentCount      INTEGER,
        iRITransactionNumber    INTEGER,
        trafficPacket           BIT STRING,
        cryptoChecksum          BIT STRING    OPTIONAL
}
```

Protocol constraints:

Response to = None

Response expected = None

9.1.2.3 Data provision and encoding

9.1.2.3.1 Version

The version field identifies the version of the present document that the data structure is defined in. By default for this, the first version of the present document, the value of this field is 1.

9.1.2.3.2 Lawful Interception instance identity

The result of interception provided at the LEMF side of the LI interface shall be given a unique tag that shall allow identification of the LEA, the target, network operator/service provider and the warrant reference. This tag shall be first returned by the management activation flow (see annex B) and form part of the subsequent header data in TARGETACTIVITYMONITOR and TTRAFFIC/CTTRAFFIC information flows, as well as being used by the management information flows.

LIIdType ::= INTEGER(0 .. 65535) -- 16 bits -

9.1.2.3.3 Correspondent count

The correspondent count field is used to distinguish the intercepted content of each of the target's correspondents. The first correspondent is given the value "0" and each successive correspondent shall be identified by incrementing the "correspondentCount".

9.1.2.3.4 IRI transaction number

Along with the Lawful Interception instance identity this field correlates the intercepted traffic to a known IRI-transaction. If correlation cannot be determined this field shall be set to zero and should be ignored by the receiving entity.

NOTE: The IRI transaction number along with the Lawful Interception instance identity performs a similar function to the Communication IDentifier (CID) defined in clause 6.2 of TS 101 671 [9].

9.1.2.3.5 Traffic packet

The traffic packet field contains a bit exact copy of the IP packet that has been intercepted.

9.1.2.3.6 Crypto check sum

The network operator may choose to assure himself of the integrity of the data intercepted by providing an cryptographic check sum to the main content of the interception record. The mechanism used should align with the overall security policy of the network operator.

Annex A (normative): ASN.1 Module

The data definitions for Lawful Interception (LI) used in TS 101 671 [9] are in the form of ASN.1 data types. The data definition rules given in annex D of TS 101 671 [9] shall apply, i.e. data shall be defined according to ITU-T Recommendation X.680 [14], and follow the Basic Encoding Rules (BER) defined in ITU-T Recommendation X.690 [15].

NOTE 1: The ASN.1 Module defined in the present document is named under the ETSI document tree and does not form a leaf of the ETSI LI tree as defined in TS 101 671 [9].

NOTE 2: The implementation provided in this annex assumes that the LIMF will be provided with the PCESP module using BER (refer to clause 5.1 for requirement on use of DER) and this in turn is exported to the TARGETACTIVITYMONITOR module before being delivered to the LEMF.

NOTE 3: Where the present document discusses "interception protocols" this term is only used to describe the information that must be carried on the handover interfaces when intercepting a target. This terminology is used to align with terminology used in the Lawful Intercept community and does not define protocol signalling.

Extension markers are not used in the ASN.1 module as the module is used in the SDL simulation model which does not support such markers. Instead the module identity contains the intercept version which shall be incremented on any change to the published module.

The data definition for each of the parameters included within the PCESP module (below) are given in the PacketCable™ Electronic Surveillance Specification PKT-SP-ESP-I04-040723 [19].

```
PCESP {iso(1) identified-organization(3) dod(6) internet(1) private(4)
       enterprise(1) cable-Television-Laboratories-Inc(4491) clabProject(2)
       clabProjPacketCable(2) pktcLawfulIntercept(5) pcesp(1) version-4(4)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN
ProtocolVersion ::= ENUMERATED {
  -- Versions IO1 and IO2 do not support protocol versioning.
  v3(3), -- Version supporting PacketCable Electronic Surveillance
         -- Specification I03
  v4(4), -- Version supporting PacketCable Electronic Surveillance
         -- Specification I04
...}

CdcPdu ::= SEQUENCE {
  protocolVersion       [0] ProtocolVersion,
  message               [1] Message,
  ...
}

Message ::= CHOICE {
  answer                [1] Answer,
  ccclose               [2] CCClose,
  ccopen                [3] CCOpen,
  reserved0             [4] NULL, -- Reserved
  origination           [5] Origination,
  reserved1             [6] NULL, -- Reserved
  redirection           [7] Redirection,
  release               [8] Release,
  reserved2             [9] NULL, -- Reserved
  terminationattempt    [10] TerminationAttempt,
  reserved              [11] NULL, -- Reserved
  ccchange              [12] CCChange,
  reserved3             [13] NULL, -- Reserved
  reserved4             [14] NULL, -- Reserved
  dialeddigitextraction [15] DialedDigitExtraction,
  networksignal         [16] NetworkSignal,
  subjectsignal         [17] SubjectSignal,
  mediareport           [18] MediaReport,
  serviceinstance       [19] ServiceInstance,
```

```
  confpartychange       [20] ConferencePartyChange,
  ...
}

Answer ::= SEQUENCE {
  caseId                [0] CaseId,
  accessingElementId    [1] AccessingElementId,
  eventTime             [2] EventTime,
  callId                [3] CallId,
  answering             [4] PartyId OPTIONAL,
  ...
}

CCChange ::= SEQUENCE {
  caseId                [0] CaseId,
  accessingElementId    [1] AccessingElementId,
  eventTime             [2] EventTime,
  callId                [3] CallId,
  cCCId                 [4] EXPLICIT CCCId,
  subject               [5] SDP OPTIONAL,
  associate             [6] SDP OPTIONAL,
  flowDirection         [7] FlowDirection,
  resourceState         [8] ResourceState OPTIONAL,
  ...
}

CCClose ::= SEQUENCE {
  caseId                [0] CaseId,
  accessingElementId    [1] AccessingElementId,
  eventTime             [2] EventTime,
  cCCId                 [3] EXPLICIT CCCId,
  flowDirection         [4] FlowDirection,
  ...
}

CCOpen ::= SEQUENCE {
  caseId                [0] CaseId,
  accessingElementId    [1] AccessingElementId,
  eventTime             [2] EventTime,
  ccOpenOption CHOICE {
  ccOpenTime            [3] SEQUENCE OF CallId,
  reserved0             [4] NULL, -- Reserved
  ...
                        },
  cCCId                 [5] EXPLICIT CCCId,
  subject               [6] SDP OPTIONAL,
  associate             [7] SDP OPTIONAL,
  flowDirection         [8] FlowDirection,
  ...
}

ConferencePartyChange ::= SEQUENCE {
  caseId                [0] CaseId,
  accessingElementId    [1] AccessingElementId,
  eventTime             [2] EventTime,
  callId                [3] CallId,
  communicating         [4] SEQUENCE OF SEQUENCE {
                            -- include to identify parties participating in the
                            -- communication.
    partyId  [0] SEQUENCE OF PartyId OPTIONAL,
                -- identifies communicating party identities.
    cCCId    [1] EXPLICIT CCCId OPTIONAL,
                -- included when the content of the resulting call is
                -- delivered to identify the associated CCC(s).
  ...
                        } OPTIONAL,
  removed               [5] SEQUENCE OF SEQUENCE {
                            -- include to identify parties removed (e.g., hold
                            -- service) from the communication.
    partyId  [0] SEQUENCE OF PartyId OPTIONAL,
                -- identifies removed party identity(ies).
    cCCId    [1] EXPLICIT CCCId OPTIONAL,
                -- included when the content of the resulting call is
                -- delivered to identify the associated CCC(s).
  ...
                        } OPTIONAL,
```

```
  joined                [6] SEQUENCE OF SEQUENCE{
                            -- include to identify parties newly added to the
                            -- communication.
    partyId  [0] SEQUENCE OF PartyId OPTIONAL,
                -- identifies newly added party identity(ies) to an existing
                -- communication.
    cCCId    [1] EXPLICIT CCCId OPTIONAL,
                -- included when the content of the resulting call is
                -- delivered to identify the associated CCC(s).
    ...
                        } OPTIONAL,
  ...
}

DialedDigitExtraction ::= SEQUENCE {
  caseId                [0] CaseId,
  accessingElementId    [1] AccessingElementId,
  eventTime             [2] EventTime,
  callId                [3] CallId,
  digits                [4] VisibleString (SIZE (1..32, ...)),
                            -- string consisting of digits representing
                            -- Dual Tone Multi Frequency (DTMF) tones
                            -- having values from the following numbers,
                            -- letters, and symbols:
                            -- '0", '1", '2", '3", '4", '5", '6", '7",
                            -- '8", '9", '#", '*", 'A", 'B", 'C", 'D".
                            -- Example: '123AB" or '*66" or '345#"
  ...
}

MediaReport ::= SEQUENCE {
  caseId                    [0] CaseId,
  accessingElementId        [1] AccessingElementId,
  eventTime                 [2] EventTime,
  callId                    [3] CallId,
  subject                   [4] SDP                     OPTIONAL,
  associate                 [5] SDP                     OPTIONAL,
  ...
}

NetworkSignal ::= SEQUENCE {
  caseId                    [0] CaseId,
  accessingElementId        [1] AccessingElementId,
  eventTime                 [2] EventTime,
  callId                    [3] CallId,
                                -- Signal
                                -- The following four parameters are used to report
                                -- information regarding network-generated signals.
                                -- Include at least one of the following four
                                -- parameters to identify the network-generated signal
                                -- being reported.
  alertingSignal            [4] AlertingSignal                    OPTIONAL,
  subjectAudibleSignal      [5] AudibleSignal                     OPTIONAL,
  terminalDisplayInfo       [6] TerminalDisplayInfo               OPTIONAL,
  other                     [7] VisibleString (SIZE (1..128, ...))  OPTIONAL,
                                -- Can be used to report undefined network signals
signaledToPartyId           [8] PartyId,
  ...
}

Origination ::= SEQUENCE {
  caseId                    [0] CaseId,
  accessingElementId        [1] AccessingElementId,
  eventTime                 [2] EventTime,
  callId                    [3] CallId,
  calling                   [4] PartyId,
  called                    [5] PartyId                   OPTIONAL,
  input                     CHOICE {
  userinput                   [6] VisibleString           (SIZE (1..32, ...)),
  translationinput            [7] VisibleString           (SIZE (1..32, ...)),
  ...
                            },
  reserved0                 [8] NULL,                     -- Reserved
  transitCarrierId          [9] TransitCarrierId          OPTIONAL,
  ...
}
```

```
Redirection ::= SEQUENCE {
  caseId                    [0] CaseId,
  accessingElementId        [1] AccessingElementId,
  eventTime                 [2] EventTime,
  old                       [3] CallId,
  redirectedto              [4] PartyId,
  transitCarrierId          [5] TransitCarrierId           OPTIONAL,
  reserved0                 [6] NULL,                      -- Reserved
  reserved1                 [7] NULL,                      -- Reserved
  new                       [8] CallId                     OPTIONAL,
  redirectedfrom            [9] PartyId                    OPTIONAL,
  ...
}

Release ::= SEQUENCE {
  caseId                    [0] CaseId,
  accessingElementId        [1] AccessingElementId,
  eventTime                 [2] EventTime,
  callId                    [3] CallId,
  ...
}

ServiceInstance ::= SEQUENCE {
  caseId                    [0] CaseId,
  accessingElementId        [1] AccessingElementId,
  eventTime                 [2] EventTime,
  callId                    [3] CallId,
  relatedCallId             [4] CallId                     OPTIONAL,
  serviceName               [5] VisibleString       (SIZE   (1..128, ...)),
  firstCallCalling          [6] PartyId                    OPTIONAL,
  secondCallCalling         [7] PartyId                    OPTIONAL,
  called                    [8] PartyId                    OPTIONAL,
  calling                   [9] PartyId                    OPTIONAL,
  ...
}

SubjectSignal ::= SEQUENCE {
  caseId                    [0] CaseId,
  accessingElementId        [1] AccessingElementId,
  eventTime                 [2] EventTime,
  callId                    [3] CallId                     OPTIONAL,
  signal                    [4] SEQUENCE {
                                -- The following four parameters are used to report
                                -- information regarding subject-initiated dialing and
                                -- signaling. Include at least one of the following four
                                -- parameters to identify the subject- initiated dialing
                                -- and signaling information being reported.
  switchhookFlash                      [0] VisibleString (SIZE (1..128, ...))  OPTIONAL,
  dialedDigits                         [1] VisibleString (SIZE (1..128, ...))  OPTIONAL,
  featureKey                           [2] VisibleString (SIZE (1..128, ...))  OPTIONAL,
  otherSignalingInformation            [3] VisibleString (SIZE (1..128, ...))  OPTIONAL,
                                -- Can be used to report undefined subject signals
  ...
                                },
  signaledFromPartyId       [5] PartyId,
  ...
}

TerminationAttempt ::= SEQUENCE {
  caseId                    [0] CaseId,
  accessingElementId        [1] AccessingElementId,
  eventTime                 [2] EventTime,
  callId                    [3] CallId,
  calling                   [4] PartyId                    OPTIONAL,
  called                    [5] PartyId                    OPTIONAL,
  reserved0                 [6] NULL,                      -- Reserved
  redirectedFromInfo        [7] RedirectedFromInfo         OPTIONAL,
  ...
}

AccessingElementId ::= VisibleString (SIZE(1..15, ...))
                           -- Statically configured element number
```

```
AlertingSignal ::= ENUMERATED {
  notUsed                   (0),    -- Reserved
  alertingPattern0          (1),    -- normal ringing
  alertingPattern1          (2),    -- distinctive ringing: intergroup
  alertingPattern2          (3),    -- distinctive ringing: special/priority
  alertingPattern3          (4),    -- distinctive ringing: electronic key
                                    -- telephone srvc
  alertingPattern4          (5),    -- ringsplash, reminder ring
  callWaitingPattern1       (6),    -- normal call waiting tone
  callWaitingPattern2       (7),    -- incoming additional call waiting tone
  callWaitingPattern3       (8),    -- priority additional call waiting tone
  callWaitingPattern4       (9),    -- distinctive call waiting tone
  bargeInTone               (10),   -- barge-in tone (e.g. for operator barge-in)
  alertingPattern5          (11),   -- distinctive ringing: solution specific
  alertingPattern6          (12),   -- distinctive ringing: solution specific
  alertingPattern7          (13),   -- distinctive ringing: solution specific
  alertingPattern8          (14),   -- distinctive ringing: solution specific
  alertingPattern9          (15),   -- distinctive ringing: solution specific
  ...
}
-- This parameter identifies the type of alerting (ringing) signal that is
-- applied toward the surveillance subject. See GR-506-CORE, LSSGR: Signaling
-- for Analog Interfaces (A Module of the LATA Switching Systems Generic
-- Requirements [LSSGR], FR-64).

AudibleSignal ::= ENUMERATED {
  notUsed                   (0),    -- Reserved
  dialTone                  (1),
  recallDialTone            (2),    -- recall dial tone, stutter dial tone
  ringbackTone              (3),    -- tone indicates ringing at called party
                                    -- end
  reorderTone               (4),    -- reorder tone, congestion tone
  busyTone                  (5),
  confirmationTone          (6),    -- tone confirms receipt and processing of
                                    -- request
  expensiveRouteTone        (7),    -- tone indicates outgoing route is
                                    -- expensive
  messageWaitingTone        (8),
  receiverOffHookTone       (9),    -- receiver off-hook tone, off-hook warning
                                    -- tone
  specialInfoTone           (10),   -- tone indicates call sent to announcement
  denialTone                (11),   -- tone indicates denial of feature request
  interceptTone             (12),   -- wireless intercept/mobile reorder tone
  answerTone                (13),   -- wireless service tone
  tonesOff                  (14),   -- wireless service tone
  pipTone                   (15),   -- wireless service tone
  abbreviatedIntercept      (16),   -- wireless service tone
  abbreviatedCongestion     (17),   -- wireless service tone
  warningTone               (18),   -- wireless service tone
  dialToneBurst             (19),   -- wireless service tone
  numberUnObtainableTone    (20),   -- wireless service tone
  authenticationFailureTone (21),   -- wireless service tone
  ...
}
-- This parameter identifies the type of audible tone that is applied toward
-- the surveillance subject. See GR-506-CORE, LSSGR: Signaling for Analog
-- Interfaces (A Module of the LATA Switching Systems Generic Requirements
-- [LSSGR], FR-64), ANSI/TIA/EIA-41-D, Cellular Radiotelecommunications
-- Intersystem Operations, and GSM 02.40, Digital cellular telecommunications
-- system (Phase 2+); Procedure for call progress indications.

CallId ::= SEQUENCE {
  sequencenumber            [0] VisibleString (SIZE(1..25, ...)),
  systemidentity            [1] VisibleString (SIZE(1..15, ...)),
  ...
}
-- The Delivery Function generates this structure from the
-- Billing-Correlation-ID (contained in the Event Messages).
-- The sequencenumber is generated by converting the
-- Timestamp (32 bits) and Event-Counter (32 bits) into
-- ASCII strings, separating them with a comma.
-- The systemidentity field is copied from the Element-ID field

CaseId ::= VisibleString (SIZE(1..25, ...))

CCCId ::= CHOICE {
  combCCC                   [0] VisibleString (SIZE(1..20, ...)),
  sepCCCpair                [1] SEQUENCE{
```

```
  sepXmitCCC                [0] VisibleString (SIZE(1..20, ...)),
  sepRecvCCC                [1] VisibleString (SIZE(1..20, ...)),
  ...
                            },
  ...
}
-- The Delivery Function MUST generate this structure
-- from the CCC-Identifier used for the corresponding
-- Call Content packet stream by converting the 32-bit
-- value into an 8-character (hex-encoded) ASCII string
-- consisting of digits 0-9 and letters A-F.

EventTime ::= GeneralizedTime

FlowDirection ::= ENUMERATED {
  downstream                (1),
  upstream                  (2),
  downstream-and-upstream   (3),
  ...
}

PartyId ::= SEQUENCE {
  reserved0                 [0] NULL                          OPTIONAL,   -- Reserved
  reserved1                 [1] NULL                          OPTIONAL,   -- Reserved
  reserved2                 [2] NULL                          OPTIONAL,   -- Reserved
  reserved3                 [3] NULL                          OPTIONAL,   -- Reserved
  reserved4                 [4] NULL                          OPTIONAL,   -- Reserved
  reserved5                 [5] NULL                          OPTIONAL,   -- Reserved
  dn                        [6] VisibleString (SIZE(1..15, ...)) OPTIONAL,
  userProvided              [7] VisibleString (SIZE(1..15, ...)) OPTIONAL,
  reserved6                 [8] NULL                          OPTIONAL,   -- Reserved
  reserved7                 [9] NULL                          OPTIONAL,   -- Reserved
  ipAddress                 [10] VisibleString (SIZE(1..32, ...)) OPTIONAL,
  reserved8                 [11] NULL                         OPTIONAL,   -- Reserved
  trunkId                   [12] VisibleString (SIZE(1..32, ...)) OPTIONAL,
  reserved9                 [13] NULL                         OPTIONAL,   -- Reserved
  genericAddress            [14] VisibleString (SIZE(1..32, ...)) OPTIONAL,
  genericDigits             [15] VisibleString (SIZE(1..32, ...)) OPTIONAL,
  genericName               [16] VisibleString (SIZE(1..48, ...)) OPTIONAL,
  port                      [17] VisibleString (SIZE(1..32, ...)) OPTIONAL,
  context                   [18] VisibleString (SIZE(1..32, ...)) OPTIONAL,
  ...
}

RedirectedFromInfo ::= SEQUENCE {
  lastRedirecting           [0] PartyId                       OPTIONAL,
  originalCalled            [1] PartyId                       OPTIONAL,
  numRedirections           [2] INTEGER (1..100, ...)         OPTIONAL,
  ...
}

ResourceState ::= ENUMERATED {reserved(1), committed(2), ...}

SDP ::= UTF8String
-- The format and syntax of this field are defined in [8].

TerminalDisplayInfo ::= SEQUENCE {
  generalDisplay            [0] VisibleString (SIZE (1..80, ...)) OPTIONAL,
    -- Can be used to report display-related
    -- network signals not addressed by
    -- other parameters.
  calledNumber              [1] VisibleString (SIZE (1..40, ...)) OPTIONAL,
  callingNumber             [2] VisibleString (SIZE (1..40, ...)) OPTIONAL,
  callingName               [3] VisibleString (SIZE (1..40, ...)) OPTIONAL,
  originalCalledNumber      [4] VisibleString (SIZE (1..40, ...)) OPTIONAL,
  lastRedirectingNumber     [5] VisibleString (SIZE (1..40, ...)) OPTIONAL,
  redirectingName           [6] VisibleString (SIZE (1..40, ...)) OPTIONAL,
  redirectingReason         [7] VisibleString (SIZE (1..40, ...)) OPTIONAL,
  messageWaitingNotif       [8] VisibleString (SIZE (1..40, ...)) OPTIONAL,
  ...
}
-- This parameter reports information that is displayed on the surveillance
-- subject's terminal. See GR-506-CORE, LSSGR: Signaling for Analog
-- Interfaces (A Module of the LATA Switching Systems Generic Requirements [LSSGR], FR-64).

TransitCarrierId ::= VisibleString (SIZE(3..7, ...))

END - PCESP
```

```
TS101909201 {itu-t (0) identified-organization (4) etsi (0) ts101909 (1909) part20 (20) subpart1(1)
interceptVersion (0)}

DEFINITIONS AUTOMATIC TAGS ::=

BEGIN

IMPORTS
    CdcPdu  FROM
        PCESP {iso(1) identified-organization(3) dod(6) internet(1) private(4)
        enterprise(1) cable-Television-Laboratories-Inc(4491) clabProject(2)
        clabProjPacketCable(2) pktcLawfulIntercept(5) pcesp(1) version-4(4)};

TARGETACTIVITYMONITOR-1 ::= SEQUENCE
{
    version                     INTEGER DEFAULT 1,         -- header, version -
    lIInstanceid                LIIDType,                  -- header, who -
    timestamp                   UTCTime,                   -- header, when -
    targetLocation              LocationType,              -- header, where -
    direction                   DirectionType,
    iRITransaction              IRITransactionType DEFAULT iRIreport,
    iRITransactionNumber        INTEGER,
    userSignal                  UserSignalType,            -- Either copy or interpreted signalling
    cryptoCheckSum              BIT STRING             OPTIONAL
}

TTRAFFIC ::= SEQUENCE
{
        version                  INTEGER DEFAULT 1,      -- header, version -
        lIInstanceid             LIIDType,
        iRITransactionNumber     INTEGER,
        trafficPacket            BIT STRING,
        cryptoChecksum           BIT STRING    OPTIONAL
}

CTTRAFFIC ::= SEQUENCE
{
        version                  INTEGER DEFAULT 1,      -- header, version -
        lIInstanceid             LIIDType,
        correspondentCount       INTEGER,
        iRITransactionNumber     INTEGER,
        trafficPacket            BIT STRING,
        cryptoChecksum           BIT STRING    OPTIONAL
}

DirectionType ::= ENUMERATED
{
   toTarget,
   fromTarget,
   unknown
}

UserSignalType ::= CHOICE
{
        copySignal          BIT STRING,
     interpretedSignal  INTEGER,
    cdcPdu          CdcPdu
}

IRITransactionType ::= ENUMERATED
{
        iRIbegin,
        iRIcontinue,
        iRIend,
        iRIreport
}

LocationType ::= CHOICE
{
        geodeticData        BIT STRING,
        nameAddress         PrintableString (SIZE (1..100))
}

LIIDType ::= INTEGER (0..65535) -- 16 bit integer to identify interception

END
```

Annex B (informative): Information call flows for Lawful Interception invocation of "voice telephony services"

B.1 On-Net to On-Net calls

In case of an On-Net to On-Net call the CMS is in full control of the call. In the case where the called party is the target, lawful interception is performed in the following way:

1) CMS identifies that the called party is subject to LI, the target identity.

2) CMS sends copies of the IRI to the LIMF (e.g. number of called party).

3) CMS sends a copy of the SDP-parameter to the LIMF, the SDP-parameters include amongst others the encryption keys.

4) CMS instructs the CMTS as part of the Gate-control messages (for the target E-MTA) to copy call-content to a specific LIMF, the LIMF is identified by an IP-address and UDP port number.

5) CMS instructs the CMTS as part of the Gate-control messages (for the target E-MTA) to copy call-events to a specific LIMF, the LIMF is identified by an IP-address and UDP port number.

6) As the LIMF receives all IRI and the bearer traffic (CC) the LIMF decrypts the bearer traffic and delivers the call content in the requested form to the LEA.

NOTE: Further examples of call flows are for further study.

B.2 On-Net to Off-Net calls

In case of an On-Net to Off-Net call the CMS treats the MG (Media Gateway) as the endpoint. In the case where the target is the originator of a call, lawful intercept is performed in the following way:

1) CMS identifies that the originator of a call is subject to LI.

2) CMS sends copies of a call-related information to LIMF (this includes e.g. number of called party).

3) CMS sends a copy of the SDP-parameter to the LIMF, the SDP-parameters include amongst others the encryption keys.

4) CMS instructs the CMTS as part of the Gate-control messages (for the target E-MTA) to copy call-content to a specific LIMF, the LIMF is identified by an IP-address and UDP port number.

5) CMS instructs the CMTS as part of the Gate-control messages (for the target E-MTA) to copy call-events to a specific LIMF, the LIMF is identified by an IP-address and UDP port number.

6) As the LIMF receives all IRI and the bearer traffic (CC) the LIMF decrypts the bearer traffic and delivers the call content in the requested form to the LEA.

NOTE: Further examples of call flows are for further study.

Annex C (informative): Bibliography

IETF RFC 768 (1980): "User Datagram Protocol".

IETF RFC 791 (1981): "Internet Protocol".

IETF RFC 826 (1982): "Ethernet Address Resolution Protocol".

IETF RFC 894 (1984): "Standard for the Transmission of IP Datagrams over Ethernet Networks".

IETF RFC 959: "File Transfer Protocol".

IETF RFC 1889 (1996): "RTP: A Transport Protocol for Real-Time Applications".

IETF RFC 1890 (1996): "RTP Profile for Audio and Video Conferences with Minimal Control".

IETF RFC 1958: "Architectural Principles of the Internet".

IETF RFC 2205: "Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification".

IETF RFC 2210: "The Use of RSVP with IETF Integrated Services".

IETF RFC 2211: "Specification of the Controlled-Load Network Element Service".

IETF RFC 2228: "FTP Security Extensions".

IETF RFC 2401: "Security Architecture for the Internet Protocol".

IETF RFC 2408: "Internet Security Association and Key Management Protocol (ISAKMP)".

IETF RFC 2409: "The Internet Key Exchange (IKE)".

IETF RFC 2747: "RSVP Cryptographic Authentication".

IETF RFC 2753: "A Framework for Policy-based Admission Control".

IETF RFC 2748 (2000): "The COPS (Common Open Policy Service) Protocol".

IETF RFC 2327 (1998): "SDP: Session Description Protocol".

Extensions to RSVP for LSP Tunnels, draft-ietf-mpls-rsvp-lsp-tunnel-07.txt, (August 2000): Awduche, D. et al.

060601COM Net Security: Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee of the Regions.

ITU-T Recommendation X.880: "Information technology - Remote Operations: Concepts, model and notation".

ITU-T Recommendation X.881: "Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) service definition".

ITU-T Recommendation X.882: "Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) protocol specification".

ITU-T Recommendation E.800: "Terms and definitions related to quality of service and network performance including dependability".

TIA/EIA J-STD-025-A-2003 (April 6, 2003): "Lawfully Authorized Electronic Surveillance".

TIA/EIA J-STD-025-B-2003 (December 1, 2003): "Lawfully Authorized Electronic Surveillance".

ETSI ES 200 800: "Digital Video Broadcasting (DVB); DVB interaction channel for Cable TV distribution systems (CATV)".

ETSI TS 101 909-1: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 1: General".

ETSI TS 101 909-2 (V.1.1.1): "Access and Terminals (AT);Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 2: Architectural framework for the delivery of time critical services over cable Television networks using cable modems".

ETSI TS 101 909-3 (V.1.1.1): "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 3: Audio Codec Requirements for the Provision of Bi-Directional Audio Service over Cable Television Networks using Cable Modems".

ETSI TS 101 909-4 (V.1.2.2): "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 4: Network Call Signalling Protocol".

ETSI TS 101 909-5 (V.1.1.1): "Access and Terminals (AT);Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 5: Dynamic Quality of Service for the Provision of Real Time Services over Cable Television Networks using Cable Modems".

ETSI TS 101 909-6 (V.1.1.1): "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 6: Media Terminal Adapter (MTA) device provisioning".

ETSI TS 101 909-7 (V.1.1.1): "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 7: Management Information Base (MIB) Framework".

ETSI TS 101 909-8 (V.1.1.1): "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 8: Media Terminal Adapter (MTA) Management Information Base (MIB)".

ETSI TS 101 909-9 (V.1.1.1): "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 9: Network Call Signalling (NCS) MIB Requirements".

ETSI TS 101 909-10 (V.1.1.1): "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 10: Event Message Requirements for the Provision of Real Time Services over Cable Television Networks using Cable Modems".

ETSI TS 101 909-13-2 (V.1.1.1): "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 13: Trunking Gateway Control Protocol; Sub-part 2: MGCP option".

ETSI TR 101 944: "Telecommunications Security; Lawful Interception (LI); Issues on IP Interception".

History

Document history		
V1.1.2	October 2005	Publication